Instituto Politécnico de Coimbra

INSTITUTO SUPERIOR DE ENGENHARIA DE COIMBRA

ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE DE COIMBRA

Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde

MESTRADO EM SISTEMAS E TECNOLOGIAS DA INFORMAÇÃO PARA A SAÚDE

AUTOR | FRANCISCO VILHENA ALVES DE CARVALHO

ORIENTADOR | **Prof. Doutor António Carvalho Santos | ESTSC**
Coorientador | Mestre João Almeida | ESTSC

Coimbra, dezembro, 2012

MSTIS Modelo Documental para Políticas de Segurança da Informação em Organizações de Saúde

2012

Instituto Superior de Engenharia de Coimbra

ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE DE COIMBRA

Instituto Politécnico de Coimbra

Instituto Superior de Engenharia de Coimbra

Escola Superior de Tecnologia da Saúde Coimbra

Mestrado em Sistemas e Tecnologias da Informação para a Saúde

Projecto/Estágio I e Projecto/Estágio II

Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde

FRANCISCO VILHENA ALVES DE CARVALHO

Orientador:

Professor Doutor António Carvalho Santos

Escola Superior de Tecnologia da Saúde de Coimbra

Co- Orientador:

Mestre João Almeida

Escola Superior de Tecnologia da Saúde de Coimbra

Coimbra, Dezembro, 2012

À Conceição, incansável esposa na minha motivação e toda a família que me tem apoiado, muitas vezes privada da minha presença, os meus especiais agradecimentos, prometo compensa-los com a minha disponibilidade e atenção futuramente.

AGRADECIMENTOS

Ao Professor Doutor António Carvalho dos Santos, meu orientador, um especial agradecimento e o meu total reconhecimento pela oportunidade criada para a realização deste trabalho, assim como a sua disponibilidade, colaboração, apoio, orientação, amizade e persistência.

Ao Mestre João Almeida, meu co-orientador, o meu agradecimento pela disponibilidade e ajuda no debater e esclarecimento de ideais e dúvidas.

Aos meus colegas de trabalho, um muito obrigado pela força dada.

Aos meus colegas do MSTIS, que ao longo de muitas e incansáveis horas de biblioteca debatemos ideias e dúvidas, um muito obrigado.

Ao Eng.º José Casinhas, Eng.º Luís Martins e Dr. Rui Gomes, um muito obrigado pela disponibilidade e pela análise crítica e construtiva realizada ao modelo desenvolvido.

Ao Instituto Superior de Engenharia de Coimbra pela formação concedida e ter proporcionado as condições necessárias para desenvolver este trabalho.

À Escola Superior de Tecnologia da Saúde de Coimbra por ter facultado as condições necessárias para que pudesse realizar, desenvolver e terminar este trabalho.

Aos muitos amigos que direta ou indiretamente contribuíram para que fosse possível realizar e concluir este trabalho, um muito obrigado.

Modelo Documental para Politicas de Segurança de Informação em Organizações de Saúde - MDPSIOS

RESUMO

A gestão da segurança da informação é uma área em que os desafios têm aumentado de forma significativa nos últimos tempos, devido em grande parte da evolução espantosa nas áreas das tecnologias de informação e comunicações (TIC). As TIC têm estado na linha da frente nas necessidades e resolução de problemas de gestão, logística e operacionais de qualquer organização em qualquer área de actividade. Esta evolução tem permitido que diferentes organizações em distintas áreas de actividade, através da sua adesão a estas novas tecnologias, passem a conviver com novos problemas que até então não seriam espectáveis na gestão da sua informação.

Estas organizações já entenderam que os seus sistemas de informação não são ilhas isoladas, que fazem parte de um sistema complexo com um fluxo de informações outrora inimaginável e que os riscos que lhe estão associados necessitam de ser identificados e tratados de forma apropriada e coerente. Mais delicado se torna quando estas organizações estão ligadas à área da saúde, e lidam sistematicamente com informação pessoal de saúde e estão subjugadas a obrigações de conformidade ética e legal, o que leva e transmite uma grande responsabilidade e peso, na gestão da informação que tratam e produzem.

No entanto, a maior dificuldade surge da necessidade de partir para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), e é necessário dar o primeiro passo para sustentar essa tomada de decisão perante os gestores da organização. A implementação de um SGSI, ainda é vista somente para fins de certificação. Os projetos e ofertas para implementação disponíveis no mercado são avultados e os recursos internamente necessários poderão ser imensos, dependendo da dimensão da organização e do nível requerido de implementação.

O objetivo principal deste trabalho foi o de propor um modelo documental simplificado (Modelo Documental para Politicas de Segurança de Informação em Organizações de Saúde - MDPSIOS) que permita a implementação e gestão de um SGSI sem fins de certificação, de forma ágil e sustentada e em qualquer organização, com especial atenção para as organizações da área de saúde.

Este modelo, está suportado pela metodologia da norma ISO/IEC 27001 para a gestão do sistema SGSI, pela norma ISO/IEC 27002 e ISO/IEC 27799 para implementação dos

controlos associados à gestão do risco. Na componente análise/avaliação de risco está suportado pela metodologia da norma ISO/IEC 27005. A utilização destas normas na criação deste modelo incorpora a devida consistência e dá o suporte necessário para que esteja de acordo com as boas práticos e metodologias, reconhecidas mundialmente. A estimativa de risco do modelo proposto é baseado no Método simplificado quantitativo de Avaliação de Riscos da Segurança da Informação (MARSI), que permite quantificar a magnitude dos riscos existentes e, como consequência, hierarquizar de modo racional a prioridade da sua eliminação ou correção. Esta combinação de normas e a integração deste método quantitativo para avaliação da estimativa de risco, faz com que a solução apresentada seja de alguma forma inovadora e acrescido da simplificação do processo de implementação e gestão de um SGSI. O modelo funcionalmente, foi desenvolvido com o recurso ao *software* Excel, para todos os aspetos operacionais, tornando-o bastante intuitivo, flexível, adaptável e fácil incremento de novas funcionalidades. O modelo está especialmente direcionado para as organizações de saúde no entanto devido a abrangência dos seus princípios pode ser utilizado por qualquer tipo de organização.

No que diz respeito à avaliação do modelo proposto, recorreu-se a uma análise qualitativa efetuada por três peritos (consultores ou auditores na área da segurança da informação). Estes peritos apresentavam no seu curriculum implementações e/ou monitorização de SGSI. O resultado da avaliação foi por unanimidade muito satisfatória na sua generalidade e possibilidade de utilização/adoção.

ABSTRACT

Information Security Management is an area where challenges have increased exponentially in recent years, due in large part to the amazing development in the Information Technology and Communications (ITC) areas. ITC have been at the forefront of the needs and solving process of management, logistical and operational problems in any organization and on any area of economic activity. This evolution allowed these different organizations, when adopting these new technologies, coping with new arriving problems that were not expected, on their information management.

Most of these organizations already understood that their information systems are not isolated islands and that they became part of a complex system with unimaginable information flow and that associated risks must be identified and treated with proper and consistent methods. It becomes even more delicate when these organizations are linked to health activity, dealing with personal information and with legal and ethical compliance obligation, having a significant weight in the handled and produced information management.

However, the main difficulty arises from the need of a, Information Security Management System (ISMS) implementation, and is required to take the first step to this decision support before the organization's managers. The ISMS implementation is still considered only for certification purposes. The available market offers and projects for implementation are expensive and the internal necessary resources may be immense, depending on the size of the organization and the required level of implementation.

This paper main objective is the creation of a simplified document model that allows management and implementation of ISMS (without certification purposes), in a fast and sustained way, especially in health care activity.

This model is supported by the methodology of ISO/IEC 27001 for ISMS, ISO/IEC 27002 and ISO/IEC 27799 for implementation of controls related to risk management. In the analysis / risk assessment component is supported by the methodology of ISO/IEC 27005. These standards use for the model creation include the proper consistency and provides the needed support in accordance with good practice and methodologies, duly recognized and tested worldwide. To support risk estimation, this model is based on the Simplified Method Quantitative Risk Assessment of Information Security (MARSI). With this combination of standards and the integration of this method of risk estimation, the presented solution becomes somewhat innovative and simplifies the process of implementation and managing an ISMS. On the functional level, it was developed using the Microsoft Excel software, for all operational aspects of the model, making it very flexible, adaptable and allowing new functionalities addiction. This model is especially directed to Health organizations nonetheless on most of its features it can be adapted to any other kind of organization.

For this model evaluation, it was issued a qualitative analysis from three experts (consulters or auditors in IT security area). These experts have ISMS implementations and/or monitoring on their curriculum.

The evaluation result was unanimously satisfactory and the possibility of its future use/adoption was recognized.

PREÂMBULO

Objetivo do MDPSIOS

Inovar > tornar mais ***simples***

Simplificar > tornar mais ***abrangente***

Abrangente > tornar mais ***flexível***

O objetivo de Gestão da Segurança da Informação neste Modelo Documental é promover:

- **Tranquilidade**
- **Continuidade**
- **Eficácia / Eficiência**
- **Produtividade**
- **Evolução**

Índice

Índice de Figuras

Acrónimo

BSI	- *British Standards Institute*
COBIT	- Control Objectives for Information and related Technology
IDC Portugal	- *International Data Corporation* Portugal
IEC	- *International Electrotechnical Commission*
ISF	- *Information Security Forum*
ISMS	- *Information System Management Security*
ISO	- *International Organization for Standardization*
ISRM	- *Information Security Risk Management*
ITIL	- *Information Technology Infrastructure Library*
MDPSIOS	- Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde
PDCA	- *Plan–Do–Check–Act*, é a metodologia proposta pela norma ISO/IEC 27001 para que um SGSI
PwC	- *Pricewaterhouse Coopers*
SOX(Sarbox)	- Lei *Sarbanes-Oxley* dos Estados Unidos
SGSI	- Sistema de Gestão da segurança da Informação
SI	- Sistema de Informação
TI	- Tecnologias da Informação
TIC	- Tecnologias da Informação e de Comunicações
UE27	- União europeia a 27

Capítulo 1 - INTRODUÇÃO

1.1 Enquadramento

Os requisitos de segurança da informação atualmente preconizados não faziam nem fazem parte da conceção de muitos dos sistemas de informação (SI) existentes nas organizações. Através da demonstração total da inexistência de uma cultura de segurança da informação no dia-a-dia, esta realidade está de tal forma presente nas organizações de saúde, que qualquer utente mais atento, facilmente se apercebe.

A informação gerada ou processada durante a prestação de cuidados de saúde são um conjunto de recursos sensíveis do ponto de vista da segurança, em que o valor de cada recurso e a sua suscetibilidade a uma quebra de segurança são na maior parte das vezes desconhecidos. No entanto sabe-se que, quanto maior for o valor do recurso, maior será o risco a ele associado [1].

1.2 Questionário sobre segurança

1.2.1 Realização do questionário

No inicio deste trabalho por a forma a perceber qual a amplitude do problema da segurança da informação nas organizações em Portugal, nomeadamente nas organizações de cuidados de saúde e no caso das implementações existentes que tiveram objetivos claros de mitigar o risco, procurar saber quais os padrões e medidas é que foram utilizados, foi realizado um questionário, para tentar determinar qual é atualmente o grau de implementação no mercado nacional dos Sistemas de Gestão da Segurança da Informação (SGSI).

Para a elaboração do questionário foi utilizada a plataforma *Web Google Docs* através da realização de 12 perguntas, sendo algumas de âmbito genérico e outras mais específicas sobre os SGSI, como se poder ver no anexo E.1, com uma abordagem que visa a obtenção do maior número de respostas, em que 5 minutos seria o tempo suficiente para responder de forma sucinta, bastando um *click* por pergunta. O *link* para preenchimento do questionário via internet, foi enviado por email (anexo E.2), para um universo de 727 organizações ou empresas, os nomes e respetivo *email* para onde foram enviados são apresentados no anexo E.3. O questionário realizou-se no espaço temporal de 2 meses,

entre 12.06.2012 e 12.08.2012. Os resultados do questionário estão descritos e analisados no ponto 1.2.2 e 1.2.3 deste capitulo.

1.2.2 Resultados

Foram enviados no total, 727 *emails* a solicitar o preenchimento eletrónico do questionário, dos quais foram entregues 608, não foram lidas (ou foram apagadas) 192, lidas mas sem resposta foram 390 e lidas com o questionário preenchido 26, o que representa 4% de respostas, relativamente ao total *emails* entregues. No anexo E.4, pode-se verificar com maior detalhe a estatística de envio do inquérito.

Pelo número de *emails* do inquérito, apagados à partida (192), adicionando os *emails* que foram lidos e sem resposta (390), o resultado, representa 96% do total entregue sem qualquer resposta ao assunto.

Uma das possíveis conclusões a extrair dos resultados do questionário é que, ainda é um grande problema senão mesmo tabu para muitas organizações, falar-se sobre segurança da informação no contexto da organização e de conhecimentos que os seus responsáveis têm sobre este assunto. Talvez por entenderem que não falando sobre o mesmo, não expõem as fragilidades ou soluções que têm, sendo uma estratégia defensiva, outros por não estarem ainda sensibilizados e desconhecerem o assunto, ou então poderá ser o reflexo da inexistência de uma cultura de segurança da informação nessas organizações.

No entanto relativamente às 26 respostas ao questionário, conseguiu-se 50% das respostas que eram expetável, sendo o assunto que é, e pelos motivos descritos no parágrafo anterior, no universo considerado pouco mais poderíamos esperar em termos de respostas. No anexo E.5, pode-se verificar com maior detalhe o resumo estatístico do questionário. Os resultados são interessantes e de destaque, conforme descrição que se segue:

. 100%, acha de grande relevância para a organização a segurança de informação;

. 54%, acha que a forma mais adequada de o fazer é através da implementação de um SGSI e 46%, acha que é através de medidas conjuntas, integradas e monitorizadas;

. 54%, conhece a norma ISO/IEC 27001 e 46%, não conhece;

. 54%, conhece a norma ISO/IEC 27002 e 46%, não conhece;

. 31%, conhece a norma ISO/IEC 27799 e 69%, não conhece;

. 65%, não tem implementado um SGSI; 31%, tem implementado um SGSI baseado na norma ISO/IEC 27001 e 4%, tem implementado um SGSI baseado noutro conceito;

. 38%, gostaria de implementar um SGSI baseado na norma ISO/IEC 27799; 15%, baseado na norma ISO/IEC 27002; 8%, baseado na norma ISO/IEC 27001; 4%, baseado noutro conceito; 8%, não gostaria de implementar um SGSI e 27%, não se aplica (nesta % estão incluídas as organizações que já têm um SGSI implementado);

. 46%, gostaria de implementar um SGSI para garantir a melhor solução para segurança da informação e certificação; 27%, para garantir a melhor solução para segurança da informação; 4%, para certificação e para 23%, não se aplica;

. 23%, está satisfeita com a solução que têm implementada; 58%, não está satisfeita; 4%, está satisfeita com outras soluções e para 15%, não se aplica;

. 27%, atribuem 3 na escala de 1 a 5 (1-Facil, …, 5-Dificil) na dificuldade de implementação de um SGSI; 38%, atribuem 4 e 35%, atribuem 5;

. 46%, são organizações da área de actividade de saúde (sector público); 19%, de saúde (sector privado); 8%, área de actividade do estado; 4%, indústria e 23%, de outras áreas de actividade;

. 4%, são organizações com menos de 21 trabalhadores; 8%, são organizações entre 21 e 50 trabalhadores; 4%, são organizações entre 51 e 100 trabalhadores; 19%, são organizações entre 101 e 250 trabalhadores; 4%, são organizações entre 251 e 500 trabalhadores e 62%, são organizações com mais de 500 trabalhadores.

1.2.3 Análise e discussão

Da análise dos resultados pode-se concluir que a segurança da informação, nos tempos atuais, têm grande relevância para qualquer organização em qualquer área de actividade, e na opinião da maioria dos inquiridos, esta deve ser assegurada por um SGSI, que gostariam de implementar com base nas normas da família ISO/IEC 27000, para garantir a melhor solução para segurança da informação e, na maioria dos casos também, com objetivo de certificação.

Em relação à implementação de um SGSI verifica-se que 65% não têm implementado e que dos 35% que têm um SGSI implementado, 58% não está satisfeita com a solução que tem. Relativamente á dificuldade de implementação de um SGSI, 73% classifica-a de difícil.

As organizações com a área de actividade mais representativa, 65% das respostas é a área de saúde (46% sector publico e 19% sector privado), onde 62% dessas organizações têm mais de 500 trabalhadores. Nos tempos que correm, este cenário vem de encontro ao despertar que se está a verificar nas organizações deste sector com maior dimensão relativamente ao número de trabalhadores do que nas de menor dimensão, no que diz respeito a necessidade e importância que a definição de políticas de segurança da informação começa a ter na gestão (administração, decisores, órgãos de gestão) e no seu dia-a-dia operacional.

Pela vasta diversidade de áreas de actividade, pela dinâmica interna na produção e tratamento da informação, pelos processos de intercâmbio de informação, pela dimensão, pela tecnologia utilizada, etc., em que as organizações estão inseridas, torna-se difícil de determinar um processo que seja genérico para criação de uma política de segurança. Logo, todo ou qualquer princípio ou metodologia genérica, terá de ser flexível de modo a permitir, a sua adaptação ou ajuste, à realidade de cada organização [1].

A solução pretendida e preconizada por qualquer organização para aquisição da estabilidade necessária relativamente a gestão da segurança da informação passa pela implementação de um Sistema de Gestão da Segurança da Informação (SGSI).
No entanto os requisitos, o custo, a complexidade, as exigências e conhecimentos que a implementação de um SGSI envolve, isto é, as dificuldades a ultrapassar fazem com que muitas das organizações, consciente ou inconscientemente, procurem conviver sistematicamente com o risco da falta de segurança ou com soluções pontuais que vão evitando danos maiores.

1.3 Objetivos

Este trabalho tem por objetivo principal propor um Modelo Documental para Políticas da Segurança da Informação em Organizações de Saúde (MDPSIOS), sem objetivos de certificação, transformando o processo de gestão da segurança da informação em algo com menor dificuldade, e de fácil implementação, que possa estar integrado no processo de gestão da organização. Este modelo documental deve cumprir com os requisitos de um Sistema de Gestão da Segurança da Informação (SGSI).
A realização deste objetivo passa por definir um modelo documental que permita a implementação de políticas de segurança da informação em qualquer organização de saúde, podendo estender-se a outras organizações.

Estando subjacente o fator dinâmico para um constante melhoramento e refinamento, através de um conjunto de processos de monitorização que poderão promover a redefinição de novos objetivos em cada um dos domínios e dimensões definidos, permitindo uma manutenção regular do sistema.

Problema (o que se pretende):

- Política de Segurança da Informação numa Organização de Saúde.

Solução (estudo de uma solução):

- Criação de Modelo Documental de Politicas de Segurança da Informação.
- Estruturar um Modelo Documental base (mínimo), cuja implementação seja ‘simples’, ‘abrangente’, ‘flexível’ e permita que uma organização fique num estado de segurança mínimo/médio. Este estado poderá ser a base de partida, para um possível processo de certificação à luz da Norma ISO 27001:2005, caso a organização tenha essa intenção como objetivo futuro.

Implementação (aplicar o modelo num caso prático, de estudo ou avaliação por peritos):

- Tentar aplicar o modelo numa organização de saúde (Hospital, Centro Saúde, Laboratório de Analises/Exames Clínicos, Farmácia, Laboratório Farmacêutico, empresa de Distribuição Farmacêutica, Centro/Grupo de Investigação, etc…). No caso de não ser possível, em alternativa, submeter o modelo documental a uma avaliação externa realizada por peritos da área da segurança da informação.

1.4 Organização da Tese

No capítulo 2 é apresentado um enquadramento relativamente a segurança de informação, nomeadamente a informação e o seu papel nas organizações, os sistemas de informação, uma descrição e análise da situação actual da segurança da informação e uma discussão a volta deste tema.

No capítulo 3 é abordado de forma a contextualizar os conceitos de informação, segurança, segurança da informação, política de segurança da informação, segurança da informação em organizações de saúde.

No capítulo 4 é feita uma abordagem aos conceitos dos principais itens que estão associados a gestão do risco, como risco, ameaça, vulnerabilidade e ataque. E feita também uma análise ao risco nos sistemas de informação de saúde. Neste capítulo aborda-se ainda os principais aspetos e características de cada uma das normas da família ISO/IEC 27000 associadas a segurança da informação, que serviram de suporte ao modelo documental proposto neste trabalho.

Sendo o modelo de gestão de risco uma das principais tarefas de suporte da estrutura de um SGSI, no capítulo 5 é feita a descrição geral do modelo proposto para a gestão de risco a utilizar pelo modelo documental que este trabalho propõe.

No capítulo 6 é feita a descrição conceptual e organizacional do modelo documental proposto, através da apresentação de um conjunto de funcionalidades e características relacionadas com o domínio ao qual o mesmo pertence.

No capítulo 7 é apresentada, a avaliação crítica e construtiva realizada por três peritos ou consultores experientes após a apresentação do modelo documental proposto, as principais conclusões e trabalhos futuros espectáveis.

Por fim, no capítulo 8, são apresentadas as referências bibliográficas.

Em anexo estão documentos de suporte aos vários assuntos abordados em alguns dos capítulos deste documento.

Capítulo 2 - ENQUADRAMENTO DA SEGURANÇA DA INFORMAÇÃO NOS SISTEMAS DE INFORMAÇÃO

2.1 Informação, a sua importância

A informação desempenha um papel importante tanto na definição, quanto na execução, de uma estratégia de uma organização. A informação auxilia os executivos a identificar as ameaças bem como as oportunidades para a organização e cria o cenário para uma resposta competitiva mais eficaz.

A informação funciona também como um recurso essencial para a definição de estratégias alternativas. A informação é essencial para a criação de uma organização flexível na qual existe uma constante aprendizagem [2].

Nas organizações, a informação é um dos ativos mais importantes, suportando todos os seus processos de negócio, com fins lucrativos ou não, devendo garantir permanentemente a continuidade do negócio, sem alteração de algumas das propriedades fundamentais da informação: confidencialidade, integridade, e disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. O seu valor por vezes é incalculável, pois está integrada com processos, pessoas e tecnologias.

Vivemos numa sociedade onde a informação é uma das suas bases de sustentação (sociedade da informação) e apresenta uma propensão para produzir e armazenar informações, em que a sua utilização efetiva e adequada permite que uma organização aumente a eficiência das suas operações [3].

A informação é reconhecida como um ativo crítico para a continuidade operacional e saúde da organização e representa a inteligência competitiva dos negócios [4].

A informação e o conhecimento são os diferenciais que permitem as empresas e profissionais destacarem-se no mercado e manter a competitividade [2].

Como qualquer ativo valioso, na sociedade da informação, a informação é o principal patrimônio de qualquer organização e está sob constante ameaça ou risco [5].

Nem toda informação é crucial ou essencial a ponto de merecer uma atenção e cuidados especiais. Mas existe sempre determinada informação crítica que pode ser tão vital que o

custo da sua integridade, qualquer que seja, será menor que o custo de não dispor dela adequadamente quando é precisa e sem qualquer alteração.

Podemos considerar que numa organização, a informação é um denominador comum sob o ponto de vista estratégico, tático e operacional entre processos, pessoas e tecnologia, conforme demonstra a figura 1.

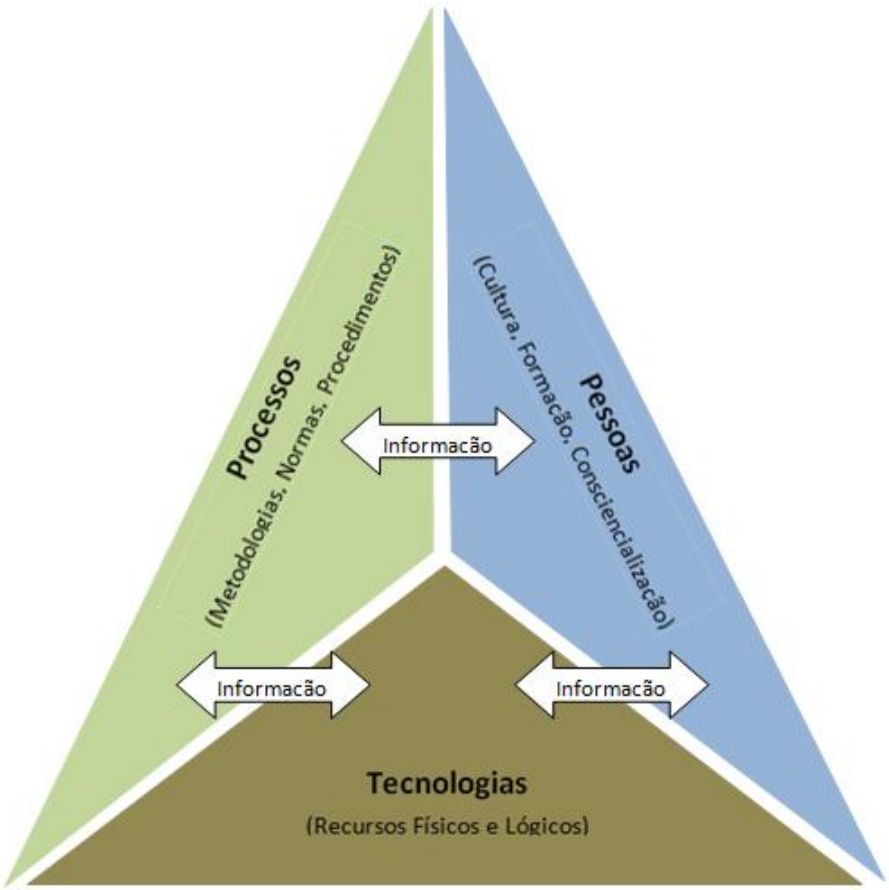


figura 1: - Informação, denominador comum [6][7].

Existe a necessidade de classificar a informação, para que seja possível assegurar ou atribuir um nível adequado de proteção [8]:

- A informação deve ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade para a organização.

- Um conjunto apropriado de procedimentos para identificar e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização.

Existem sistemas de classificação da informação, os mais comuns são os seguintes:

a) Baseada em níveis de confidencialidade para a organização, sendo identificadas como [9][10]:

- Pública

  - Informação que pode ser disponibilizada ao público em geral, sem que haja consequências de maior em termos de danos, no funcionamento da organização e em que a sua integridade não é vital para a mesma.

- Interna

  - Deve-se evitar o acesso público a este tipo de informação, embora as consequências da sua utilização não autorizada, não provoquem grande impacto ou sejam muito sérias. A sua integridade é importante, mesmo que não seja vital.

- Confidencial

  - Esta informação é restrita aos limites da organização, a sua divulgação ou perda pode levar a um desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, pode também permitir vantagem expressiva ao concorrente.

- Secreta

  - Informação crítica para as atividades da organização, cuja integridade deve ser preservada a qualquer custo e que o acesso a mesma, deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a organização.

b) Baseada em níveis de integridade para a organização, sendo identificadas como [10]:

- Básica

- Informação cuja perda de integridade a partir de um determinado prazo não implica ou não têm qualquer impacto para à organização, e, portanto não exigem controlos de auditoria e de acesso.

- Relevante

  - Informação cuja perda da integridade pode provocar transtornos de baixo impacto para a organização. Devem ser adotados controlos de forma habitual para garantia da integridade como a manutenção de uma cópia ou original de segurança, controle e registro dos acessos, etc.

- Vital

  - Informação que necessita de uma proteção especial no que diz respeito à sua integridade, pois a organização deve ter a capacidade de garantir que a mesma se preservou ou preserva no seu estado original ao longo do seu tempo de vida caso tal não aconteça pode criar grande impacto e comprometer em grande escala os objetivos ou a organização.

Ter informação correta, em qualquer momento, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos sistemas, tratamento de dados e armazenamento, a informação adquiriu mobilidade, 'inteligência' e uma grande capacidade de influenciar a gestão das organizações e mesmo a vida privada das pessoas.

"A vantagem competitiva … depende do acesso superior à informação" [11].

A informação como substrato da inteligência competitiva deve ser, devidamente administrada nos seus particulares, diferenciada, guardada e protegida.

2.2 Sistema de Informação (SI)

Sistema de informação é um sistema em que o elemento principal é a informação. Tem como objetivo armazenar, tratar e disponibilizar informação que permite apoiar ou mesmo executar funções ou processos numa organização. Um SI é composto por um subsistema social e por um subsistema automatizado [12], exemplificado na figura 2:

- O subsistema social: inclui pessoas, processos, informações e documentos.
- O subsistema automatizado: é composto por meios automatizados suportados por diferentes equipamentos (servidores, computadores, redes de comunicação, periféricos, etc.) que interligam os elementos do subsistema social.

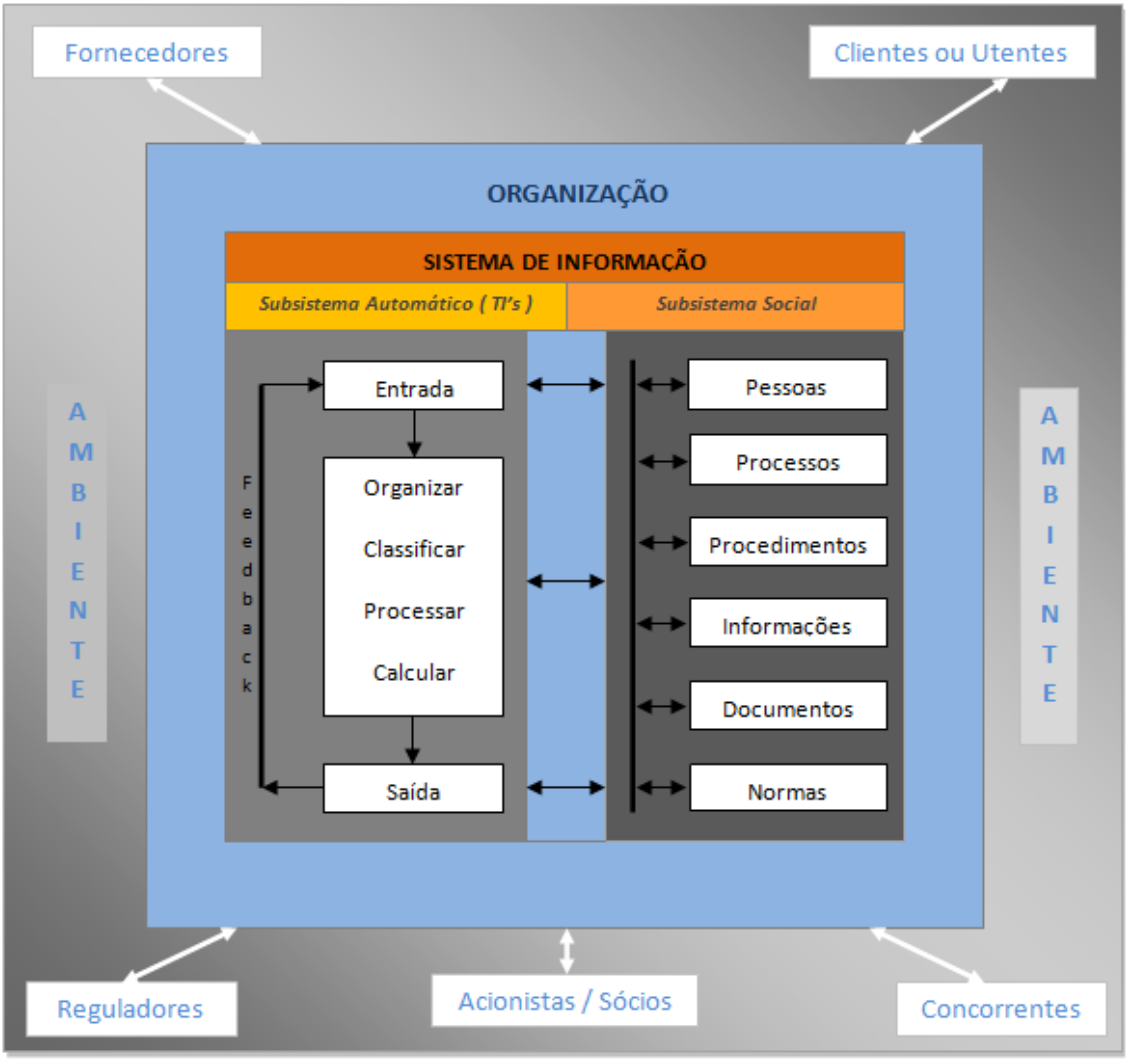


figura 2: - Sistema de Informação (SI) [7][12].

Ao contrário do que se pode imaginar ou pensar, as pessoas (em conjunto com os processos que executam e as informações e documentos que manipulam) também fazem parte do SI.

O SI é um sistema que está para além de qualquer *software* não só inclui o *hardware* e o *software*, mas também inclui os processos (e seus agentes) que são executados fora dos equipamentos. Com base neste conceito, as pessoas que não utilizam equipamentos (computadores) também fazem parte do SI e consequentemente têm de ser acompanhadas, observadas ou mesmo guiadas nos processos de planeamento e análise de um SI.

O perigo de não se dar importância, e/ou, a devida atenção ao subsistema social pode resultar no fracasso do SI em que o subsistema automatizado ou os sistemas automatizados (incluindo o *software*), poderão não ser eficazes ou mesmo não ser utilizados, apesar de funcionarem perfeitamente, pelo menos em ambientes de teste. Em ambiente real, isto é, estando o SI em produção, os aspetos sociais têm grande impacto e interferem em grande escala no seu funcionamento. Os processos contemplados no SI podem ser modificados em razão de aspetos sociais que não foram devidamente acautelados ou integrados. Por esta razão, alguns SI depois de implementados acabam por não ser utilizados ou sofrem grande resistência por parte dos utilizadores na sua implementação e acabam por provocar prejuízos ou dificuldades no normal funcionamento das organizações [12].

2.3 Situação actual

À medida que os sistemas de informação assumem um papel de maior preponderância, tanto ao nível dos processos como nos objetivos de negócio, a pertinência da sua segurança aumenta consideravelmente, despertando o interesse de todos os intervenientes nos processos decisórios, estratégicos e técnicos. Por outro lado, acontecimentos como o de 11 de Setembro de 2001 trouxeram para a ribalta a importância da existência de mecanismos que assegurem a sobrevivência das organizações face aos possíveis e diversos desastres [13].

Na sociedade atual cujo suporte de intercâmbio de informação entre organizações, instituições e mesmo com o comum dos cidadãos ou entre eles, está na maior parte dos casos assente sobre uma rede global a nível mundial, isto é, está suportada fundamentalmente na Internet. Esta exposição global apresenta novas ameaças dirigidas aos sistemas de informação organizacionais, independentemente do tipo de organização, da

dimensão, da natureza (pública ou privada) e dos recursos tecnológicos de informação e comunicação existentes.

É necessário, para a segurança da informação nas organizações, uma análise dos sistemas e atores que interagem com a organização, de forma a identificar atuais e futuras ameaças aos seus recursos e fluxos de informação. Esta análise permitirá apresentar uma visão macroscópica das ameaças existentes, que procuram explorar de forma contínua ou não, possíveis vulnerabilidades nos diversos sistemas de informação que suportam os vários níveis de gestão das organizações.

Entre as muitas tarefas diárias que a maioria das organizações executa, encontram-se as funções de processar, manipular, organizar, arquivar e proteger a informação recebida ou produzida. O crescimento anual da informação nas organizações ronda os 20%, mas existem situações em que esse valor aumenta de forma significativa, podendo chegar aos 50% ou mesmo duplicar de um ano para outro. Estes dados, da *International Data Corporation* (IDC) Portugal, servem para demonstrar a forte pressão a que uma grande parte das organizações está sujeita, tendo em conta a importância e o valor da informação para o negócio da empresa [14].

Neste sentido os decisores questionam-se em relação ao melhor lugar para guardar os dados, porque, apesar do armazenamento estar muito barato, obriga a mais despesas de manutenção, que se traduzem em mais custos para os departamentos de Tecnologias de Informação (TI). Além dos custos associados ao armazenamento e posterior criação de arquivos da informação, existem pressões relacionados com a pesquisa, com o acesso e com a prevenção da perda da informação. Todas estas situações podem ser cruzadas com a necessidade de aceder à informação dentro ou fora da organização através de dispositivos da empresa ou pessoais. Esta realidade acarreta um novo grau de complexidade aos departamentos de TI, que começam a ser confrontados com o imperativo de fazer mais com menos recursos.

Para além dos desafios enumerados, existe um outro que ganha cada vez mais espaço e importância nas grandes e médias organizações portuguesas e mundiais, que é a forma como a informação começa a circular. Com mais de 30 mil novas ameaças informáticas registadas por dia, as preocupações das empresas não aumentaram só com a segurança em geral, como tornaram-se mais específicas e conscientes de que os riscos vão para além do perímetro tradicional. A forma como a informação circula está a mudar, estando a ganhar cada vez mais dinamismo.

Como afirma A.F. Cristina [15], ”As infeções massivas passaram a história e os ataques são agora mais cirúrgicos e têm por objetivo o lucro económico. São silenciosos para durarem o

maior tempo possível. As ameaças saíram do espaço tradicional e ocupam zonas mais críticas nas empresas".

E, segundo P. Fernandes, *partner* da *Pricewaterhouse Coopers* (PwC) de *Forensic Services* em Portugal (anexo A.1), " O crime económico continua a ser generalizado, afetando tanto as grandes como as pequenas organizações, em todo mundo. Nenhuma empresa ou indústria é imune ao impacto causado pela fraude. Num mundo onde a maioria das empresas depende da tecnologia, há uma cada vez maior exposição ao risco de actividade criminosa, através de qualquer lugar do planeta desde que haja um computador, um *smartphone* ou qualquer outro dispositivo com acesso a internet. O aumento do número de incidentes de perda e roubo de dados, vírus, *hackers* e outras formas de crime económico demonstra a necessidade de uma abordagem mais proactiva na prevenção de fraudes."

Nesta linha de pensamento Antonio F. Sousa (anexo A.2) afirma que, " O crime económico não abranda. Pelo contrário. E até desenvolveu um novo campo de interesses: o cibercrime[1] ".

No relatório da PwC este descreve que (anexo A.1), " O Cibercrime é classificado como um dos quatro crimes económicos mais frequentes. A perceção do cibercrime como uma ameaça predominantemente externa está a mudar, estando agora as organizações a reconhecer que o risco do cibercrime pode também surgir dentro da organização. Os inquiridos referem que o departamento de tecnologias da informação é a fonte mais provável de cibercrime. O departamento de TI foi assim citado por 53% dos inquiridos, seguido pelas operações (39%), Vendas e Marketing (34%) e departamento Financeiro (32%). E que, apesar da maioria do inquiridos referir uma maior sensibilidade para a ameaça de cibercrime, a maioria deles refere que não tem, nem planeia ter, um plano de combate ao cibercrime nas suas organizações. Alem disso, 60% dos inquiridos referem que a sua organização não monitoriza as redes sociais. …".

A confirmar a evolução do cibercrime, no anexo A.3, a PwC na sua edição de Novembro de 2011 da '*Global Economic Crime Survey*' (GECS, resultante de entrevistas a 3.877 responsáveis por organizações de 78 países diferentes) revela que um dado novo deve ser devidamente ponderado pelas organizações: " a cibercriminalidade chegou ao topo da lista dos crimes económicos mais difundidos e praticados a nível global. De facto, e pela primeira vez, o cibercrime (palavra que a dez anos nem sequer fazia parte do léxico do 'economês') surge na quarta posição do GECS, logo a seguir à apropriação indevida de ativos, fraude contabilística e suborno e corrupção ".

[1] Cibercrime: prática que consiste em fraudar a segurança de computadores ou redes empresariais [76][77].

No anexo A.3 pode-se verificar qual é o alinhamento de Portugal relativamente ao resto do mundo em relação a este assunto, quando no ano 2011 é com grande espanto e de forma razoavelmente impotente, que assiste à exemplificação no terreno do que quer dizer cibercrime, ao ver algumas das suas organizações como, o Departamento Central de Acção e Investigação Penal, PSP, SIS, Portal das Finanças, Hospital da Cruz Vermelha, PS, PSD, CDS e Direção Geral do Ensino Superior - DGES (como se pode ler no anexo B.1), a terem os seus '*sites*' devassados por alguém que provavelmente ninguém irá conhecer ou ouvir falar. Nessa altura verificou-se que o orçamento nacional para combate ao crime informático era ridículo, por ser tão baixo. No entanto, apesar de realidades diferentes mas, para resolver o mesmo problema, nos Estados Unidos, o combate ao cibercrime tem a maior dotação financeira logo a seguir ao terrorismo.

O impacto que o cibercrime está a ter a nível da Europa (anexo A.2) levou, segundo a *Computerworld* na sua publicação *online* de 28.Março.2012 (anexo A.4) a informar que, a Comissão Europeia está a propor uma nova força de combate ao cibercrime integrada na Europol que deverá chamar-se Centro Europeu de Cibercrime, focada no desmantelamento de redes de cibercrime e estará sedeada em Haia, na Holanda. A nova estrutura deverá custar cerca de 3,6 milhões de euros no primeiro ano, cujo objetivo será endurecer as suas ações contra a cibercriminalidade.

Segundo o documento da Comissão Europeia, COM(2012) 140 final de 28.03.3012, "Luta contra a Criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade", os custos globais da cibercriminalidade para as nossas sociedades são consideráveis. Um relatório recente de 2011 revelou que as vítimas do cibercrime perdem anualmente cerca de 388 mil milhões de dólares em todo o mundo, o que torna este tipo de crime mais rentável que o conjunto do tráfico mundial de marijuana, cocaína e heroína [16].

Como tudo indica, o cibercrime tem tendência para crescer e reforçado pelos dados estatísticos que se seguem, podemos concluir que existe um longo caminho a percorrer no sentido da implementação dos Sistema de Gestão da Segurança da Informação (SGSI) nas empresas, tanto a nível nacional como mundial.

Já em 2004 a SGS[2] Portugal publicava na sua distribuição gratuita o seguinte parágrafo [17]: "No seu livro *Business@The Speed of Though*, Bill Gates afirma que o modo como uma empresa reúne, administra e usa a informação determina o seu sucesso ou insucesso. A segurança da informação tem vindo a assumir, assim, um maior protagonismo nas organizações. Num estudo recente, conduzido pelas consultoras *KPMG* e *Ernst & Young*, perto de 90% das organizações afirmam que a segurança da informação é de elevada

[2] SGS Portugal - Sociedade Geral de Superintendência, S.A.

importância para o alcance dos objetivos da empresa e 78% veem a redução de riscos como a força motriz do investimento em segurança da informação.”

No final de 2004, mais de mil empresas, um pouco por todo o mundo (figura 3), tinham já implementado e certificado o seu SGSI de acordo com o referencial BS 7799 - Parte 2.

Número de Certificados emitidos — BS 7799 - Parte 2 (Ano 2004)

Japão	510	China	11	México	3	Líbano	1
Reino Unido	185	Hungria	11	Arábia Saudita	3	Luxemburgo	1
Índia	81	Irlanda	11	Espanha	3	Macau	1
Taiwan	45	Singapura	11	Argentina	2	Macedónia	1
Alemanha	36	Noruega	9	Bélgica	2	Marrocos	1
Coreia	31	Áustria	5	Dinamarca	2	Qatar	1
Itália	23	Suécia	5	Isle of Man	2	Eslováquia	1
Holanda	18	Suíça	5	Malásia	2	Eslovénia	1
Hong Kong	17	Islândia	4	UAE	2	África do Sul	1
EUA	15	Polónia	4	Colómbia	1		
Finlândia	12	Brasil	3	República Checa	1	Total Relativo	1104
Austrália	11	Grécia	3	Egipto	1	Total Absoluto	1095

Fonte: ISMS User Group

figura 3: - Número de certificações BS 7799 (2004) [17].

Também em Portugal as organizações começam a ganhar consciência da importância da segurança das suas informações críticas. Ainda que em 2004 no mercado nacional não existisse nenhuma empresa certificada de acordo com a norma BS 7799, o referencial não é desconhecido e muitas já implementaram as boas práticas instituídas pelo mesmo. “É preciso ter em linha de conta que a certificação surge após a adoção das boas práticas, ou seja, depois de se ter assegurado uma gestão efetiva da segurança da informação na organização” [17]. Com base neste pressuposto relativamente a situação actual, pode-se colocar a seguinte questão:

- Quantas organizações estão certificadas a nível mundial e nacional com a norma ISO/IEC 27001?

De acordo com o *International Register of ISMS Certificates* (versão 213, Abril 2012) figura 4, o total de certificações existentes em todo o mundo era de 7.840, e Portugal surge com 10 certificações.

Register Search (Version 213 April 2012) click on a letter to see the certificates

Click on ISMS Certificates to go to certificate database search facility to search for certificates by Organisation, Name or by Country.

ISMS Scopes

If you want to look at the ISMS scope of registration for the certificates listed below you can see the scopes using the Register Search (either for specific certificates or an overview of all).

Number of Certificates Per Country

Japan	4061	Netherlands	22	South Africa	4
UK	549	Slovenia	21	Belgium	3
India	545	Bulgaria	18	Gibraltar	3
China	504	Iran	18	Macau	3
Taiwan	459	Philippines	16	Albania	2
Germany	209	Argentina	14	Bosnia Herzegovina	2
Czech Republic	111	Pakistan	14	Cyprus	2
Korea	106	Russian Federation	14	Ecuador	2
USA	104	Saudi Arabia	14	Jersey	2
Italy	86	Vietnam	14	Kazakhstan	2
Spain	77	Iceland	13	Luxembourg	2
Hungary	70	Indonesia	13	Macedonia	2
Poland	62	Colombia	12	Malta	2
Malaysia	58	Kuwait	11	Ukraine	2
Thailand	55	Canada	10	Mauritius	2
Ireland	50	Norway	10	Armenia	1
Austria	44	Portugal	10	Bangladesh	1
Romania	35	Sweden	10	Bolivia	1
Greece	32	Switzerland	9	Belarus	1
Hong Kong	32	Bahrain	8	Denmark	1
Australia	29	Chile	5	Kyrgyzstan	1
Singapore	29	Egypt	5	Lebanon	1
Turkey	29	Oman	5	Moldova	1
Mexico	28	Peru	5	New Zealand	1
Croatia	27	Qatar	5	Sudan	1
Slovakia	27	Sri Lanka	5	Uruguay	1
France	26	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4		
UAE	20	Lithuania	4	Total	7840

figura 4: - Estatística de certificações (ISMS *Certificates*, Abril 2012) [18].

No entanto na (versão 215, Agosto 2012) figura 5, o total de certificações existentes em todo o mundo passou para 7.940, e Portugal surge com 18 certificações.

Register Search (Version 215 August 2012) click on a letter to see the certificates

Click on ISMS Certificates to go to certificate database search facility to search for certificates by Organisation, Name or by Country.

ISMS Scopes

If you want to look at the ISMS scope of registration for the certificates listed below you can see the scopes using the Register Search (either for specific certificates or an overview of all).

Number of Certificates Per Country

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

figura 5: - Estatística de certificações (ISMS *Certificates*, Agosto 2012) [19].

Ao comparar os dados de Abril de 2012 e Agosto de 2013, verificamos que houve um incremento de 100 certificações, o que demonstra que nos últimos tempos se tem verificado uma real preocupação relativamente a questão da segurança da informação por parte das organizações.

Com base nos dados da figura 5, podemos verificar que o universo de países em que existe certificação com a norma ISO/IEC 27001 é de 85 países. Em que se evidenciam os seguintes países no top 10: - Japão (4.152), Reino Unido (573), India (546), Taiwn (461), China (393), Alemanha (228), Republica Checa (112), Korea (107), USA (105) Itália (82).

O Japão tem mais de metade das certificações de todo o mundo, esta situação pode estar associada a uma estratégia de mercado, e/ou disciplina legislativa, e/ou a cultura organizacional Japonesa. No entanto a India e a China são grandes produtores de equipamentos de segurança e desenvolvimento de *software*, tendo como clientes empresas ocidentais, e estas necessitam de garantias sobre os procedimentos utilizados. Provavelmente pelo facto da dimensão populacional destes países o número de certificações é baixo, espera-se um crescimento nos próximos anos.

Nos Estados Unidos da América (USA) a norma 27001 aparenta não ter sido bem aceite. Este facto prende-se pelas organizações optarem pelo COBIT[3] e ITIL[4] que se adequa melhor ao *Sarbanes-Oxley*[5] (SOX) [20], e pela alternativa gratuita *National Institute of Standards and Technology Special Publication* 800-*series* (NIST SP 800-*series*).

Nestes registos Portugal aparece na figura 4, a meio da tabela em 49º lugar com 10 certificações e na figura 5, em 34º lugar com 18 certificações, tendo no espaço de 3 meses incrementado 8 novas certificações. Este número tenderá a crescer até ao final do corrente ano.

[3] COBIT: - *Control Objectives for Information and related Technology*, é um guia de boas práticas apresentado como *framework*, dirigido para a gestão de tecnologia de informação (TI). Possui uma série de recursos que podem servir como um modelo de referência para gestão da TI [78].

[4] ITIL: - *Information Technology Infrastructure Library* é um conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação (TI). A ITIL busca promover a gestão com foco no cliente e na qualidade dos serviços de TI [79].

[5] Sarbanes-Oxley: - é uma lei, assinada em 30 de julho de 2002 pelo senador *Paul Sarbanes* e pelo deputado *Michael Oxley*. Motivada por escândalos financeiros corporativos, esta lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da gestão adequada das empresas. A lei *Sarbanes-Oxley*, apelidada de *Sarbox* ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas [80].

Em relação a Portugal, em Agosto de 2012 as empresas certificadas são as descritas na figura 6:

Certificate Register

Certificate Search page

International ISMS Register

Results of Your Certificate Query: (click here to go back to the Search Page)

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
ARENA MEDIA	Portugal	83889CC2-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
Caixa Económica de Cabo Verde	Portugal		Bureau Veritas Certification	ISO/IEC 27001:2005
Departamento de Jogos da Santa Casa da Misericordia de Lisboa (DJSCML)	Portugal	IS 524281		ISO/IEC 27001:2005
ENAME S.A.	Portugal	GB11/82769	SGS United Kingdom Ltd	ISO/IEC 27001:2005
HAVAS SPORT & ENTERTAINMENT	Portugal	83889CC6-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
INSTITUTO DE INFORMÁTICA, I.P.	Portugal	3896769	Bureau Veritas Certification	ISO/IEC 27001:2005
INTEGRITY S.A.	Portugal	GB12/85456	SGS United Kingdom Ltd	ISO/IEC 27001:2005
LATTITUDE	Portugal	83889CC3-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
Maksen Consulting, S.A.	Portugal	PT001307	Bureau Veritas Certification	ISO/IEC 27001:2005
MEDIA CONTACTS	Portugal	83889CC9-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
MOBEXT	Portugal	83889CC10-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
MPG	Portugal	83889CC13-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
ONE TO ONE	Portugal	83889CC8-2010-AIS-IBE-UKAS	DNV	ISO/IEC 27001:2005
Ponto.C - Desenvolvimento de Sistemas de Informação, Lda.	Portugal	GB11/83230	SGS United Kingdom Ltd	ISO/IEC 27001:2005
Portugalmail SA	Portugal	12/86073	SGS United Kingdom Ltd	ISO/IEC 27001:2005
TV Cabo Portugal	Portugal	202194	Bureau Veritas Certification	ISO/IEC 27001:2005
VORTAL-COMÉRCIO ELECTRÓNICO CONSULTADORIA E MULTIMEDIA SA	Portugal	IS 515264		ISO/IEC 27001:2005
ZON TV CABO PORTUGAL, SA	Portugal	202194	Bureau Veritas Certification	ISO/IEC 27001:2005

figura 6: - Portugal, Empresas certificações (ISMS *Certificates*, Agosto 2012) [19].

É importante realçar também, que o panorama da segurança da informação na União Europeia (EU) figura 7, mostra que a percentagem de grandes empresas com uma política de segurança da informação formalmente definida com um plano de revisão periódica é três vezes superior, a percentagem de pequenas empresas.

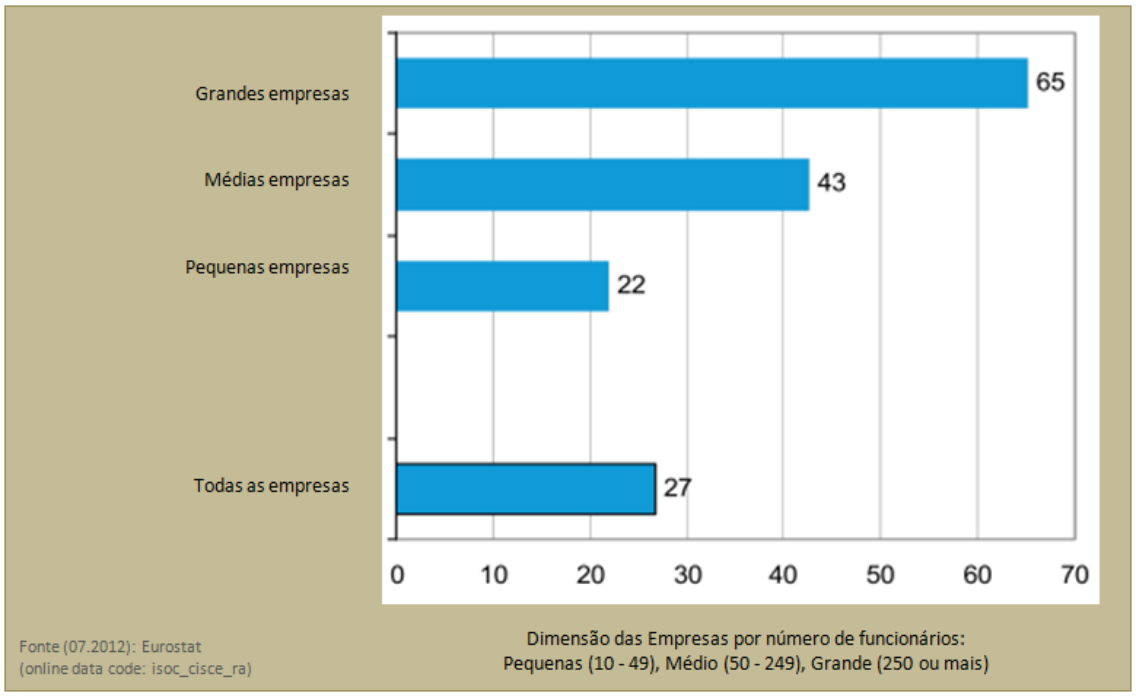


figura 7: - União europeia a 27 (UE27), empresas por dimensão (numero de funcionários), com uma política de segurança da informação formalmente definida com um plano de revisão periódica, janeiro de 2010 (% de empresas) [21].

A maior proporção de empresas com política formalmente definidas (52%) na UE-27 está associada ao sector das empresas de Informação e Comunicação, figura 8. As proporções mais baixas – inferiores a um quarto (¼) das empresas - foram registradas nos setores de Transporte e Armazenamento, Construção, Serviços de Alojamento e Restauração.

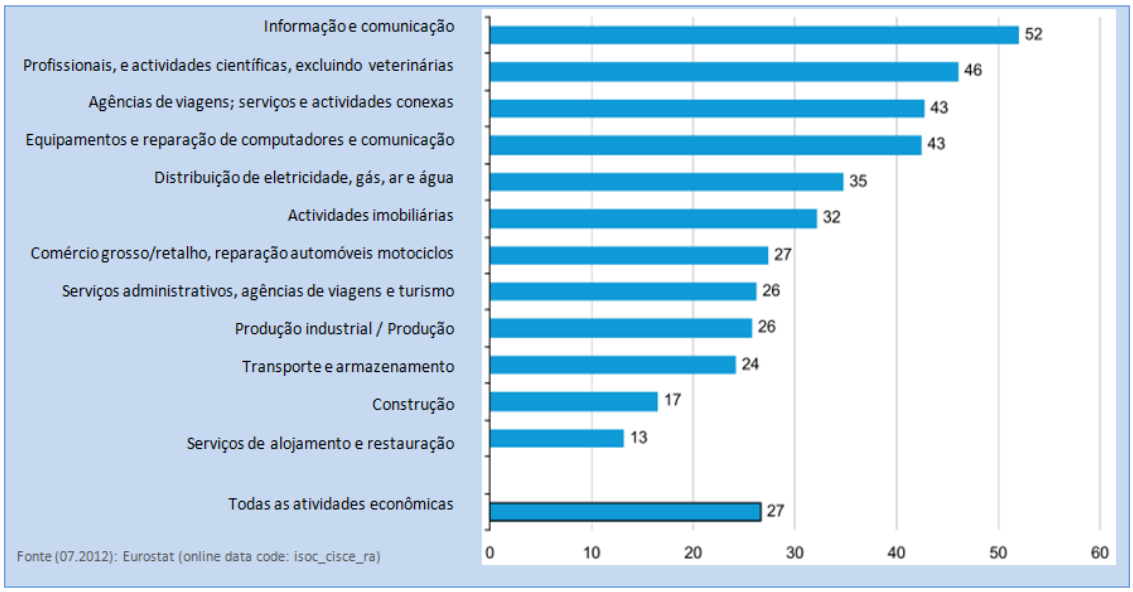
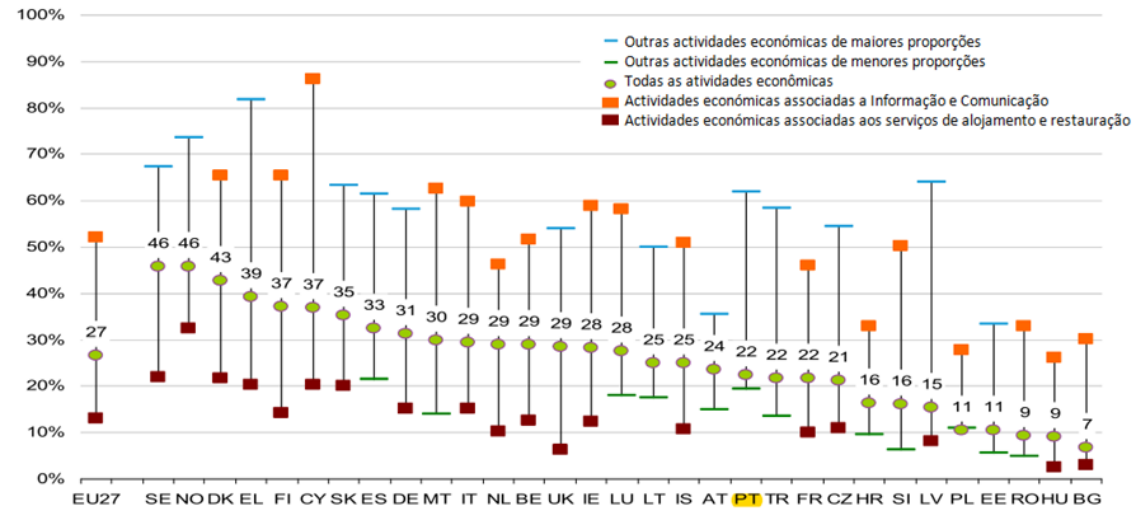


figura 8: - União europeia a 27 (UE27), empresas por atividade econômica, com uma política de segurança da informação formalmente definida com um plano de revisão periódica, janeiro de 2010 (% de empresas) [21].

A mais alta percentagem de empresas com uma política de segurança da informação formalmente definida com um plano de revisão periódica, foram registradas na Suécia e Noruega (ambas com 46%) seguido da Dinamarca (com 43%), figura 9.



Source: Eurostat (online data code: isoc_cisce_ra)

figura 9: - União europeia a 27 (UE27), Empresas por país e por atividade econômica, com uma política de segurança da informação formalmente definida com um plano de revisão periódica, janeiro de 2010 (% de empresas) [21].

Na figura 9, em mais de metade dos países, o sector da informação e comunicação tem a maior percentagem de empresas com uma política de segurança da informação formalmente definida com um plano de revisão periódica. A menor percentagem verifica-se no sector de actividade de serviços de Alojamento e Restauração na maior parte dos países. Menos de 10% das empresas na Roménia, Hungria e Bulgária relataram que tinham uma política de segurança da informação formalmente definida.

2.4 Discussão

Longe vai o tempo em que a grande preocupação das organizações era proteger a infraestrutura e o bom funcionamento. Com o aumento da complexidade, a preocupação/prioridade passou a ser salvaguardar a informação quanto à sua integridade, confidencialidade e disponibilidade no entanto o resto continua a ser importante, mas não é tudo.

Atualmente, a segurança da informação está a tornar-se numa das prioridades mais relevantes das organizações, passou a ser considerado um problema do negócio que requer uma gestão adequada, um requisito essencial para competir numa economia globalizada e para atingir resultados sustentáveis a médio e longo prazo.

A crescente utilização das tecnologias de informação e comunicações (TIC) como um meio de viabilização de processos de negócio cria vantagens competitivas, expandindo e ultrapassando continuamente e sistematicamente, as fronteiras da segurança. E desta forma começam a surgir crescentes vulnerabilidades dos sistemas e tecnologias introduzidas no suporte aos negócios e assim expondo-se a um crescente conjunto de ameaças com elevado grau de sofisticação que por sua vez coloca as organizações perante novos riscos diariamente.

Neste cenário, o conceito e a abordagem tradicional de gestão da segurança, com base ou focada apenas na utilização de ferramentas tecnológicas, torna-se inadequada e ineficaz. A segurança terá de se situar num contexto organizacional e operacional mais amplo e, portanto, não pode ser gerida com uma abordagem de tarefa estanque. É necessário uma abordagem de gestão global (holística[6]), efetiva e proactiva, tendo em conta processos, pessoas e ferramentas com o objetivo de identificar, quantificar e minimizar os riscos associados ao negócio.

As organizações terão cada vez mais de ter em conta a implementação de políticas de segurança da informação como um garante para a sua sobrevivência nesta sociedade de informação, cada vez mais globalizada e interligada, cada vez mais sofisticada tanto em tecnologias de informação, comunicações e outros, como em vulnerabilidades e ameaças, sob pena de terem a sua informação (o ativo precioso do seculo XXI) exposto a riscos diários.

Tem sido uma tendência natural, quando se fala em segurança da informação, associar esta necessidade ou requisito a instituições financeiras ou organizações conotadas com segredos industriais ou estatais. Não deixa de ser verdade, no entanto, estes

[6] Holística: - significa totalidade, considerar o todo tendo em conta as partes e suas inter-relações.

acontecimentos nos dias que correm podem também ocorrer em empresas de outros sectores.

Recuando ligeiramente no tempo (figura 10), pode-se afirmar que a informação mais delicada, sensível, crítica de uma organização poderia ficar guardada perfeitamente numa gaveta de alguma mesa, arquivo, cofre ou pasta de um gestor ou responsável.

figura 10: - Exemplo de mecanismos de segurança de informação obsoletos.

Atualmente (figura 11), tendo em conta a fase ou etapa tecnológica da organização, a proteção da informação continua a ser um aspeto importante

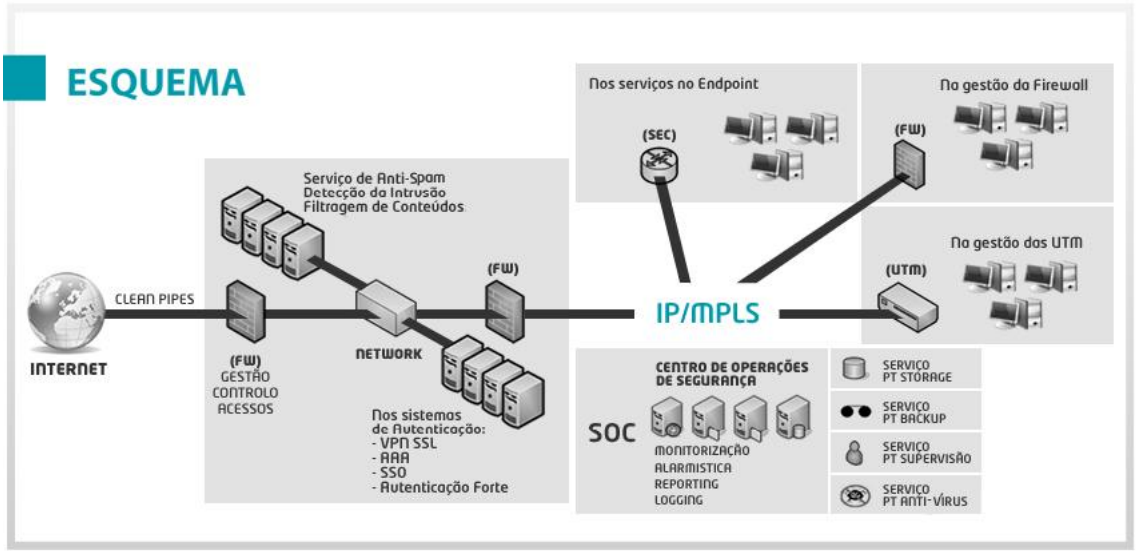


figura 11: - Esquema de serviços de segurança tecnológica da informação [22].

A segurança da informação é um processo que tem um início, mas sem fim previsto. Existe para permitir que os recursos da informação na organização possam estar presentes, acontecer e ou ocorrer, de forma sustentável e devidamente segura para organização.

Capítulo 3 - SEGURANÇA DA INFORMAÇÃO

No atual contexto em que vivemos, a problemática associada à segurança da informação é uma constante.

Os termos Informação e Segurança, são difíceis de definir, têm uma diversidade de significados que depende em grande parte do contexto em que estão inseridos, no âmbito deste trabalho é importante clarificar o conceito a que cada um dos termos esta intimamente ligado.

Genericamente a segurança da informação é o conjunto de mecanismos, ações que promovem a proteção sobre a informação de uma determinada organização ou pessoa [23][1][24].

3.1 Informação

Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe. Enquanto conceito, carrega uma diversidade de significados, do uso quotidiano ao técnico. Genericamente, o conceito de informação está intimamente ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, perceção e representação de conhecimento [25][26].

É comum nos dias de hoje falar-se sobre a Era da Informação, o advento da "Era do Conhecimento" ou Sociedade do Conhecimento. Como a Sociedade da Informação, a Tecnologia da Informação, a Ciência da Informação e a Ciência da Computação, a palavra "informação" é frequentemente utilizada sem muita consideração pelos vários significados que adquiriu ao longo do tempo.

Informação é um termo com muitos significados dependendo do contexto, mas como regra é relacionada de perto com conceitos tais como significado, conhecimento, instrução, comunicação, representação e estímulo mental. Simplificando, informação é uma mensagem recebida e entendida [25][26][27].

De forma resumida a informação, é todo e qualquer conteúdo ou dado que tenha valor para uma organização ou pessoa podendo estar protegida para uso restrito ou exposta ao público para consulta ou aquisição. Ou seja, acima de tudo, informação é o resultado do

processamento, manipulação e organização de dados numa forma que pode ser consumida por quem a recebe, permitindo a aquisição de conhecimento [26], e pode existir sob as seguintes formas:

a) Informação como mensagem: - quantidade arbitrária de informação cujo início e fim estão definidos. Qualquer pensamento ou ideia expressa de forma breve numa linguagem aberta ou secreta (código), preparada numa forma possível de transmissão por qualquer meio de comunicação [26].

b) Informação como padrão: - documento que estabelece uma engenharia uniforme ou especificações técnicas, critérios, métodos, processos, ou práticas. Algumas normas são obrigatórias, e outras podem ser voluntárias [28][29][30].

c) Informação como estímulo sensorial: - conhecimento inscrito ou gravado sob uma forma escrita, oral ou audiovisual. Esta informação comporta um elemento associado aos sentidos, com um significado transmitido a um ser consciente por meio de uma mensagem veiculada num meio que pode ser impresso, um sinal elétrico, uma onda sonora, etc. [31].

d) Informação como influência que leva a transformação: - é qualquer tipo de padrão que influência a formação ou transformação de outros padrões [31].

e) Informação como dados: - as palavras informação e dados são, intercambiáveis em muitos contextos. No entanto, não são sinônimos. De acordo com a observação de *Adam M. Gadomski* [32], “dados é tudo o que pode ser processado, e informação são dados que descrevem um domínio físico ou abstrato”, no entanto *Knuth* [33] aponta que “o termo dado refere-se a representação do valor ou quantidade medida ao passo que informação, quando usada num sentido técnico, é o significado do referido dado”

f) Informação como registos: - são uma forma especializada de informação. Essencialmente, registos são informações produzidas como subprodutos de actividades comerciais ou transações, ou conscientemente como um registo de tais actividades ou transações e retidas ou guardados em virtude do seu valor. Em primeiro lugar o seu valor é uma evidência das atividades da organização, mas também podem ser conservados pelo seu valor informativo. A gestão de registos (*records management*) deve garantir que a sua integridade seja preservada enquanto forem necessários [34][35].

Quanto ao suporte a informação, esta pode ser materializada/armazenada em diferentes materiais e/ou formas:

a) Pedra;
b) Madeira;
c) Pele;
d) Pano;
e) Papel;
f) Fita Magnética;
g) Disquete,
h) Disco Magnético;
i) Disco Ótico;
j) CD;
k) DVD;
l) *Pen drive*;
m) etc.

É pacífico para nós, aceitar uma determinada sequência histórica na utilização dos diferentes suportes de informação, conforme descrição anterior, isto é, uma sequência natural assente em motivos perfeitamente identificáveis e onde a sucessão nunca é absoluta, como é o caso do papel.
O papel é um caso estranho e persistente. Até á pouco tempo, acreditava-se que com o aparecimento das TIC seria possível reduzir drasticamente a quantidade de papel utilizada na maior parte das organizações, em que os escritórios eletrónicos, cada vez mais sofisticados, permitiriam trocar informação em grandes quantidades e a grande velocidade, sem necessidade de papel e de um mensageiro.

Fatores como o peso, a transportabilidade, a fidelidade, a facilidade de gravação, o espaço ocupado, a durabilidade, a segurança contra acessos indevidos, a densidade, a rapidez de acesso e a atitude psicológica dos utilizadores de informática, assumem incontestavelmente um valor diferente para cada suporte. O conjunto das vantagens e desvantagens de cada um, acabam por pesar nas decisões da indústria e dos consumidores na escolha dos suportes a utilizar.

A informação pode estar em vários “estados”, no mesmo ou em diferentes momentos da sua existência, isto é, tempo de “vida” como por exemplo:

a) Estar em processo de criação, consulta, alteração, eliminação ou armazenamento.
b) Estar armazenada, partilhada ou em processo de transmissão.

Independentemente da forma em que é materializada, do tipo de suporte de armazenamento, do estado em que esteja ou possa assumir, sendo a informação no contexto actual um bem ou ativo valioso e precioso para a organização ou pessoa, deve estar sempre devidamente protegida, isto é, em segurança (figura 12).

figura 12: - Segurança da informação

3.2 Segurança

Segurança é a perceção que se tem de estar protegido de possíveis riscos, perigos ou perdas [36][37].

Como suporte à segurança, verifica-se em muitas situações, uma política a ela inerente ou aplicada de forma empírica, que pode estar subjacente a existência de duas filosofias: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido). Estes princípios estão sistematicamente presentes na segurança da informação praticada nas diversas organizações quando não existe um Sistema de Gestão da Segurança da Informação (SGSI).

A segurança pode subdividir-se em segurança Física e segurança Lógica:

a) A segurança física, que tem como objetivo proteger equipamentos (bens materiais) e informação (bem imaterial), prevenindo o acesso a esses recursos. Normalmente pode basear-se na definição de perímetros de imediações desses recursos, como áreas de acesso restrito. Pode ser abordada por duas subdivisões [38][39]:
    - Segurança de acesso: gere as medidas de proteção contra o acesso físico não autorizado;

- Segurança ambiental: gere a prevenção e medidas corretivas contra os danos que possam resultar de causas naturais.

b) A segurança lógica, que define um conjunto de medidas e procedimentos, que devem ser utilizados pela organização e/ou intrínsecos aos sistemas e aplicações utilizadas. Tendo como objetivo a proteção de dados e a proteção dos sistemas e das aplicações contra a tentativa de acesso não autorizado por utilizadores ou outras aplicações [38][39].

De uma forma geral a segurança, tem conceitos e princípios que se aplicam de certa forma e com profundida diferente, relativamente a situações ou contextos em que se insere o objetivo da segurança, dependendo do ativo ou bem que deve ser protegido. Estes conceitos definem a criação de sucessivas barreiras de modo a minimizar ou anular as vulnerabilidades que estão expostas a potenciais ameaças, aplicando se necessário alguns dos conceitos, princípios ou técnicas que se seguem, de modo a fortalecer o conjunto de medidas e procedimentos a utilizar, para garantir os objetivos da segurança [40]:

C1. *Sobreposição de medidas de segurança,*

- Não existe um sistema de segurança perfeito ou de proteção total.
- A existência de uma falha na segurança é algo que está sempre eminente (seja ele resultado de negligencia, falha tecnológica, habito, esquecimento, vicio ou circunstancial), podendo a mesma ser explorada por um possível invasor/agressor. Se existirem outras medidas de segurança ativas e sobrepostas à primeira, a possibilidade da ameaça se concretizar, isto é, o invasor ou agressor ter sucesso será muito menor ou reduzida.

C2. *Ameaças apontadas a um ativo, aumentam a necessidade de segurança,*

- A planificação de um mecanismo de segurança obriga a ter em conta o valor do ativo que deve ser protegido e como deve ser protegido. O custo da implementação da segurança pretendida deve estar devidamente dimensionado em relação ao valor do ativo a proteger. Um custo elevado de segurança para proteger um ativo de valor inferior não faz qualquer sentido.

C3. *A fraqueza de um sistema de segurança está associada ao seu ponto mais fraco:*

- Qualquer sistema de segurança tem sempre um ponto mais fraco, como a segurança tem de funcionar num todo, na sua implementação ou reanálise deve-se identificar de forma eficiente e dar a maior atenção a seleção das medidas a serem adotadas. Se necessário deve-se aplicar o 1º conceito ***(C1)*****.**

C4. *A intervenção da defesa deve ser imediata e deve-se retardar ao máximo a possibilidade de agressão:*

- No momento em que acontece uma invasão ou agressão, quando mais rápida for a intervenção, mais fácil será o seu controlo e redução do dano. A chave de sucesso da segurança implementada, reside por vezes na rapidez de reação defensiva a mesma.

C5. *O acesso a informação sigilosa deve estar associado, a função da pessoa:*

- Deve-se restringir ao máximo o número de pessoas que têm acesso a informações restritas. Só deve ter acesso a ela quem pelas suas funções deve ter conhecimento do seu conteúdo. Nestes casos é necessário saber quem têm acesso, quando teve e como teve.

C6. *A informação sigilosa não deve ser dada a pessoas vulneráveis:*

- As pessoas vulneráveis representam uma vulnerabilidade no sistema de segurança como um todo, tornando-o fraco através da presença deste ponto mais fraco (3º conceito – ***C3***). Deverão ser tomadas medidas adicionais de segurança em torno dessa pessoa para diminuir essa vulnerabilidade (1º conceito – **C1**). Cabe ressalvar que esse conceito deve permanecer sempre dentro dos limites da ética e da legalidade, como será visto mais adiante (13º conceito – **C13**).

C7. *Os riscos devem ser agrupados e os segredos devem ser divididos:*

- Agrupar os riscos permite ter uma segurança única.
- Porem quando é possível, aquilo que pretendemos proteger deve ser fracionado, sendo decomposto em partes que, por si só, não tenham significado, e cada parte deve ser protegida por diferentes medidas de segurança. Desta forma, se o invasor ou agressor tiver sucesso em ultrapassar sucessivas barreiras e conseguir chegar ao bem protegido, terá acesso somente à parte do segredo. Para conseguir ter acesso ao bem, por completo, terá de ultrapassar outra sequência de barreiras de segurança, o que diminui substancialmente as hipóteses de sucesso.

C8. *Os bens a proteger devem estar sob uma responsabilidade bem definida:*

- A melhor pessoa para proteger um bem, é o seu proprietário, dono ou responsável pelo bem.
- Quando não existe uma propriedade individual, mas sim coletiva, deve existir ou ser atribuída uma responsabilidade individual pelo bem claramente definida

perante a coletividade. Este conceito, associado ao 11º ***(C11)*** e 14º conceito (**C14**), é remetido a gestão dos recursos humanos (RH).

- As pessoas são mais responsáveis, quando lhes são atribuídas tarefas importantes e de confiança.

C9. *O que serve para proteger um segredo ou algo valioso, é secreto:*

- Qualquer segredo deixa de o ser, quando um potencial invasor ou agressor tem conhecimento da sua existência, o que faz com que normalmente seja atraído para a sua descoberta.
- Uma boa prática é manter em segredo aquilo que é valioso e tudo o que o protege, para que outros não saibam que existe algo que é protegido.
- Este conceito define que a primeira opção da segurança deve ser sempre, não fazê-la de forma ostensiva para que agressores não saibam que existe algo que está a ser protegido. Isto é, a primeira opção da segurança deve ser atuar na área da segurança da informação, que por natureza é não-ostensiva. Já a segurança física faz parte da segurança ostensiva e é sempre uma segunda opção e deve-se minimizar ao máximo a aparência agressiva das barreiras aplicadas. Exceções à regra são os casos em que pela própria natureza da atividade da organização ou pessoa, não existe qualquer forma de não dar a conhecer à existência de algo valioso ou a proteger.

C10. *Qualquer sistema de segurança deve ter no mínimo, um elemento/fator de surpresa para o invasor ou agressor:*

- Se o segredo defensivo estiver bem guardado, o invasor ou agressor será surpreendido por fatores desconhecidos e inesperados.
- As surpresas eficientes são aquelas que causam nervosismo, hesitação e perca de tempo por parte do invasor ou agressor, desistindo dos seus objetivos. Este conceito complementa o 4º conceito (**C4**).

C11. *As medidas de segurança não devem ter impacto nem dificultar o normal funcionamento da organização:*

- Não existe um sistema de segurança perfeito ou de proteção total (1º conceito – **C1**), no entanto é possível conseguir-se um elevado grau de proteção através da sobreposição de medidas de proteção. No entanto se estas medidas provocarem impacto ou entrave no trabalho realizado pelas pessoas, trará desconforto e problemas, levando-as a negligenciar a segurança, o que provocará prejuízos à organização. Este conceito é remetido a gestão dos recursos humanos (RH).

C12. *A segurança deve ser compreendida, aceite e aprovada por todos:*

- Ao contrário do que geralmente se pensa, a segurança não é um encargo que diz respeito somente aos especialistas, mas sim, de todos os elementos de uma organização.
- Para ser eficaz, deve ter em conta a cooperação de todos, é em função do empenho e discrição de cada um individualmente, porque interage com o seu trabalho diário.
- Este conceito define a importância do profissional de segurança em dominar técnicas de marketing e atuar agressivamente em endomarketing.

C13. *A defesa tem sempre associado um princípio legal e moral:*

- A proteção só se justifica se for implementada respeitando a liberdade e dignidade da pessoa humana.
- Não há segurança se ela não for moral e legal.
- Os prejuízos a médio/longo prazo resultantes de ações ilegais ou amorais suplantam em muito os ganhos a curto prazo que essas medidas podem trazer.
- Este conceito envolve todos os outros e remete também ao assunto da "Ética Profissional".

C14. *A segurança exige um entendimento harmonioso no interior da organização:*

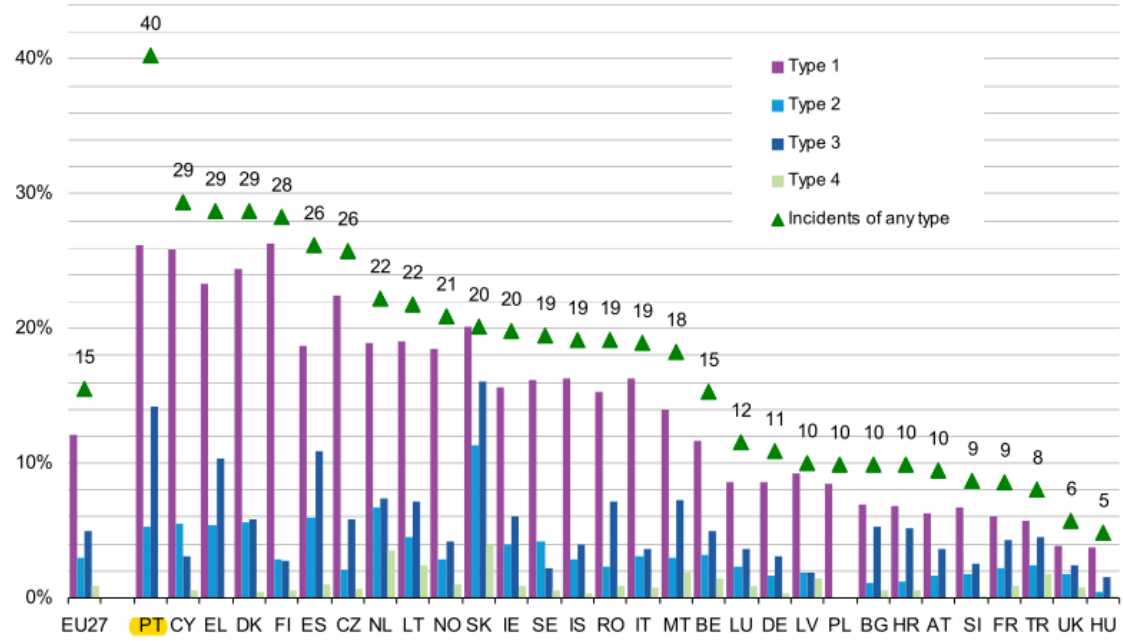
- As organizações com empregados descontentes são um alvo fácil para aliciamento por parte de invasores e agressores.
- Um empregado descontente constitui um potencial perigo para a segurança da organização, e o profissional de segurança deve estar atento a estas situações.
- Este conceito é remetido a gestão recursos humanos (RH).

Especificamente, a segurança da informação, que é a vertente da segurança sobre a qual este trabalho incide é, um dos temas mais frequentemente discutidos nos tempos que correm, e continua infelizmente a ser muitas vezes negligenciada. Alias o número de organizações que afirma ter perdido dados importantes devido a ameaças de segurança aumenta de ano para ano [41].

No entanto como mostra a figura 13, em 2009 (última estatística obtida da Eurostat) os incidentes mais relatados, pelas empresas, foram os que resultaram em falta de disponibilidade de serviços de TIC, destruição ou corrupção de dados devido a falhas de *hardware* ou de *software* (tipo 1), com quotas superiores a 20% registado em Chipre, Portugal e Finlândia (26% de empresas, respetivamente), Dinamarca (24%), Grécia (23%), República Checa (22%) e Eslováquia (20%).

A proporção mais elevada de empresas com incidentes que resultaram da destruição ou corrupção de dados devido a *software* malicioso, infeção ou acesso não autorizado (Tipo 3) foi registrado na Eslováquia (16%), Portugal (14%), Espanha (11%) e Grécia (10%).
A percentagem de empresas que relataram indisponibilidade de Serviços de TIC, devido a um ataque de fora/externo (tipo 2), o mais elevado foi na Eslováquia (11%) e Países Baixos (7%). Na maioria dos Estados-Membros da UE27, a divulgação de dados confidenciais, devido à intrusão, ataques de *pharming* ou *phishing* foi relatada por 1% ou menos das empresas em 2009.

Em conclusão podemos verificar que em 2009, em termos estatísticos relativamente a percentagem de incidentes de segurança ocorridos nos países da comunidade europeia (CE), Portugal destaca-se em 2º lugar em dois tipos de incidentes, nomeadamente do tipo 1 (Indisponibilidade de serviços de TIC, destruição ou corrupção de dados devido a falhas de hardware ou software) e tipo 3 (Destruição ou corrupção de dados devido a infeção, software malicioso ou acesso não autorizado). Estes dados permitem concluir que em diversos países da UE27 em particular Portugal, existe ainda um longo caminho a percorrer em matéria de segurança da informação.



Source: Eurostat (online data code: isoc_cisce_ic), EU27 without EE

figura 13: - Incidentes de segurança que afetam os sistemas de TIC das empresas, por países da Comunidade Europeia e tipo de incidente, 2009 (% de empresas) [21].

Legenda:

Type 1: - Indisponibilidade de serviços de TIC, destruição ou corrupção de dados devido a falhas de *hardware* ou *software*.

Type 2: - indisponibilidade de serviços de TIC, devido por exemplo à ataques de fora (externo) relacionados com negação de serviços.

Type 3: - Destruição ou corrupção de dados devido a infeção, *software* malicioso ou acesso não autorizado.

Type 4: - Divulgação de dados confidenciais devido a intrusão, *pharming*, ataques de *phishing*.

3.3 Segurança da Informação

A segurança da informação é para alguns autores a proteção dada aos sistemas de informação [5][9][42]:

a) Contra a intrusão;
b) Contra a modificação não-autorizada de dados ou informações armazenadas, em processamento ou em trânsito;
c) Contra a indisponibilidade de serviços aos utilizadores autorizados;
d) Para assegurar a segurança dos recursos humanos, da documentação, do material/equipamentos;
e) Para assegurar a segurança das áreas e instalações de comunicações e *data-center* (centro processamento);
f) E garantir a função permanente e sistemática de prevenir, detetar, deter e documentar eventuais ameaças ao desempenho e desenvolvimento dos sistemas de informação.

Segurança da informação é a base que pode dar às empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio [7]. É evidente que os negócios estão cada vez mais dependentes das novas tecnologias e das comunicações, e estes sistemas têm de assegurar e proporcionar a confidencialidade, integridade, disponibilidade e se necessário outras dimensões, propriedades ou princípios básicos que permitam garantir a segurança da informação [42][7][10].

Confidencialidade é a dimensão que permite garantir que a informação não seja revelada a uma pessoa, sistema, entidade ou órgão não autorizado ou credenciado. Do ponto de vista dos sistemas, é a proteção de sistemas de informação para impedir que pessoas, ou equipamentos, não autorizadas tenham acesso ao mesmo. Um dos pontos mais importantes desta dimensão é garantir a identificação e autenticação das partes envolvidas.

Integridade é a dimensão que permite garantir que a informação não seja modificada ou destruída, inclusive quanto à sua origem, a transmissão e ao destino. A informação deve ser retornada na sua forma original, isto é, idêntica ao momento em que foi armazenada. É a proteção de dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Disponibilidade é a dimensão que permite que a informação esteja acessível e utilizável quando é solicitada por uma pessoa, sistema, entidade ou órgão a qualquer momento. A informação ou sistema de informação deve estar disponível no momento em que a mesma é necessária.

É normal por vezes criar-se alguma confusão entre a dimensão, integridade e confiabilidade do conteúdo da informação (o seu significado). Uma informação pode ser imprecisa, ou não entendida, mas deve manter-se integra, isto é sem sofrer alterações por utilizadores não autorizados.

A segurança da informação tem também por objetivo, aumentar a produtividade dos utilizadores, implementando um ambiente mais organizado e dinâmico, promovendo um maior controlo sobre os sistemas de informação em particular os recursos de informação, e de permitir a utilização de aplicações com objetivo e/ou missão crítica [7].

A conjugação de medidas adequadas e devidamente apropriadas das dimensões confidencialidade, disponibilidade, integridade e outras se necessário, permite que se crie um ambiente e suporte estável, de modo a que as organizações possam alcançar os seus objetivos de forma confiável e segura através dos seus sistemas de informação.

Alguns autores defendem a integração de outras dimensões, tais como o Não Repúdio, Autenticidade, Auditoria, Legalidade, Privacidade para que a informação seja segura no sistema onde reside [5][4][43].

Não repúdio é a dimensão que não permite que seja negado (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação, nem o envio ou receção de uma informação ou dado.

Autenticidade é a dimensão que garante que a informação ou o utilizador da mesma é autêntico. Permite confirmar com exatidão, a origem do dado ou informação.

Auditoria é a dimensão que permite a rastreabilidade dos diversos passos que um processo ou ação esteve sujeito, passou ou a que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em *software* significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria, consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

Legalidade é a dimensão que garante a legalidade (jurídica) da informação. Adesão de um sistema à legislação. Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais definidas ou com a legislação política institucional, nacional e ou internacional vigente.

Privacidade é a dimensão que foge do aspeto de confidencialidade, pois a informação pode ser considerada confidencial, mas não privada. A informação privada somente é vista, lida e alterada pelo seu proprietário/dono. Esta dimensão garante ainda, que a informação não é

disponibilizada a outras pessoas (neste caso é atribuído o caráter de confidencialidade a informação). Pode-se considerar que é a característica que permite que um utilizador realize ações num sistema sem que seja identificado.

Para a ISO/IEC 27002 a definição de segurança da informação é a [23], "preservação da confidencialidade, integridade e disponibilidade da informação (para além de outras dimensões, tais como: autenticidade, responsabilidade/autoria, não repúdio e confiabilidade que também podem estar envolvidas) através da implementação de um conjunto de controlos[7] ajustados, que podem ser políticas, práticas, procedimentos ou até mesmo funções de *software*".

A forma de tratamento das actividades associadas ou direcionadas à segurança da informação devem ser assumidas em pleno como actividades de gestão, independentemente da sua realização através da implementação de um conjunto de controlos, como políticas, práticas, procedimentos, mudança nas estruturas organizacionais com a ajuda de funções de *software* e *hardware* [24].

A norma ISO/IEC 27001 (capitulo 4) define o conceito do Sistema de Gestão da Segurança da Informação (SGSI), que consiste num instrumento de gestão baseada na gestão de risco que permite, implementar, operar, monitorizar de forma pró-ativa, rever, manter e otimizar a segurança da informação de uma organização. O SGSI não é uma ferramenta tecnológica, como o nome pode levar a crer, é um instrumento completo de gestão que inclui, por exemplo, a definição da estrutura organizacional, definição de papéis e políticas de segurança. Há um consenso no mercado de que a criação de um SGSI, por si só, não resolve absolutamente todos os problemas de segurança existentes numa organização, apenas trata de sistematizar a gestão de riscos e descrever as melhores práticas para tratá-los [6][8].

Dentro deste quadro, a norma ISO/IEC 27002 (capitulo 4) tem como principal objetivo descrever controlos preventivos, que na sua grande maioria, evitam a ocorrência de incidentes envolvendo a informação da organização. Há também controlos de monitorização, que permitem reduzir o tempo de exposição ao risco, que permitem detetar, de forma rápida e efetiva, eventuais violações às regras do sistema de segurança da informação [6][23].

[7] Controlo: - é uma 'medida preventiva' que permite evitar que algo aconteça.

3.4 Política de Segurança da Informação

Para proteger as organizações das ameaças à segurança da sua informação ou da informação que está sob a sua responsabilidade, deve a organização possuir uma política de segurança, sendo necessário simultaneamente uma identificação e avaliação de riscos.

A segurança dos sistemas de informação, mais do que um simples produto ou tecnologia, que se pode adquirir, aplicar e esquecer, deverá ser encarada de forma integrada com o negócio da empresa, como um processo em permanente evolução que requer uma enorme capacidade para promover e gerir mudanças, tanto nos hábitos e comportamentos como nas infraestruturas organizativas e tecnológicas [13].

Considerando uma organização um determinado nível de risco aceitável, a segurança da informação resulta da aplicação de um conjunto de medidas e controlos que têm por objetivo evitar que as vulnerabilidades dos sistemas em causa sejam explorados por potenciais ameaças. A figura 14 mostra um diagrama que permite visualizar a relação entre ameaças, vulnerabilidades e medidas [8] [1].

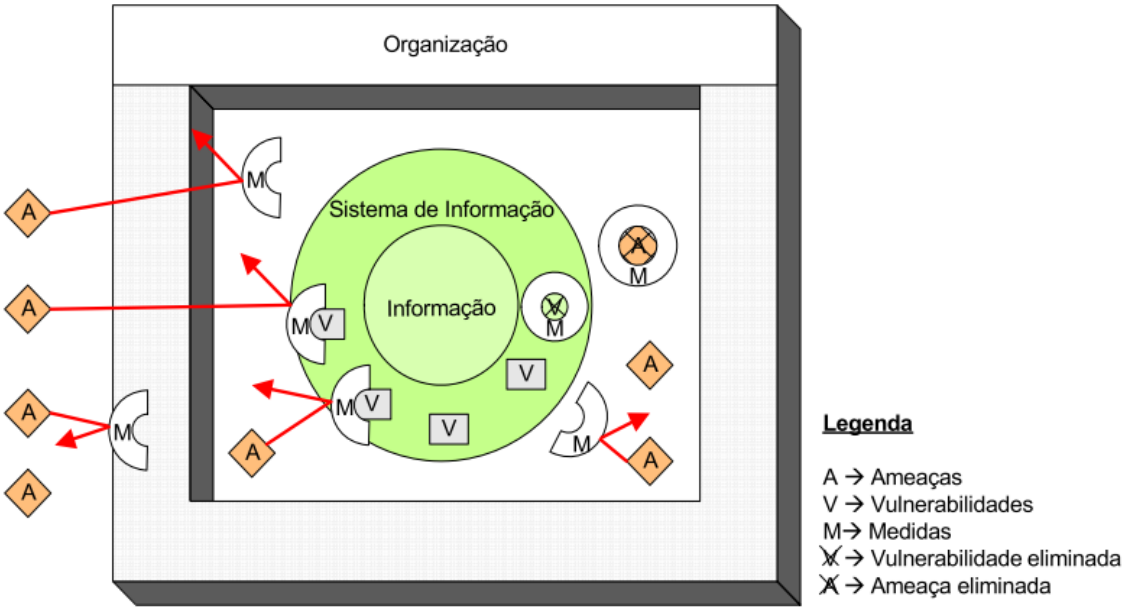


figura 14: - Exemplo de modelo de segurança [1].

Se as medidas consideradas para controlar a situação forem aplicadas de forma isolado ou avulso, isto é, não integradas numa política global de segurança, o seu resultado poderá ter um efeito negativo, e por vezes dispendioso para a organização. Para que o resultado das medidas tenha, o efeito desejado, estas devem estar enquadradas por uma ou numa política

de segurança da informação que tem como objetivo garantir um nível de proteção adequado e devidamente controlado, apoiada por uma avaliação adequação e eficiente que resulta de acompanhamento ou monitorização sistemática.

A política de segurança da informação deve descrever para além do entendimento, as diretrizes e objetivos da organização em relação à segurança da informação. Essa política deve ser suficientemente simples para que seja facilmente compreendida por todos os colaboradores da empresa, deve ser também genérica para que seja aplicável a toda a corporação. Uma política normalmente é implementada através de processos que descrevem quais atividades é que devem ser executadas para que uma tarefa seja devidamente cumprida conforme pretendido pela organização [6].

Deste modo, 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 as suas diretrizes [8] [1] .

Uma política de segurança define vários propósitos, entre os quais os seguintes:

- Descreve o que está a ser protegido, e por quê;
- Define prioridades sobre o que deve ser protegido em primeiro lugar e qual o custo subjacente;
- Permite estabelecer um acordo explícito com várias partes da organização em relação ao valor da segurança;
- Fornece ao departamento de segurança um motivo válido para dizer “não” quando é necessário;
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não” sempre que é preciso;
- Impede que o departamento de segurança tenha um desempenho fútil.

A política de segurança da informação, deverá estar enquadrada e devidamente definida na vida da própria organização, com ou maior responsabilidade e maturidade que outra atividade qualquer, porque vai interferir nos sistemas de informação que estão intima e diretamente ligados a vida e dinâmica de todo a organização, somente desta forma será possível obter e consolidar uma boa política de segurança [1].

Segundo *Peltier*, a segurança da informação, e consequentemente a política a ela associada, deve assentar sobre os seguintes princípios [44] :

- Estar alinhada com os objetivos, ou missão, da organização;
- Ser suportada por um conjunto de processos compreensíveis e integrados;
- Ser avaliada periodicamente com vista à deteção de possíveis desvios e/ou para a implementação de novos mecanismos que contribuam para uma melhoria do processo;
- Estar enquadrada 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 é determinado com base na análise resultante da gestão do risco.

A segurança de informação definida numa política adotada por qualquer organização, não é tarefa trivial de fácil implementação ou finalizável, normalmente resulta de um aperfeiçoamento e esforços sucessivos e contínuos por forma a atingir um nível optimo de segurança pretendida e exigida pela organização, esta realidade atribui á segurança da informação a característica de um processo de gestão, o que alias se identifica nas normas ISO 9001[8], ISO 14001[9] e ISO/IEC 27001. Estas recomendam que para o processo de segurança seja usado o modelo *Plan–Do–Check–Act* (PDCA[10]), em tudo semelhante ao utilizado nos processos de gestão [8][1].
Assim é conferido a segurança de informação o estatuto de um Sistema de Gestão de Segurança da Informação (SGSI).

3.5 Segurança da Informação de Saúde

Do ponto de vista da segurança da informação existem de modo geral nas organizações de saúde, nomeadamente nos Hospitais, duas áreas importantes de salientar: área administrativa/económica e a clínica/administrativa. Estas duas áreas carecem de uma política de segurança. No entanto, dada a natureza distinta de cada área, a atitude por parte da organização no que respeita à segurança da informação tem ou pode ser diferente[1].

Se ocorrer uma quebra de segurança na área administrativa/económica pode ser grave para o bom funcionamento da unidade de saúde enquanto "empresa/organização", uma quebra de segurança na área clínica/administrativa pode ser bem mais nefasta enquanto prestador

[8] ISO 9001: - A norma ISO 9001 constitui uma referência internacional para a Certificação de Sistemas de Gestão da Qualidade.
[9] ISO 14001: - A norma ISO 14001 constitui uma referência internacional para a Certificação de Sistemas de Gestão Ambiental.
[10] PDCA: - *Plan–Do–Check–Act*, é a metodologia proposta pela norma ISO/IEC 27001 para um SGSI.

de cuidados de saúde. Dada a natureza da informação da área clínica/administrativa, esta têm necessidades especiais quanto às seguintes dimensões da segurança (confidencialidade, disponibilidade, integridade e autoria/responsabilidade) [45][46].

A evolução tecnológica tem obrigado a que o conceito de segurança da informação na área clínica/administrativa sofra uma grande evolução e desta forma a noção de confidencialidade da informação clínica já ultrapassou a relação médica/doente, tanto pelo fator tecnológico como pelo surgimento de outros profissionais de saúde. O proteção da privacidade que em tempos estava somente consagrada nos códigos deontológicos das carreiras dos profissionais da área da saúde atualmente é exigido aos sistemas de informação visto que qualquer quebra de segurança neste sector tem um impacto pessoal significativo, principalmente quando se verifica na perda da confidencialidade da informação clinica/administrativa, isto é informações pessoais associadas a hábitos e doenças socialmente rejeitadas [47][48].

A integridade da informação clínica/administrativa também tem uma importância primordial. Uma informação que tenha perdido a sua integridade pode conduzir, por exemplo, à aplicação de um tratamento menos adequado, cujas consequências poderão ser imprevisíveis ou muito graves para o paciente.
A disponibilidade da informação, é tão importante como a confidencialidade e integridade da informação, porque permite evitar que haja consequências negativas por indisponibilidade da informação, quando ela e necessária a quem necessita de um determinado cuidado de saúde [48].

Para alguns autores esta área tem uma natureza específica e consideram que às três dimensões clássicas da segurança da informação se deve juntar a dimensão da autoria/responsabilidade. Esta é caraterizada como a dimensão que permite conhecer o autor e ou responsável por uma determinada informação ou processo. A dimensão autoria/responsabilidade é muita importância nos tempos atuais, pela necessidade de determinar com exatidão onde começa e acaba a responsabilidade de cada profissional de saúde que intervêm nos cuidados prestados a um doente [1][49].

3.6 Discussão

Quando se analisam dados estáticos como os apresentados no anexo C, verifica-se que, no caso dos Hospitais (anexo C.1) em 2010 num universo de 235, existiam em termos percentuais com actividades gerais informatizadas, 93% com gestão financeira e administrativa, 86% com marcação de tratamentos e consultas, 60% com trocas internas de

imagens médicas e com actividades médicas informatizadas, 86% com serviço internamento, 75% com base de dados da informação clinica do paciente, 60% com processo clinico eletrónico. No que se refere a segurança formalmente definida, somente 22% é que tem uma subscrição de um serviço de segurança.

Relativamente as Empresas (anexo C.2) em 2010 num universo de 2 843, pode-se verificar que somente 23% das empresas (com 10 ou mais funcionários) é que apresenta políticas de segurança formalmente definidas com plano de revisão regular. Onde relativamente a área de actividade o sector financeiro e de seguros representam 65% dessas empresas e, em relação ao número de funcionários, as empresas com 250 ou mais funcionários representam 62%.

Estes dados mostram que, em Portugal a cultura que as organizações têm, em que não é necessário que a segurança da informação deve estar assente e formalmente definida numa política de segurança suportada por um SGSI, tem de mudar e já começa a dar sinais dessa mudança, sob pena de verem os seus ativos cada vez mais em risco e por consequência a sua própria sobrevivência.

A actividade associada a segurança da informação deve estar integrada nos processos de gestão e decisão, para que a definição de políticas de segurança e o seu respetivo papel, seja assumida na plenitude por toda a organização.

Este trabalho, procura contribuir para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), suportado pelas normas internacionais (família de normas ISO/IEC 27000), que definem os princípios fundamentais e boas práticas (isto e, conjunto de políticas, práticas, procedimentos, mecanismos ou ações que promovem a proteção sobre a informação de uma determinada organização ou pessoa), e por um modelo de gestão de risco que permite, implementar, monitorizar de forma pró-ativa, manter e otimizar a segurança da informação de uma organização através da utilização de controlos preventivos que evitem a ocorrência de incidentes por forma a garantir um nível de proteção adequado e devidamente controlado. E desta forma, permitir que a organização adquira a tranquilidade necessário para gerir as espectativas da sua actividade, a continuidade dos seus resultados e negócio, a eficácia/eficiência dos seus processos, a produtividade pretendida, e a evolução desejada de forma segura e confiável através de um ambiente estável dos seus sistemas de informação. Sendo a gestão de risco, um instrumento determinante para a eficiência de um SGSI, a sua escolha e definição é um requisito fundamental muito importante que merece toda a atenção e cuidado.

Capítulo 4 - GESTÃO DO RISCO

4.1 Introdução

Com as organizações a depender cada vez mais dos seus sistemas de informação e o aparecimento de novas tecnologias e novas formas de trabalhar, como a massificação das redes de comunicações, da internet, do correio e comércio eletrônico, das redes virtuais privadas e *wireless*, os funcionários móveis, etc., as organizações começaram a despertar para a necessidade de segurança, uma vez que se tornaram cada vez mais vulneráveis a um grande número de potenciais ameaças. Isto é, expostas a grandes riscos que podem comprometer e por em causa os seus objetivos e, ou a sua existência [50].

4.2 Vulnerabilidade, Ameaça e Ataque

Os termos vulnerabilidade, ameaça e ataque estão diretamente, ou indiretamente ligados à gestão do risco da segurança da informação. De seguida será retratado cada um destes itens relativamente ao conceito e significado que cada um representa.

Vulnerabilidade é a característica ou ponto em que um determinado sistema está suscetível a um ataque, ou seja, é uma condição encontrada num determinado ativo (recurso, processo, configuração, etc.), que denota fragilidades e fraquezas que podem ser exploradas por uma ameaça ou mais ameaças e resultar em prejuízo ou danos para a organização ou pessoa. Todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros, facilmente podemos concluir que as vulnerabilidades fazem parte do cotidiano das organizações e estão presentes em todas as áreas de actividade de uma organização [7][51][52].

As vulnerabilidades podem estar ligadas às propriedades de um ativo, que podem ser utilizadas de forma ou para um propósito diferente daquele para o qual o ativo foi adquirido ou desenvolvido. É necessário considerar vulnerabilidades resultantes de diferentes fontes, como por exemplo; as intrínsecas ao ativo e as extrínsecas [51][52].

Para cada uma das vulnerabilidades existentes podem ocorrer determinados incidentes de segurança por concretização das ameaças a que cada uma pode estar sujeita. Desta forma, podemos concluir que as vulnerabilidades são as principais causas de ocorrências de incidentes de segurança, conforme esquema representado na figura 15.

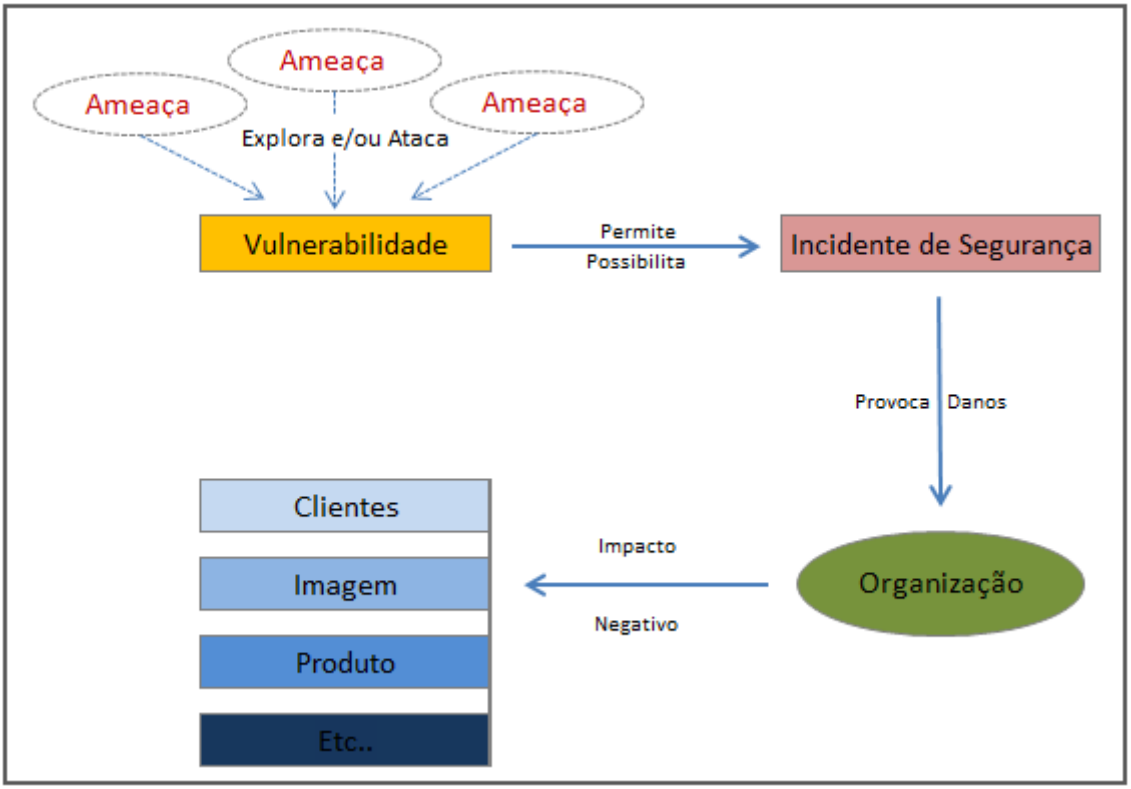


figura 15: - Vulnerabilidade, principal causa de incidentes de segurança da informação.

A evolução tecnológica tem permitido que cada vez mais haja maior capacidade de armazenamento de informação em formato eletrónico (suporte digital), aumentando desta forma a sua exposição e vulnerabilidade a muito mais tipos e variedade de ameaças do que existe ou 'existia' quando a informação estava no formato manual (papel, etc.). A relação de dependência em muitas organizações dos sistemas de informação com as telecomunicações permite que as mesmas, em diferentes localidades possam estar interligadas por meio de redes de telecomunicações entre filiais ou organizações do grupo, ou entre clientes e fornecedores, veio esta relação ampliar ainda mais essas vulnerabilidades. De entre as várias vulnerabilidades, esta relação aumenta o potencial de ameaças por acesso não autorizado, por abuso ou fraude, não ficando limitada a um único lugar, mas podendo ocorrer em qualquer um dos pontos de acesso à rede. Para complementar este cenário, são exigidos cada vez mais, complexas e diversas configurações de *hardware*, *software*, pessoas e processos organizacionais para as redes de telecomunicações que permitem a criação de novas áreas e oportunidade de invasão e manipulação, tal como por exemplo as redes sem fio, que baseadas em tecnologia rádio são mais vulneráveis à invasão, as redes de telecomunicações são altamente vulneráveis a falhas de *hardware*, *software,* e a fenómenos naturais [53]. Estão ilustrados na figura 16, alguns exemplos de vulnerabilidades das redes de telecomunicação.

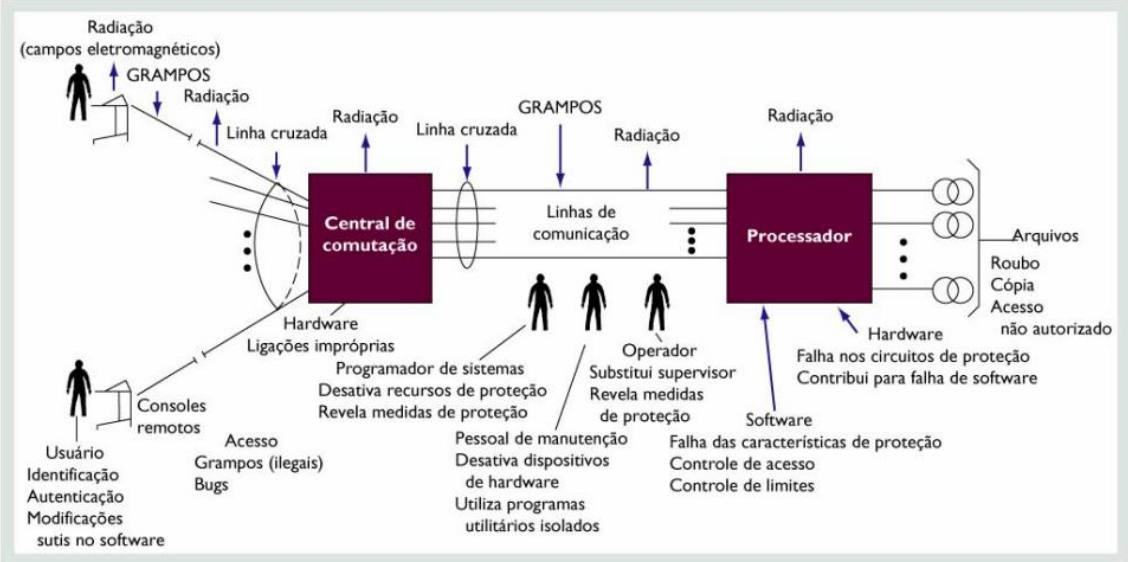


figura 16: - Alguns exemplos de vulnerabilidades das redes de telecomunicação [7].

No anexo D.1, é apresentada a interligação entre a utilização da internet e a sua implicação nas vulnerabilidades dos sistemas.

Ameaça, pode ser definida como qualquer ação, acontecimento ou entidade que pode atuar sobre um ativo, processo ou pessoa, através de uma possível vulnerabilidade e consequentemente provoca um determinado impacto, prejuízo ou dano. Só existe uma ameaça se existirem uma ou mais vulnerabilidades que possam ser exploradas [7][52].

Outro conceito é de ”ameaça inteligente”, que é definida como a circunstância em que uma determinada entidade tem potencialidade técnica e operacional para detetar e explorar uma vulnerabilidade de um determinado sistema [7].

A tendência atual é que, as ameaças à segurança da informação continuam a crescer não apenas em número de ocorrências, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e de mitigação de incidentes cada vez mais difícil e sofisticado, figura 17 [6].

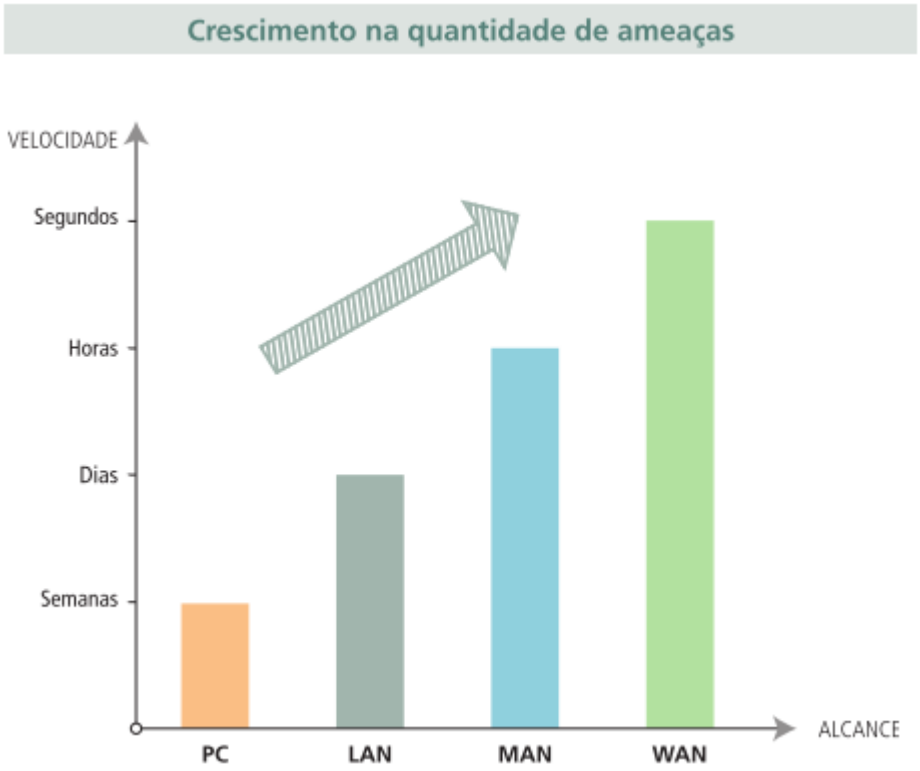


figura 17: - Evolução do número de ameaças em relação as TIC [6].

Não são apenas as ameaças externas que representam riscos numa corporação organização, os próprios funcionários representam um alto risco quando mal-intencionados ou quando não têm consciência dos riscos envolvidos na manipulação da informação [6][7].

As ameaças podem ser classificadas pela sua intencionalidade e ser divididas em grupos [4] [51]:

- Naturais: – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.
- Acidental / Involuntárias: – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados por acidentes, erros, falta de energia, incêndio, falha de *hardware* ou *software*, problemas elétricos, alterações no programa/aplicação, etc.
- Intencional / Voluntárias: – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários, falha de *hardware* ou *software,* invasão pelo terminal de acesso, roubo de dados e equipamentos, problemas elétricos, alterações no programa/aplicação, problemas de telecomunicação, etc.

As ameaças podem ter origem em fatores técnicos, organizacionais e Ambientais, e podem ser agravadas por más decisões administrativas [53].

A norma ISO/IEC 27005:2008 tipifica no seu anexo C, o exemplo de ameaças mais comuns que estão associados aos Sistemas de Informação, transcritas neste documento no anexo F.3 (Catálogo Ameaças mais comuns “Tipo e Origem”).

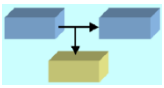
Ataque, pode ser considerado um assalto realizado por uma ameaça ou resultante de uma ameaça ‘inteligente’ sobre um sistema de informação. Pode ser considerado um ato inteligente de uma tentativa deliberada, método ou técnica para ultrapassar ou invadir serviços de segurança e comprometer as politicas de segurança do sistema e ou da organização [43][52].

Ataque é um ato de contorno, desvio, passagem pelos mecanismos e controlos de segurança de um sistema de gestão da segurança quebrando os seu princípios e propósitos.

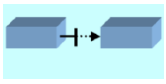
Um ataque pode ser classificado como [9][52]:

- Ativo, quando visa a alteração da informação (ou dados);
- Passivo, quando visa disponibilizar, roubar informação (ou dados);
- Destrutivo, quando visa à negação do acesso a informação (ou dados) ou serviços.

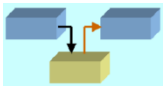
Num sistema de informação podem ocorrer as seguintes classes de ameaças, [7]:



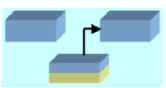
- Interceção: acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).



- Interrupção: pode ser definida como a interrupção do fluxo normal das mensagens ao destino.



- Modificação: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.



- Personificação: considera-se personificação a entidade que acede a informação e/ou transmite mensagens passando-se por uma entidade autêntica, violação da autenticidade.

Do ponto de vista motivacional os ataques podem ter a sua origem por questões: :

Desafio, Ego, Rebeldia, Vingança, *Status*, Dinheiro, Ganho monetário, Destruição de informações, Divulgação ilegal de informações, Utilização de recursos de outro sistema, Alteração de dados não autorizados, Chantagem, Ganho politica, Vantagem competitiva, Espionagem económica e/ou militar e/ou de Serviços de inteligência, Erros e omissões não intencionais [51].

4.3 Risco e Gestão do Risco

Existem várias definições para o conceito de risco, em função da área de estudo, do autor, das quais destacam-se as seguintes:

- Risco, é o efeito da incerteza nos objetivos [54]. Risco, pode ser considerado uma expectativa de perda que é expressa como a probabilidade de que uma determinada ameaça explorar uma determinada vulnerabilidade, e provocar um determinado problema ou dano no sistema [43].
- Risco é a combinação das consequências que resultam da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo [51].
- Para, Dawel [55], o risco é apenas uma forma de representar a probabilidade de algo acontecer. Trata-se de uma possibilidade.

Em resumo, risco da segurança da informação, é a possibilidade de uma ameaça explorar um determinado ativo[11] ou um conjunto de ativos, e desta forma prejudicar a organização. É medido em função da combinação da probabilidade de um evento e da sua consequência [51].

Neste contexto Beal [56], acredita que a gestão de risco é o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Quando existe uma potencial ameaça que explora uma vulnerabilidade cujo seu nível de proteção é baixo, estamos perante uma grande probabilidade da ameaça se concretizar e provocar danos, logo existe um risco associado a essa vulnerabilidade. O risco de modo geral existe sempre, tem é valores diferentes dependendo da presença de possíveis falhas,

[11] Ativo(s): - é um bem ou conjunto de bens, valores, créditos, direitos e assemelhados que forma o patrimônio de uma pessoa, singular ou coletiva, num determinado momento, avaliado pelos respetivos custos [81][82].

isto é, níveis baixos de proteção ou fraquezas associadas aos ativos, e que resultam em vulnerabilidades. Uma verdade incondicional, é que todos os ativos de qualquer organização estão sujeitos a vulnerabilidades normalmente associadas a falhas nos seus controlos, que podem ser de maior ou menor gravidade, dependendo da ameaça que as explora e que podem proporcionar riscos para a organização [50].

Dawel [55] considerava que, o grande objetivo da segurança da informação é aprender a lidar e conviver com o risco, e não a eliminá-los completamente, o que na maioria das vezes é impossível.

Um dos maiores problemas de quem gere a segurança da informação, é como mostrar à administração a verdadeira necessidade de investimentos nesta área e quais os benefícios que este investimento pode trazer. A resposta é simples e objetiva, através da gestão do risco [24][50] .

A gestão de risco é a tentativa de minimizar as fontes de riscos de segurança da informação, através da implementação, modificação ou reatribuição de recursos de segurança. Utiliza como entrada para a decisões a tomar os resultados da análise de riscos e vulnerabilidades, avaliação/análise de risco, os ativos a serem protegidos, as consequências de ataques bem-sucedidos e os recursos disponíveis para providenciar a segurança e tem como saída o tratamento a dar ao risco [52]:

- A Análise de Riscos e Vulnerabilidades permite:
  - Uma análise de riscos e vulnerabilidades possibilita a deteção de falhas sendo o mais importante, a possibilidade de aplicação de controlos objetivos nos pontos mais críticos e com reais necessidades de investimento. Desta forma é possível verificar ou determinar quais seriam as possíveis perdas e consequências por falta de controlos adequados.
  - Utilizar relatórios que resultem da análise de riscos e vulnerabilidades devidamente organizados e com objetivos bem definidos (onde, para além dos riscos relacionados com aspetos tecnológicos devem estar também aspetos, físicos e administrativos), permitindo aos gestores da Segurança da informação a possibilidade de apresentar as necessidades desta área de forma clara e concisa a administração da organização.
- A análise/avaliação de riscos permite [51]:
  - Quantificar ou descrever o risco qualitativamente o que permite aos gestores a priorização dos mesmos, de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

- Determinar o valor dos ativos de informação, identificar as ameaças e vulnerabilidades existentes (ou que poderiam existir), identificar os controlos existentes e seus efeitos no risco identificado, determinar as consequências possíveis e, finalmente prioriza os riscos derivados e ordenados de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

- Tratamento do Risco [57][51] :
  - Existem quatro opções para o tratamento do risco (reduzir, reter, evitar e transferir), que não são mutuamente exclusivas, por vezes as organizações podem beneficiar substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e a transferência ou retenção dos riscos residuais. Algumas formas de tratamento do risco podem lidar com mais do que um risco efetivamente (por exemplo: o treino e a consciencialização em segurança da informação). No entanto convêm que um plano de tratamento de risco seja definido, identificando claramente a ordem de prioridade em que as formas específicas de tratamento do risco devem ser implementadas, assim como os referidos prazos de execução.

4.4 Risco nos Sistemas de Informação de Saúde

Nas organizações e instituições de saúde a troca de informação entre os diversos agentes é uma prática comum e de extrema necessidade funcional dos diversos sectores e processos, que na sua maioria estão cheios de incertezas relativamente a privacidade e nível de segurança de informação necessária tendo em conta que a mesma, incorpora normalmente para além da informação administrativa do paciente ou utente, informação financeira, as condições de saúde e os cuidados médicos prestados. Partindo do princípio que esta informação somente deveria estar acessível aos profissionais autorizados (obedecendo aos princípios da confidencialidade) o que não se verifica em muitas das realidades em algumas organizações de saúde, é também importante e fundamental que ao mesmo tempo essa informação (especificamente quando se trata da prescrição de cuidados e terapêuticas) não estivessem sujeitas a possibilidade de serem corrompidas ou alteradas por terceiros, seja de forma casual, acidental ou mesmo deliberadamente.

Na figura 18, estão descritos alguns dos tipos de problemas mais comuns evidenciados nos hospitais portugueses através de um levantamento empírico, realizado em 2010 [24]. Muito destes problemas, atualmente ainda transparecem e persistem em muitas organizações de saúde, expondo a um elevado risco de segurança a informação que produzem e tratam

apesar de alguma evolução verificada em alguns dos mecanismos ou controlos de segurança da informação, aplicados de forma isolada conforme se pode verificar no anexo C.1 (Hospitais: Internet - estatística por tipo de aplicações de segurança).

1.	Existem poucas ou nenhumas políticas de segurança da informação e poucos estão familiarizados com normas como por exemplo, segurança, risco clínico e não clínico, ambiente, qualidade, etc.
2.	O número de profissionais da equipa das TI é reduzido e raramente existe uma aposta num gestor de segurança, coordenador ou até comité onde exista a participação explícita de um elemento do Conselho de Administração.
3.	Existem diversos serviços de *outsourcing* mas falta a capacidade para a gestão de contratos e de serviços para um acompanhamento e monitorização da prestação de serviço dessas entidades (seja em presença física ou remota).
4.	Não estão definidas grande parte das responsabilidades dos funcionários nas suas actividades dentro e fora do hospital.
5.	O serviço de recursos humanos não participa na gestão dos acessos e credenciais dos funcionários e não existe controlo no acesso à informação de gestão (*userid*, *password*, biometria, impressão, cartão magnético, etc.).
6.	Não existe documentação nem procedimentos para política de abertura de utilizadores no acesso à infra-estrutura, gestão de palavras passe, sistemas de *single sign-one* e gestão de identidades (bloqueio de acesso por cessação de contrato de trabalho por exemplo).
7.	Não estão definidos quais os recursos humanos com acesso à informação crítica nem quais os locais (zonas) críticas do hospital que deverão ter níveis de detecção e extinção de incêndios ou sistemas de controlo ambiental.
8.	Deveria existir uma monitorização do acesso de utilização de todos os recursos do hospital utilizados pelas entidades externas (nomeadamente bases de dados com dados do hospital, pastas partilhadas, serviços de rede, etc.).
9.	Deveria existir uma monitorização de sistemas com recurso a *logs* e auditoria com consola central para a gestão de eventos e alertas.
10.	Normalmente não estão descritas as políticas e procedimentos de *backups*.
11.	Não existe uma política documentada para a gestão da segurança das redes.
12.	Não são utilizados armários seguros ou cofres para salvaguardar informação crítica.
13.	Existem PCs portáteis em actividades de negócio, sem critérios de utilização, nem mecanismos de segurança, onde seja permitida a utilização no exterior do hospital.
14.	A circulação interna da informação física não é efectuada de forma segura (processo clínico, prescrições, etc.).
15.	Existem acessos remoto a sistemas e aplicações pelos funcionários que não estão documentados nem registadas como incidências.
16.	Não existem registos de incidências ao serviço de *helpdesk* interno e gestão de stocks (conceitos ITIL para a gestão de TI) nem políticas de *hardening* (*clear desk*, *clear screen*).
17.	Não existem estudos para avaliação de catástrofe ou a implementação de planos e ensaios de continuidade de negócio e *disaster recovery*.
18.	Não existem políticas para a confidencialidade e privacidade em dados privados dos utentes.
19.	Não existem garantias de conformidades para com as legislações aplicáveis ao negócio.

figura 18: - Exemplo de problemas mais comuns nos hospitais [24].

Tem sido evidenciada ainda mais nos tempos que correm, a importância que a segurança da informação e dados tem vindo a assumir de forma crescente nas diferentes e diversas organizações e mesmo na vida privada e social do comum dos cidadãos, especificamente desde da era digital (das Tecnologias de Informação e Comunicações) em que a distribuição, destruição e manipulação não autorizada da informação está ou é muito mais facilitada e exposta na era digital do que estava na era do papel.

Com vista a assegurar de forma adequada e consistente a proteção total da informação, têm sido criadas regulamentações e normas nacionais e internacionais com a especificidade de proteger a informação como ativo das organizações. Para área da informação de saúde, para além das regulamentações nacionais, existe a norma internacional ISO/IEC 27799:2008 criada especificamente para esta área. A família de normas ISO/IEC 27000 disponibiliza orientações técnicas e boas práticas que permitem a implementação de um Sistema de Gestão da Segurança da Informação (SGSI).

4.5 Normas ISO/IEC sobre a Segurança da Informação

Sem um conjunto de regras toda a execução de uma actividade ou tarefa poderá ser executada de distintas formas, seguir diversos caminhos ou percursos, apresentar resultados disparos ou absurdos, não ser repetível e encaminhar-se em grande parte para a dependência de um individuo especificamente, não permitindo muita das vezes a obtenção de indicadores válidos, permite sistematicamente a subjetividade e a sua falta de otimização. As normas são um documento estabelecido por consenso e aprovado por um organismo reconhecido nacional ou internacionalmente, que fornece, para o uso comum e repetitivo, regras, diretrizes ou características para atividades ou resultados, que visam a obtenção de um grau ótimo para o controlo e desempenho de actividades operacionais e especificas de um dado contexto numa organização que a pretenda implementar [58].
As nomas associadas à segurança da informação, surgem de forma a apresentar um conjunto de recomendações para a gestão da segurança da informação, definindo as melhores práticas internacionais nesta matéria ou área.

Elas fornecem uma abordagem sistemática de gestão para adotar as melhores práticas em controlos, quantificar o nível de risco aceitável, implementação e monitorização das medidas adequadas que protejam a confidencialidade, integridade e disponibilidade da informação [59].

Algumas normas definem aspetos que se deve ter em consideração ao elaborar e implementar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela

British Standards Institution) e a ISO/IEC 17799. A ISO começou a publicar a família de normas 27000 (figura 19), em substituição à ISO/IEC 17799 (e por conseguinte à BS 7799), das quais a primeira ISO 27001 foi publicada em 2005, e que se concentram nos requisitos, controlos de segurança e orientação para implementação de um Sistema de Gestão de Segurança da Informação (SGSI) numa organização.

Cronologia de Publicações das Normas ISO/IEC - Segurança da Informação			
Ano	**Nome da Norma**	**Finalidade**	**OBS**
1989	Britsh Standard (BS) 7799	Código de Prática do Utilizador	Nasceu no Commercial Computer Security Center do Departamento of Trade na Industry
1995	Britsh Standard (BS) 7799-1 (Parte 1)	Código de Prática para a Gestão da Segurança da Informação	Resulta do aperfeiçoamento da BS 7799 que dá origem a BS 7799-1 (parte 1)
1998	Britsh Standard (BS) 7799-2 (Parte 2)	Sistema de gestão da Segurança da Informação – Especificações e guia para utilização	
Abr.1999	Britsh Standard (BS) 7799-1:1999	Código de Prática para a Gestão da Segurança da Informação	Publicação da 1ª revisão da BS 7799-1 que dá origem a BS 7799-1:1999
Dez.2000	ISO/IEC 17799:2000	Código de prática para gestão da segurança da informação também referenciada como BS ISO/IEC 17799:2000	A BS 7799-1 foi poposta em Out.1999 como norma ISO, publicada em Dez.2000 como ISO/IEC 17799:2000, não permitia a certificação
Set.2002	BS 7799-2:2002	Sistema de gestão da Segurança da Informação – Especificações e guia para utilização	Foi lançada a BS 7799-2 (parte 2), que passa a estar em harmonia com a ISO 9000 e a ISO 14000 e tem por objetivo a implemetação de um SGSI, considerando os controlos seleccionados a partir da ISO/IEC 17799:2000
Out.2005	ISO/IEC 27001:2005	Sistemas de Gestão da Segurança da Informação - Requisitos	A BS 7799-2 transforma-se em ISO/IEC 27001 tal como aconteceu com a ISO/IEC 17799
2005	ISO/IEC 27002:2005	Código de Boas Práticas para a Gestão da Segurança da Informação	A ISO/IEC 17799 tranforma-se na ISSO/IEC 27002
2008	ISO/IEC 27011:2008	Diretrizes de Gestão da Segurança da Informação para Organizações de Telecomunicações baseadas na norma ISO / IEC 27002	
2008	ISO/IEC 27799:2008	Gestão da Segurança da informação em Saúde, baseada na norma ISO / IEC 27002	Código de Boas Práticas para a Gestão da Segurança da Informação em Saúde
2009	ISO/IEC 27004:2009	Gestão da Segurança da Informação - Medição	
2010	ISO/IEC 27003:2010	Orientação da Implemetação de um Sistema de Gestão da Segurança da Informação	
2011	ISO/IEC 27005:2011	Gestão de Riscos da Segurança da Informação	
2011	ISO/IEC 27006:2011	Requisitos para Organismos de Auditoria e Certificação de Sistemas de Gestão da Segurança da	
2011	ISO/IEC 27007:2011	Diretrizes para Auditoria ds Sistemas de Gestão da Segurança da Informação	
2012	ISO/IEC TR 27000:2012	Sistemas de Gestão da Segurança da Informação - Visão Geral e Vocabulário	
2012	ISO/IEC TR 27010:2012	Gestão da Segurança da Informação para a Comunicação Inter-Setoriais e Inter-Organizacional	
2012	ISO/IEC 27013:2012	Orientações sobre a implementação integrada de ISO / IEC 27001 e ISO / IEC 20000-1	
2012	ISO/IEC TR 27015:2012	Diretrizes de Gestão da Segurança da Informação para Serviços Financeiros	

figura 19: - Cronologia de Publicações das Normas ISO/IEC - Segurança da Informação [60][61].

A figura 20 mostra a família de normas ISO/IEC 27000 mais utilizadas desde a implementação até a certificação e auditoria de um SGSI.

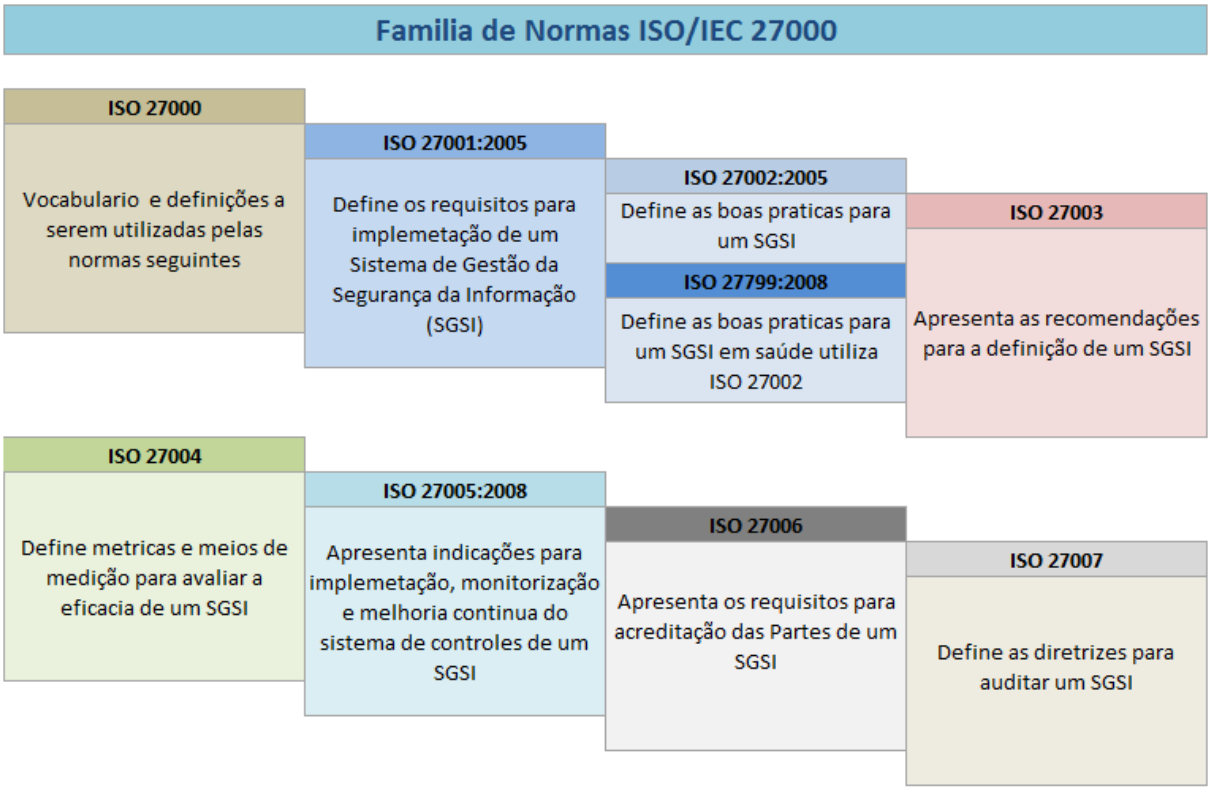


figura 20: - Família de Normas ISO/IEC 27000 mais utilizadas - Segurança da Informação.

Qualquer organização que pretenda implementar, com ou sem fins de certificação a norma ISO/IEC 27001, isto é, um Sistema de Gestão da Segurança da Informação (SGSI), obtém os benefícios descritos na secção 4.5.2 no 8º paragrafo, (página 59, “Uma organização …, de entre outros benefícios obtém a partida os seguintes:”).

4.5.1 Norma ISO/IEC 17799:2005

A norma ISO/IEC 17799:2005 passou a chamar-se ISO/IEC 27002:2005 em meados de 2007, para fazer parte da família de normas ISO/IEC 27000, o texto permanece idêntica a norma ISO/IEC 17799:2005 e, é de fato a norma ISO/IEC 17799 padrão que é vendida com a observação na capa da mudança de número. O portal de recursos e informação da norma ISO/IEC 17799 descreve-a como o mais reconhecido padrão de segurança da informação. É baseada no padrão BS 7799 da Instituição *British Standard* cuja última publicação foi em Maio de 1999 com uma edição que, por si só, incluiu muitas melhorias e benefícios em relação às suas versões anteriores. A norma ISO/IEC 17799 foi inicialmente publicado em dezembro de 2000, e em Junho de 2005 foi publicada a mais recente e ultima versão como ISO/IEC 17799:2005, como mencionado acima, essa versão figurou até meados de 2007 e hoje é conhecida como norma ISO/IEC 27002: 2005 [60][62].

Esta norma apresentava de entre outras as seguintes características:

- Oferecia uma base comum e devidamente sustentada que permite:
    1. Desenvolver e implementar boas práticas de gestão de segurança eficazes;
    2. Estabelecer relações de confiança na troca de informação de negócio;

- Disponibiliza 10 domínios/cláusulas (que se traduziam em 117 controlos) diferentes [62]:

    1. Política de segurança;
    2. Organização da segurança;
    3. Classificação e controle de recursos;
    4. Segurança pessoal;
    5. Segurança física e ambiental;
    6. Gestão de comunicações e operações;
    7. Controlo de acessos;
    8. Desenvolvimento e manutenção de Sistemas;
    9. Gestão da continuidade de negócio;
    10. Conformidade;

- As recomendações apresentadas deverão ser escolhidas e utilizadas tendo em conta às normas e regulamentações aplicáveis ao negócio em causa.
- Encoraja as organizações a desenvolverem as suas próprias diretrizes.
- Não permite por si só a certificação da gestão da segurança da informação.

4.5.2 Norma ISO/IEC 27001:2005

Foi publicada em Outubro de 2005, tendo como origem a BS 7799-2 e a norma ISO/IEC 17799-2. Especifica os requisitos que permitem desenvolver, implementar, monitorizar, rever, manter e melhorar um ISMS - *Information Security Management System* (SGSI - Sistema de Gestão de Segurança da Informação), no contexto do negócio de uma organização. A norma ISO/IEC 27001 foi desenvolvida por uma variedade de diversas organizações que tinham o objetivo comum de proteger os seus ativos de informação, que para eles seria como "sangue vital" para todos os negócios [62][63][64].

Esta norma é utilizada em todo o mundo por organizações comerciais e governamentais, como base para a gestão da política de uma organização para implementação da gestão de segurança da informação. É ou pode ser, utilizada por pequenas, médias e grandes organizações, porque o seu padrão foi projetado para ser suficientemente flexível de modo a ser utilizado por qualquer tipo de organização [62][63].

Esta norma, para além de estabelecer estratégias de segurança para uma determinada organização, pode ainda ser utilizada para avaliar a conformidade pelas partes interessadas internas e externas. O SGSI proposto pela norma assegura a seleção de controlos de segurança adequados e proporcionados para proteger os ativos de informação e assegurar a confiança desejada. Todos os controles de segurança recomendados pela norma ISO/IEC 27001:2005 são detalhados na norma ISO/IEC 27002:2005, e na norma ISO/IEC 27799:2008 especificamente para as organizações de saúde [24][64].

A norma ISO/IEC 27001:2005 introduz o conceito de um Sistema de Gestão de Segurança da Informação – SGSI, representado na figura 21, e descreve a necessidade de um *framework* detalhado de controlos para alcançar os objetivos de segurança apresentados como relevantes pela avaliação de risco, como também, especifica um ciclo sistêmico de processos de uma organização, em conjunto com a identificação e interações destes processos [63][64][8].

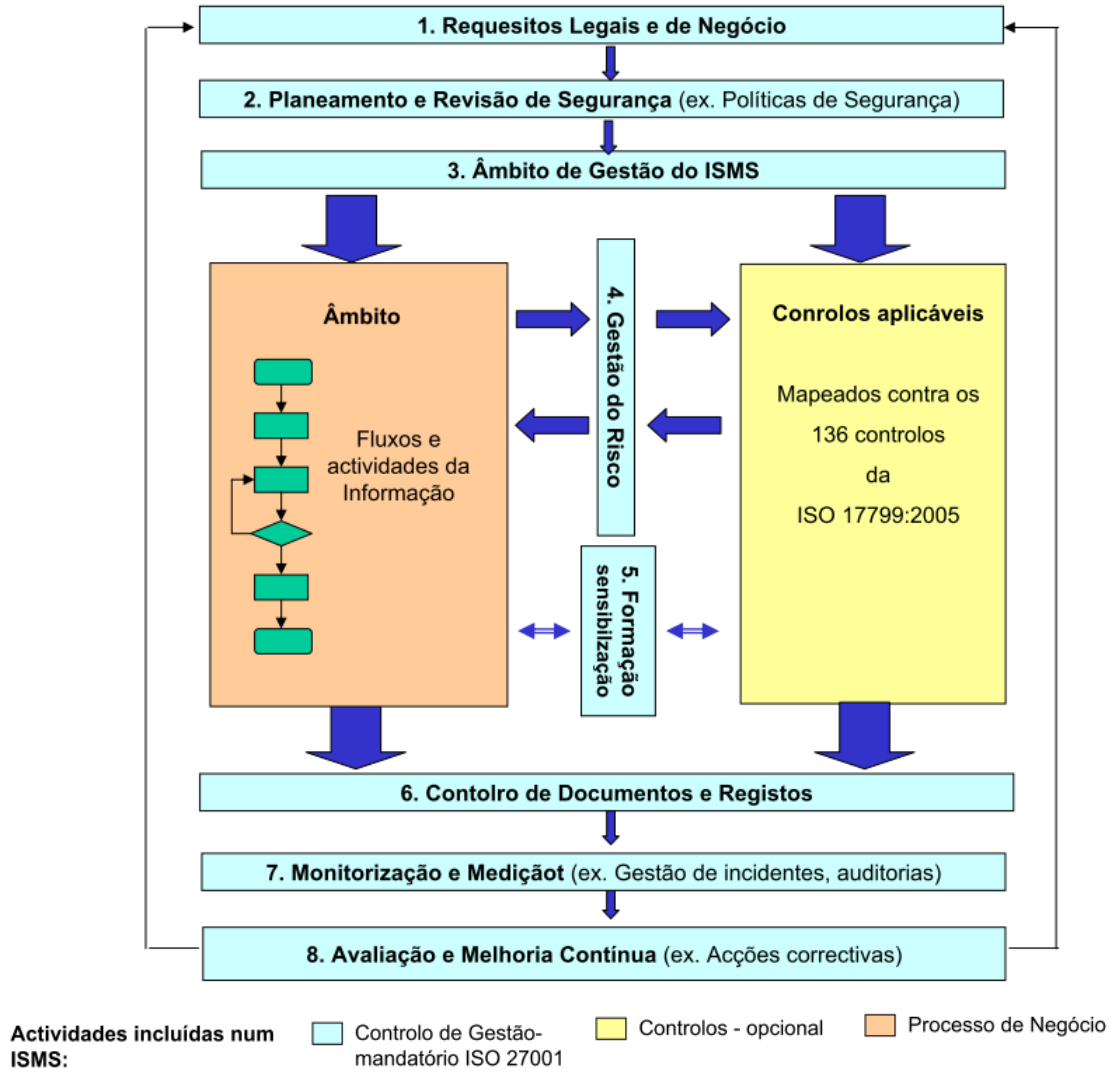


figura 21: - Processos e actividades de um SGSI.

A norma ISO/IEC 27001:2005 incorpora o ciclo sistêmico *Plan-Do-Check-Act* (PDCA[12]), representado na figura 22, que é adotado em toda a estrutura dos processos do Sistema de Gestão de Segurança da Informação (SGSI). O ciclo PDCA apoia-se no ciclo de melhoria contínua que consiste em planificar (*Plan* – P), fazer (*Do* – D), verificar (*Check* – C) e agir (*Act* – A). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais, contribuindo para a tomada de decisões de gestão e para o alcance das metas e objetivos porque apresenta processos estruturados para uma organização que deseje implementá-los [8][65][64].

[12] PDCA: - é a metodologia proposta pela norma ISO/IEC 27001 para que um SGSI esteja sujeito a um processo de melhoria continua e consiste em 4 etapas (*Plan, Do, Check, Act*).

Ciclo PDCA (Plan, Do, Check, Act)

O ciclo **PDCA,** é a metodologia proposta pela norma ISO/IEC 27001 para que um **SGSI** - Sistema de Gestão de Segurança da Informação esteja sujeito a um processo de melhoria continua e consiste em 4 etapas (Plan, Do, Check, Act). É um metodo interativo em que as suas etapas são sequênciais, quando aplicado a um SGSI, permite que a medida que se vai conhecendo a organização podem aparecer novas necessidades e requisitos que obrigam a mudanças na planificação e na propria opercionalidade do SGSI.

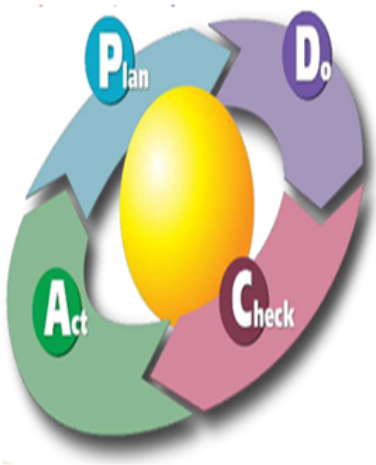
Os princípios definidos pelas Diretrizes de OECD para a Segurança de Sistemas de Informação e Redes aplicam-se para toda a política e níveis operacionais que governam a segurança de sistemas de informação e redes. Esta Norma provê uma estrutura de um sistema de gestão de segurança da informação para implementar alguns dos princípios da OCDE que usam o modelo PDCA e os processos descritos nas seções 4, 5, 6 e 8, como indicado na tabela B.1. do anexo B da norma ISO/IEC 27001.

P (Plan) - Planificação do SGSI

Esta é a etapa da planificação, onde são definidas as estrategias e planos a seguir com base na norma 27001 perante o cenario e problemas a resolver.

D (Do) - Implementação e Operação do SGSI

Nesta etapa incia-se a avaliação e tratamento dos pontos identificados como criticos pela organização. São implementados mecanismos ou ferramentas, é realizada formação e sensibilização de todos os intervenientes, são realizadas analise e tomadas as ações adequadas e necessárias em função do aval dos responsáveis.



A (Act) - Manutenção e Melhoria

Nesta etapa são tomadas decisões para corrigir possivies desvios indesejaveis e não conformidades de modo a que seja possivel manter a solução inicialmente planificada ou mesmo melhora-la.

C (Check) - Monitorização e Analise Critica

Nesta etapa a organização terá a percepção da maturidade do seu sistema, atraves da analise critica dos dados obtidos atraves da monitorização das medidas e ações decididas e implemetadas. Verifica os desvios e não conformidades onde podem surgir questões como:

. O problema foi resolvido?

. Como podemos melhorar a solução?

figura 22: - PDCA aplicado a um SGSI.

A norma ISO/IEC 27001 é um guia complementar para a norma ISO/IEC 27002, explica como deve ser implementada a norma ISO/IEC 27002 e a utilização do SGSI que é necessário para garantir um ciclo contínuo de atividades. As normas ISO/IEC 27001 e ISO/IEC 27002 são padrões mais genéricos e, portanto, é necessária uma orientação específica quanto à sua aplicação na área da saúde. Esta situação levou e motivou a publicação da norma ISO/IEC 27799, que será posteriormente analisada neste capítulo na secção 4.5.4 [24][62].

A norma ISO/IEC 27001, desde os critérios mais táticos até aos mais operacionais abrange o leque de todos os aspetos a ter em consideração, o que faz com que seja atualmente a única norma para certificação na gestão da segurança da informação. A sua popularidade deve-se ao facto de que, a sua abrangência a torna capaz de ser utilizada em qualquer organização (indústria, comércio, distribuição, saúde, finanças, etc.), e a sua flexibilidade permite que possa complementar-se com outras normas de segurança para as TIC [24][62].

Uma organização que tenha um Sistema de Gestão da Segurança da Informação (SGSI) implementado com base nesta norma, estando ou não certificada, de entre outros benefícios obtém a partida os seguintes [6][63][66]:

- Credibilidade comercial;

  O facto de a organização ser reconhecida ao nível da proteção da informação é uma garantia para os seus clientes e parceiros da forma como os seus dados são tratados pela organização.

- Redução de custo;

  O custo de um único incidente de segurança poderá ser consideravelmente superior ao investimento em sistemas de proteção. Por outro a certificação pode diminuir o custo de eventuais prémios de seguros que tenham como objeto a segurança da organização.

- Cumprimento de leis e regulamentos;

  A implementação da norma ISO 27001 ou a certificação demonstra às autoridades competentes e acionistas que a organização cumpre as leis e regulamentos aplicáveis, tanto do ordenamento jurídico português como regulamentos sectoriais.

- Redução do risco de incidentes de segurança;

  A implementação da norma ISO 27001 ou a certificação proporciona um melhor conhecimento dos sistemas de informação, das suas vulnerabilidades e da forma como os proteger, o que resulta num aumento do nível de proteção contra riscos de negócio.

- Integração da segurança da informação com os objetivos de negócio;

- Segurança da informação demonstrável e monitorada;

- Linguagem internacional única, com padrões da família ISO/IEC 27000.

A tabela a seguir (adaptada da ISO/IEC 27001) apresenta os capítulos da norma com os seus respetivos requisitos:

Nº	Capítulo	Descrição
0	Introdução	Apresentação da norma
1	Objetivo	Abrangência da norma
2	Referencia Normativa	Outras normas necessárias para o SGSI. Exemplo referenciação a ISO/IEC 27001 ou ISO/IEC 27799
3	Termos e Definições	Termos e definições sobre segurança da informação
4	Sistema de Gestão de Segurança da Informação	Informações sobre o objetivo, a implementação, a monitorização, melhoria e documentação de um SGSI
5	Responsabilidades da direção	Compromisso da direção, treino, sensibilização e disponibilização de recursos para o SGSI
6	Auditorias internas do SGSI	Auditorias internas, realizadas por pessoal treinado e comprometido com o SGSI
7	Análise crítica do SGSI pela direção	A direção deve analisar as ações efetuadas pelo SGSI, e atuar como um elemento de controlo do mesmo
8	Melhoria do SGSI	Melhorias contínuas da eficácia, através de a ações corretivas e preventivas efetuadas pelo SGSI

4.5.3 Norma ISO/IEC 27002:2005

Anteriormente, esta norma era conhecida como norma ISO/IEC 17799, a partir de 2005 a nova edição da norma ISO/IEC 17799 foi incorporada na família de normas ISO/IEC 27000 e passou a ter a designação de norma ISO/IEC 27002:2005, conforme descrição cronológica da figura 19.

A ISO/IEC 27002 estabelece um código com as melhores práticas em segurança da informação, apresenta uma relação de objetivos de controlo e recomenda uma série de controlos de segurança específicos. Os objetivos de controlo e os controlos desta norma têm como finalidade ao serem implementados, dar resposta aos requisitos de segurança identificados por meio da análise/avaliação de riscos. Esta norma serve também como guia prático, para desenvolver e implementar procedimentos de segurança da informação numa organização, permitindo a utilização de eficientes práticas de gestão da segurança, e ajudar a criar confiança nas atividades interorganização [23][59][64].

Esta norma disponibiliza uma *checklist* padrão de objetivos de controlo em 11 áreas (secções), num total de 39 categorias principais de segurança, cada uma com uma

descrição de um ou mais controlos de segurança. O anexo A da norma ISO/IEC 27002:2005 apresenta uma relação completa de todas as secções, objetivos de controlo, e sua descrição. Os domínios ou cláusulas fundamentais da norma são as seguintes [23]:

- 5[13]. Política de Segurança: - Descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.
- 6. Segurança Organizacional: - Descreve a estrutura de gestão para a segurança de informação, assim como estabelece/define responsabilidades, incluindo terceiros e fornecedores de serviços.
- 7. Classificação e Controlo de Ativos de Informação: - Trabalha a classificação, o registro e o controlo dos ativos da organização.
- 8. Segurança Relacionada Com as Pessoas: - Foca o risco decorrente de actos intencionais ou acidentais relacionados com pessoas. Pode também abordar aspetos, como a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e formação em assuntos relacionados com a segurança.
- 9. Segurança Física e Ambiental: - Descreve a necessidade de se definirem áreas de circulação restrita e a necessidade de proteger os equipamentos e a infraestrutura de tecnologia de informação.
- 10. Gestão das Operações e Comunicações: - Descreve as principais áreas que devem ser objeto de especial atenção da segurança. Entre estas áreas destacam-se as questões relativas a procedimentos operacionais e respetivas responsabilidades, homologação e implantação de sistemas, gestão de redes, controlo e prevenção de vírus, controlo de mudanças, execução e armazenamento de *backups*, controlo de documentação, segurança de correio eletrónico, etc.
- 11. Controlo de Acesso: - Regula o controlo de acessos aos sistemas, definição de competências, o sistema de monitorização de acesso e uso, a utilização de senhas, etc.
- 12. Desenvolvimento e Manutenção de Sistemas: - Descreve os requisitos de segurança dos sistemas, controlos de criptografia, controlo de arquivos e segurança do desenvolvimento e suporte de sistemas.

[13] Número da Cláusula/Domínio na norma ISO/IEC 27002, isto referente ao domínio ou categoria principal de segurança. Esta numeração resulta da sequência numérica das secções do documento da norma [23].

- 13. Gestão de Incidentes de Segurança: - Descreve a notificação de fragilidades e eventos de segurança da informação, bem como a gestão de incidentes de segurança da informação e melhorias.
- 14. Gestão da Continuidade do Negócio: - Descreve a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.
- 15. Conformidade: - Descreve a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção da informação de clientes ou utentes.

A norma não referência a utilização de qualquer tecnologia ou sistema de segurança específico, é totalmente neutra e abstrai-se dessa situação, no entanto é bastante flexível e tão abrangente que facilmente se ajusta e adaptada aos mais diversos e variados ambientes das TIC, crescendo dentro destes ambientes quando os mesmos estão sujeitos a rápidas e significativas alterações ou mudanças tecnológicas, métodos ou processos e pessoas. As boas praticas introduzidas na organização, podem levá-la a apostar na adoção de um modelo de gestão que permita obter expectativas de grande, médio impacto e de convergência. Segundo descrito pela *Information Security Forum*[14] (ISF) o resultado, expetativas e benefícios mais comuns esperados do grande, médio impacto, e de convergência associado à adoção das medidas na introdução do modelo de boas práticas da norma ISO/IEC 27002:3005 na organização são os seguintes [24]:

- Grande impacto:
  - Implementação de boas práticas;
  - Avaliação do estado dos controlos;
  - Definir metas para a segurança da informação
  - Redução da frequência e impacto de incidentes
- Médio impacto:
  - Conformidade com as políticas internas
  - Integração do sistema com o programa ISRM[15]
  - Ir ao encontro dos requisitos de regulamentação
  - Maximizar o investimento realizado

[14] *Information security Forum* (ISF): - é uma organização internacional, independente e sem fins lucrativos que se dedica ao *benchmark* e à identificação de boas práticas no que se relaciona à segurança da informação.
[15] ISRM: - *Information Security Risk Management*

- De convergência:
    - Obtenção de vantagens competitivas
    - Ir ao encontro dos requisitos da tutela
    - Adaptar-se as alterações do mercado
    - Controlo e redução de custos

A abordagem geral adotada pela norma ISO/IEC 27002:2005 é encorajar cada organização a considerar e interpretar o padrão dentro de seu próprio contexto, requisitos legais e de negócio. Experiências obtidas em muitos países incluindo Austrália, Canadá, França, Holanda, Nova Zelândia, África do Sul e no Reino Unido têm mostrado a necessidade de certas cláusulas de controlo e categorias de controlo, nos quais as informações pessoais de saúde têm de ser suportadas para estarem devidamente seguras. No caso das organizações de saúde que desejem implementar esta norma facilmente verificam que, a maioria dos objetivos de controlo é aplicada em quase todas as situações no entanto, alguns utilizadores desta norma na área de saúde aperceberam-se e reconheceram situações em que são necessários objetivos de controlo adicionais. Nestes casos a solução passa pela implementação ou adoção da norma ISO/IEC 27799 que define diretrizes para auxiliar as organizações da área da saúde e outras que trabalham com informação médica ou de saúde a gerirem de forma eficiente e correta a segurança da informação relacionada com este sector de actividade [63][64].

4.5.4 Norma ISO/IEC 27799:2008

As normas ISO/IEC 27001 e ISO/IEC 27002 são específicas para segurança da informação, sendo normas gerais que podem ser utilizadas independentemente do sector de actividade da organização. No entanto a norma ISO/IEC 27799:2008, é a norma específica e de referência do sector de saúde, apoiada pelas normas ISO/IEC 27001 e ISO/IEC 27002, por não apresentar as actividades operacionais e especificas de um SGSI. A figura 23 mostra a relação entre estas três normas e o papel de cada uma delas.

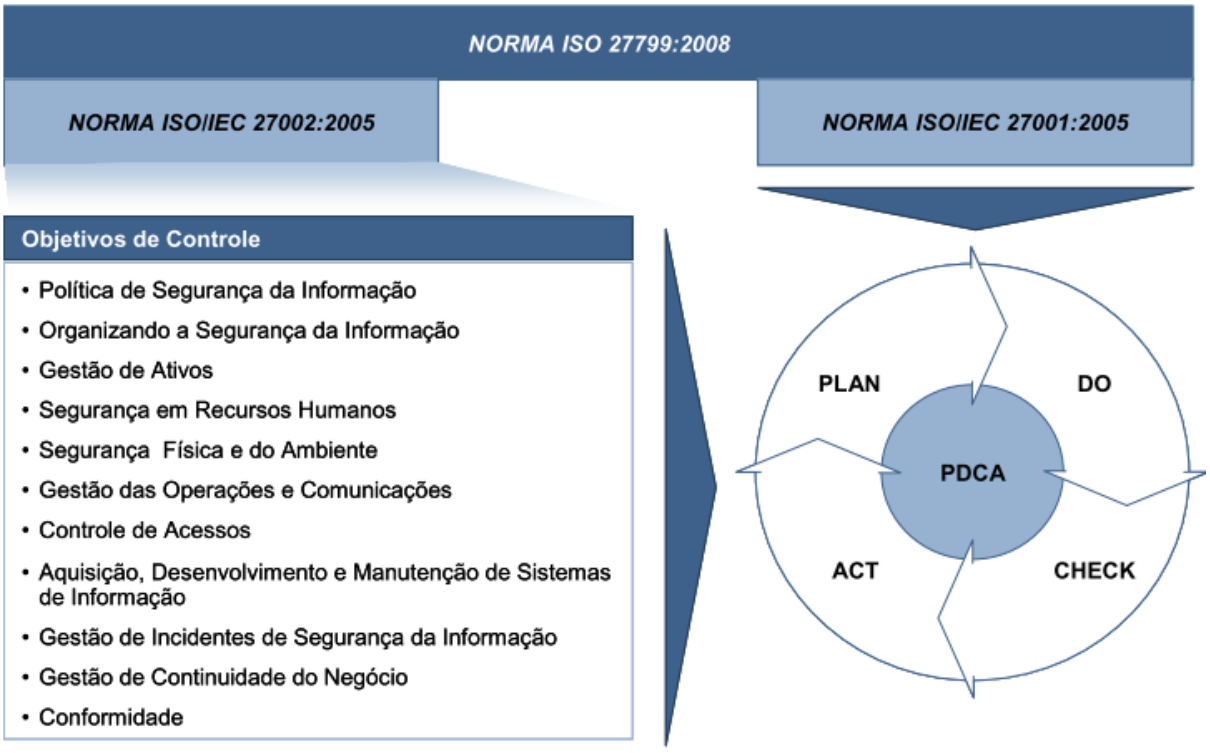


figura 23: - Relação entre as normas ISO/IEC 27799:2008, ISO/IEC 27001:2005 e ISO/IEC 27002:2005 [64].

Especificamente, esta norma internacional define as diretrizes especiais de gestão da segurança da informação do setor da saúde, nos seus diferentes ambientes operacionais enquanto a proteção e a segurança da informação pessoal de saúde[16] for um ativo importante para todos os indivíduos, corporações, instituições e governos há requisitos específicos do setor de saúde que têm de ser cumpridos para assegurar a confidencialidade, a integridade, a disponibilidade, a auditabilidade e a responsabilidade/autoria da informação pessoal de saúde [62][64].

A norma disponibiliza um conjunto de controlos para a gestão de segurança da informação de saúde e fornece orientações sobre melhores práticas. A implementação desta norma, de acordo com a ISO, vai permitir que as organizações de saúde assim como outras entidades que tratam informações de saúde possam garantir, um nível mínimo de segurança adequado e requerido de acordo com o seu tamanho e circunstâncias [67].

Embora se tenha baseado na norma ISO/IEC 27002, a estrutura da norma ISO/IEC 27799 difere, começa com um preâmbulo e introdução (não numerada) e tem as sete secções numeradas de 1 a 7. Semelhante ao da norma ISO/IEC 27002, a introdução e secções 1 a 6

[16] Informação pessoal de saúde: - De acordo com a norma ISO 27799:2008, refere-se à informação sobre uma pessoa identificável, relacionada com à saúde física ou mental do indivíduo, à provisão de serviços de saúde ou cuidados de saúde prestados ao indivíduo.

abordam aspetos introdutórios e informativos, como uma introdução à segurança de informação em saúde, o objetivo da norma, termos e referências normativas de saúde, informações de segurança e definições e uma ampla discussão sobre o plano de ação para implementar a norma ISO/IEC 27002. A maior parte da norma é feita na Seção 7, que abrange os domínios/cláusulas de segurança, secções, objetivos de controlo e controlos da norma a figura 24 apresenta uma comparação com a norma ISO/IEC 27002 relativamente ao número de domínios/cláusulas, secções e controlos. A última parte da norma compreende três anexos e uma bibliografia. É importante notar que a norma ISO/IEC 27799 incorpora aspetos da norma ISO/IEC 27001 na sua Seção 6, que discute um plano de ação para implementar a norma ISO/IEC 27002 [62][67].

	ISO/IEC 27002	ISO/IEC 27799
Número de Dominios/Cláusulas de Segurança	11	12
Número de Secções de Segurança	39	41
Número de Controlos	133	136

figura 24: - Normas, ISO/IEC 27002 versus ISO/IEC 27799 [62].
(domínios/cláusulas, secções e controlos)

Nas organizações de saúde, devido ao grande incremento que se tem verificado na troca de informação de saúde dos pacientes, de forma eletrônica entre profissionais desta área, existe a necessidade e benefícios em adotar uma referência comum para a gestão da informação produzida e tratada nestas organizações. A norma internacional ISO 27799:2008 baseia-se na experiência obtida em esforços nacionais e internacionais, em lidar com a segurança de informação pessoal de saúde, e é um documento associado à norma ISO/IEC 27002:2005. Em conclusão, esta norma aplica a norma ISO/IEC 27002:2005 no domínio da área de saúde de forma a considerar cuidadosamente a aplicação apropriada de controlos de segurança obrigatórios e ou adicionais, para assegurar os propósitos de proteção de informação pessoal de saúde [64].

4.5.5 Norma ISO/IEC 27005:2008

Em 2009 foi lançada pela ISO a norma ISO/IEC 31010:2009 Risk *management – Risk assessment techniques* (traduzido seria, Gestão de Riscos – Técnicas de avaliação de riscos) e deve ser trabalhada em apoio à norma ISO/IEC 31000:2009 Gestão de Riscos –

Principio e Diretrizes. A norma descreve as diversas técnicas e ferramentas de análise de risco. Este grupo de normas da família ISO/IEC 31000 tem por objetivo dar repostas ou proporcionar, uma conceção ampla e genérica da gestão de risco de qualquer tipo de ambiente de uma organização, permite avaliar e tratar qualquer tipo de risco corporativo.
Durante o desenvolvimento da família de normas ISO/IEC 31000, foi publicada em 2008, pelo grupo de trabalho específico de tecnologias da informação a norma ISO/IEC 27005:2008 Tecnologias da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Esta norma foi desenvolvida com base nos estudos da norma ISO/IEC 31000, portanto integra os seus requisitos e processos de gestão de risco. A ISO/IEC 27005 faz parte da família de normas ISO/IEC 27000 sobre o Sistema de Gestão de Segurança da Informação (SGSI), onde estão incluídas as normas ISO/IEC 27001 e ISO/IEC 27002 e ISO/IEC 27799. Apresenta as melhores práticas e possibilita o aprofundamento em aspetos exclusivos da segurança da informação, enquanto a ISO/IEC 31010:2009 é mais genérica e contempla todos os sectores [68].

A norma ISO/IEC 27005:2008 fornece as diretrizes para a gestão de risco de segurança da informação. Esta norma suporta os conceitos gerais descritos na ISO/IEC 27001 e foi concebida para facilitar a implementação de forma satisfatória da segurança da informação tendo como base a abordagem da gestão de risco. O conhecimento dos conceitos, modelos, processos e terminologias descritos na norma ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27799 são importantes para uma completa compreensão desta Norma. Ela é aplicável a todos os tipos de organizações (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos) que pretendem gerir os riscos que podem comprometer a segurança da informação da organização.
Uma visão geral do processo de gestão de riscos da segurança da informação é descrita na secção 6 da norma, conforme esquema representado na figura 27 (capítulo 5, secção 5.2 deste documento). As actividades de gestão de riscos de segurança da informação, apresentadas na secção 6 da norma, são descritas nas seguintes secções da mesma [51]:

- Definição do contexto (secção 7 da norma):
    - Considerações gerais;
    - Critérios básicos;
    - Objetivo e limites;
    - Organização para gestão de riscos de segurança da informação;

- Análise/Avaliação de risco (secção 8 da norma):
    - Descrição geral do processo de análise/avaliação[17] de riscos de segurança da informação;
    - Análise de riscos;
    - Avaliação de riscos.
- Tratamento do Riscos (secção 9 da norma):
    - Descrição geral do processo de tratamento do risco de segurança da informação (exemplificado na figura 28);
    - Redução do risco;
    - Retenção do risco;
    - Evitar (ação de evitar) o Risco;
    - Transferir o risco;
- Aceitação de risco (secção 10 da norma),
- Comunicação do risco (secção 11 da norma),
- Monitorização e análise crítica do risco (secção12 da norma).
    - Monitorização e análise crítica dos fatores de risco;
    - Monitorização e análise crítica e melhoria do processo de gestão de risco.
- As informações adicionais para as atividades de gestão de risco de segurança da informação estão apresentadas nos anexos da norma.

Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. A norma recomenda que a abordagem seja adequada ao ambiente da organização e em particular esteja alinhada com o processo maior de gestão de riscos corporativos.
A norma recomenda que a gestão de risco de segurança da informação seja um processo contínuo, em que esteja definido o contexto, a avaliação e tratamento dos riscos, usando um plano de tratamento que permita implementar as recomendações e decisões. Recomenda também que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito, com a finalidade de reduzir os riscos a um nível aceitável [51].

[17] De acordo com a norma ISO 27005:2008, cabe à organização selecionar o seu próprio método para a análise/avaliação de riscos baseado nos objetivos e nas metas definidas.

A norma ISO/IEC 27001 determina que os controlos implementados no objetivo, limites e contexto do SGSI devem ser baseados no risco. A aplicação de um processo de gestão de riscos de segurança da informação pode satisfazer este requisito. Existem vários métodos através dos quais o processo pode ser implementado com sucesso numa organização. No entanto convêm que a organização use o método que melhor se adeque as suas necessidades e circunstancias, para cada aplicação específica do processo [8][51].

Num SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento de risco e a aceitação do risco, fazem parte da fase "*Plan* - Planificação". Na fase "*Do* - Implementação" do SGSI, as ações e controlos necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco definido na fase anterior. Na fase "*Check* – Monitorização e análise crítica", os gestores determinam a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase "*Act* – Manutenção e melhoria", as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação. A figura 25 resume, os processos e actividades de gestão de riscos de segurança da informação, alinhados com as quatro fases do processo de SGSI definidos pela ISO/IEC 27001 [8][51].

Processo de Gestão de Riscos da Segurança da Informação (ISO/IEC 27005)	Processo do SGSI (ISO/IEC 27001)
Definição do contexto Análise/avaliação de riscos Definição do plano de tratamento do risco	Planeamento (*Plan*)
Implemetação do plano de tratamento do risco	Implementação (*Do*)
Monitorização contínua e análise crítica de riscos	Monitorização e análise crítica (*Check*)
Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação	Manutenção e melhoria (*Act*)

figura 25: - Processos de Gestão de Riscos de Segurança da Informação alinhados com as quatro fases do processo de SGSI.

A norma ISO/IEC 27005 apresenta as boas práticas para a gestão de riscos da segurança da informação, e as técnicas que descreve seguem o conceito, os modelos e os processos globais especificados na norma ISO/IEC 27001, para além de apresentar a metodologia de avaliação e tratamento dos riscos requeridos pela mesma norma, esta norma, acaba por descrever todo o processo e actividades necessárias para uma perfeita execução e realização da gestão de riscos da segurança da informação, que pode ser adotada por qualquer organização [68].

Capítulo 5 - MODELO PROPOSTO PARA GESTÃO DO RISCO

A gestão de riscos é um processo que traz benefícios a qualquer organização que tenha este processo implementado. A melhoria das condições de segurança da informação passa obrigatoriamente pelo conhecimento das fraquezas e vulnerabilidades que podem ser exploradas por ameaças que se podem concretizar. Indiscutivelmente, a melhor forma de o fazer é através da Gestão de Risco. A figura 26, ilustra o esquema conceptual de um processo de Análise do Risco, em que o item Riscos é, o elemento central (eixo) que faz girar toda a roda da gestão deste processo [8][64][67].

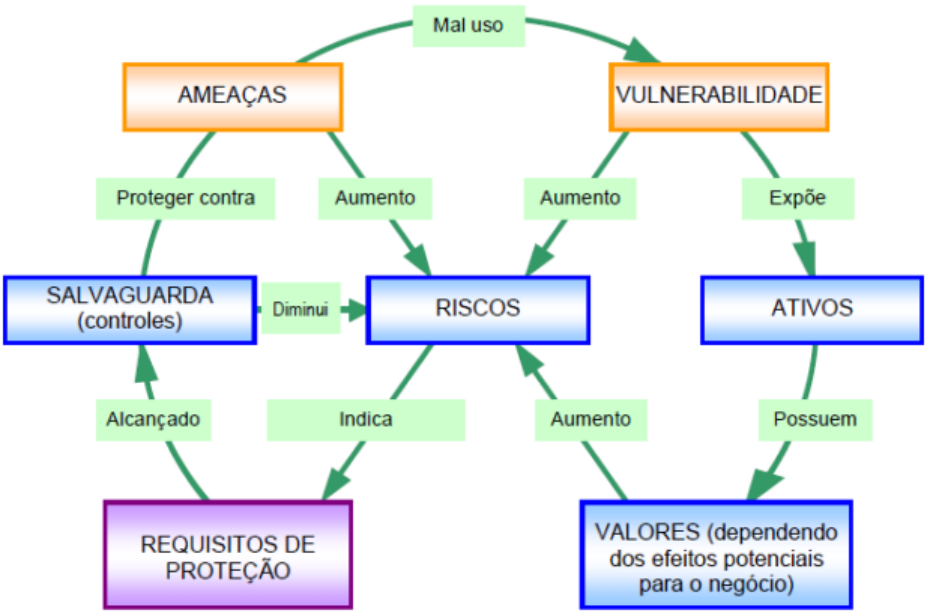


figura 26: - Relação entre fonte e tratamento do risco num modelo simplificado.

5.1 Arquitetura do Modelo Desenvolvido

Sendo o primeiro objetivo do Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde – **MDPSIOS** ser adotado para implementar um SGSI no sector da saúde, terá obrigatoriamente que cumprir com os requisitos necessários do sector, em que a especificidade da informação produzida e tratada impõe um conjunto de conformidades[18] e responsabilidades acrescidas na gestão de risco de segurança da informação.

[18] Conformidades legais, profissionais e operacionais

Como segundo objetivo, é o de ser adotado para implementar um SGSI em qualquer organização independentemente do seu sector de actividade.

Para que estes dois pressupostos sejam cumpridos com o mínimo de garantia relativamente ao modelo para Gestão de Risco, o modelo escolhido, foi indiscutivelmente o proposto pela norma ISO/IEC 27005:2008, que fornece as diretrizes e facilita a implementação de forma satisfatória, da segurança da informação tendo como base a abordagem de gestão de risco. A escolha desta norma, como modelo de gestão de risco, estando esta alinhada com as fases dos processos de um SGSI permitiu, um perfeito enquadramento e alinhado com as normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27799 que são as referências normativas que suportam todo o MDPSIOS e que lhe confere a característica de um SGSI.

5.2 Estrutura do Modelo

As actividades de gestão de riscos de segurança da informação a considerar são as apresentadas na secção 6 da norma ISO/IEC 27005:2008 [51], de acordo com fluxo de informação representado na figura 27, e cujos conceitos utilizados pelo **MDPSIOS**, são descritos nas próximas subsecções [51][58].

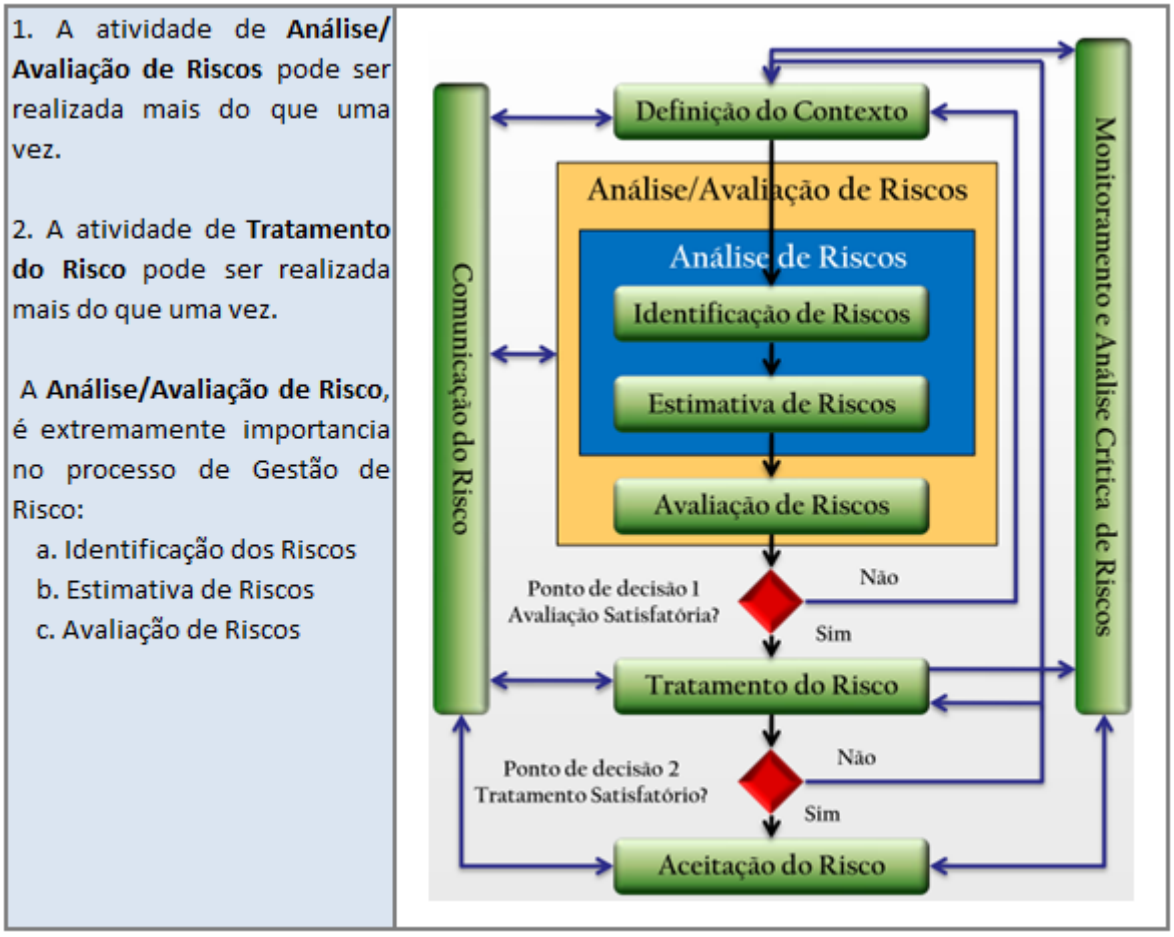


figura 27: - Estrutura funcional da análise/avaliação de riscos.

5.2.1 **MDPSIOS** - definição do contexto

Recomenda-se que o contexto para gestão de riscos de segurança da informação seja estabelecido, e que envolva a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação, a definição do objetivo e dos limites e defina uma organização apropriada para operar a gestão de riscos de segurança da informação.

- É essencial determinar o propósito da gestão de riscos de segurança da informação, pois ela pode afetar o processo em geral e a definição do contexto em particular. Esse propósito pode ser:
    a) Suporte a um SGSI;
    b) Conformidade legal e a evidência da realização dos procedimentos corretos;
    c) Preparação de um plano de continuidade de negócios;

d) Preparação de um plano de resposta a incidentes;
e) Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

No caso do **MDPSIOS**, para formalizar este ponto, deve ser utilizado o documento que se encontra no anexo F.1 - (Documento Padrão), página 174.

5.2.2 **MDPSIOS** - análise/avaliação de risco

- Descrição geral do processo de análise/avaliação de riscos de segurança da informação:

  Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

  Um risco é a combinação das consequências advindas da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo. A análise/avaliação de riscos quantifica ou descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

No caso do **MDPSIOS**, ao verificar-se a necessidade de formalizar este ponto, deve ser utilizado o documento que se encontra no anexo F.1 - (Documento Padrão), página 174.

5.2.2.1 **MDPSIOS** - análise de riscos

- Identificação de riscos:

  O propósito da identificação de riscos é determinar eventos/ocorrências que possam provocar potenciais perdas e deixar claro como, onde e porque pode a perda acontecer.

- Identificação dos ativos:

  É de boa prática, que os ativos dentro do objetivo definido sejam identificados (secção 4.2.1.d) 1) da norma ISO/IEC 27001[19]).

[19] Página 4 da norma ISO/IEC 27001 [8].

Um ativo é algo que tem valor para a organização e que, requer proteção. Para a identificação dos ativos convém que se tenha presente que um sistema de informação compreende mais do que *hardware* e *software*.

Recomenda-se, que a identificação dos ativos seja executada com detalhe adequado que forneça informações suficientes para a análise/avaliação de riscos. O nível de detalhe usado na identificação dos ativos influenciará a quantidade geral de informações reunidas durante a análise/avaliação de riscos. O detalhe pode ser aprofundado em cada iteração da análise/avaliação de riscos.

É aconselhado, que seja identificado um responsável para cada ativo, a fim de oficializar a sua responsabilidade e garantir a possibilidade da prestação de contas caso seja necessário.

O limite da análise crítica é o perímetro dos ativos da organização a serem considerados pelo processo de gestão de riscos de segurança da informação.

No caso do **MDPSIOS**, para formalizar este ponto, deve-se preencher o(s) campo(s) respetivo(s) ao mesmo, no documento que se encontra no anexo F.2 - (Inventario de Ativos), página 175. Deve-se ter em conta o nº da iteração[20] em que se está a trabalhar.

- Identificação das ameaças:

  É de boa prática, que as ameaças e suas fontes sejam identificadas (secção 4.2.1 d) 2) da norma ISO/IEC 27001[21]).

  Uma ameaça tem o potencial de comprometer ativos (tais como, informações, processos e sistemas) e, por isso, também as organizações. As ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais.

  Recomenda-se, que tanto as fontes das ameaças acidentais, como as intencionais, sejam identificadas. Uma ameaça pode surgir dentro ou fora da organização. Convém que as ameaças sejam identificadas genericamente e por classe (por exemplo: ações não autorizadas, danos físicos, falhas técnicas) e, se for apropriado, as ameaças específicas devem ser identificadas dentro das classes genéricas. Isso poderá significar que, nenhuma ameaça seja ignorada,

[20] Iteração, neste caso é considerada o número do processo ou ciclo do SGSI em que este se encontra. Um processo ou ciclo do SGSI corresponde a uma passagem pelas quatro fases do PDCA. Por exemplo a avaliação inicial ou ciclo "0" do SGSI, correspondera a Iteração T0. A 2ª avaliação dará início ao ciclo "1" do SGSI e correspondera a Iteração T1 e assim sucessivamente.

[21] Página 4 da norma ISO/IEC 27001 [8].

incluindo as não previstas, mas que o volume de trabalho exigido para tal, seja limitado.

Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes, dependendo da importância dos ativos afetados.

Recomenda-se que experiências internas de incidentes e avaliações anteriores de ameaças sejam consideradas na avaliação atual.

Quando forem utilizados catálogos de ameaças ou os resultados de uma avaliação anterior das ameaças, convém que se tenha consciência de que as ameaças mais relevantes estão sempre a mudar, especialmente se o ambiente de negócio ou se os sistemas de informações mudarem.

No caso do **MDPSIOS**, para ajudar na identificação das ameaças mais comuns, pode ser utilizado o catálogo que se encontra no Anexo F.3 - (Catálogo Ameaças mais comuns “Tipo e Origem”), página 176.
- Para formalizar este ponto, deve-se preencher o “Documento Inventário de Ativos” – anexo F.2, página 175, o campo associado a este item, na linha do ativo em causa. Deve-se ter em conta o nº da iteração em que se está a trabalhar.

- Identificação dos controlos existentes:

  É aconselhado, que a identificação dos controlos existentes seja realizada para evitar custos e trabalho desnecessário, por exemplo: duplicação de controlos. Enquanto os controlos existentes são identificados, deve-se efetuar uma verificação para assegurar que estão funcionar corretamente – caso exista, uma análise aos relatórios já existentes de auditoria do SGSI pode reduzir o tempo gasto nesta tarefa.

  Um controlo que não esteja a funcionar devidamente pode provocar o aparecimento de vulnerabilidades. Recomenda-se que seja tido em consideração a possibilidade de um controle selecionado (ou estratégia) falhar durante sua operação.

  Esta deteção pode ser auxiliada pela medição da eficácia dos controlos. Uma maneira para estimar o efeito do controle é verificar quanto reduz, por um lado, a probabilidade da ameaça e a facilidade com que uma vulnerabilidade pode ser explorada ou, por outro lado, o impacto do incidente.

  Recomenda-se que os controlos cuja implementação está planificada para tratamento do risco, tenham em conta aqueles que já estão implementados.

Os controlos existentes e ou planificados podem ser considerados ineficazes, insuficientes ou injustificados. Recomenda-se que um determinado controlo que seja insuficiente ou injustificado seja verificado ou reavaliado para determinar se convém que seja removido ou substituído por outro controlo mais adequado ou se convém que o controle permaneça em vigor, por exemplo, em função dos custos.

No caso do **MDPSIOS**, para formalizar este ponto, deve-se preencher o "Documento Inventário de Ativos" – anexo F.2, página 175, o campo associado a este item, na linha do ativo em causa. Deve-se ter em conta o nº da iteração em que se está a trabalhar.

- Identificação das vulnerabilidades:

  É de boa prática, que as vulnerabilidades que podem se exploradas por ameaças e comprometer os ativos ou a organização sejam identificadas (secção 4.2.1 d) 3) da norma ISO/IEC 27001[22]).

  Vulnerabilidades podem ser identificadas nas seguintes áreas:

  a) Organização;
  b) Processos e procedimentos;
  c) Rotinas de gestão;
  d) Recursos humanos;
  e) Ambiente físico;
  f) Configuração do sistema de informação;
  g) *Hardware*, *software* ou equipamentos de comunicação;
  h) Dependência de entidades externas.

  A presença de uma vulnerabilidade por si só não causa prejuízo, é necessário que haja uma ameaça presente a explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas recomenda-se que seja reconhecida como tal e monitorizada, para o caso de ocorrerem mudanças.

  Note-se que um controlo implementado, que funciona ou é utilizado incorretamente, pode, por si só, representar uma vulnerabilidade.

  Um controle pode ser eficaz ou não, dependendo do ambiente no qual está inserido. Inversamente, uma ameaça que não tenha uma vulnerabilidade correspondente pode não resultar em um risco.

[22] Página 4 da norma ISO/IEC 27001 [8].

Vulnerabilidades decorrentes de fontes diferentes devem ser consideradas, por exemplo: as intrínsecas ao ativo e as extrínsecas.

No caso do **MDPSIOS**, para ajudar a identificar as vulnerabilidades mais comuns, pode ser utilizado o catálogo que se encontra no anexo F.4 - (Catálogo Vulnerabilidades Comuns "Tipos e Exemplos de Ameaças"), página 178.
- Para formalizar este ponto, deve-se preencher no documento de "Inventário de Ativos – anexo F.2", o campo associado a este item, na linha do ativo em causa. Deve-se ter em conta o nº da iteração em que se está a trabalhar.

- Identificação das consequências:

  É de boa prática, que as consequências que a perda de confidencialidade, de integridade, de disponibilidade ou outra dimensão podem ter sobre os ativos, sejam identificadas (secção 4.2.1 d) 4) da norma ISO/IEC 27001[23]).

  Uma consequência pode ser, por exemplo, a perda da eficácia, condições adversas de operação, a perda de oportunidades de negócio, reputação afetada, prejuízo, etc.

  Esta atividade deve identificar o prejuízo ou as consequências para a organização que podem decorrer de um cenário de incidente[24]. O impacto dos cenários de incidentes é determinado considerando-se os critérios de impacto definidos durante a atividade de definição do contexto. Pode afetar um ou mais ativos ou apenas parte de um ativo. Aos ativos podem ser atribuídos valores correspondentes tanto aos seus custos financeiros, quanto às consequências no negócio se forem danificados ou comprometidos. Consequências podem ser de natureza temporária ou permanente como no caso da destruição de um ativo.

No caso do **MDPSIOS**, para formalizar este ponto, deve-se preencher no documento de "Inventário de Ativos – anexo F.2", o campo associado a este item, na linha do ativo em causa. Deve-se ter em conta o nº da iteração em que se está a trabalhar.

5.2.2.2 **MDPSIOS** - Estimativa de riscos

- Metodologias para a estimativa de riscos:

[23] Página 4 da norma ISO/IEC 27001 [8].

[24] Um cenário de incidente é a descrição de uma ameaça que explora uma certa vulnerabilidade ou um conjunto delas num incidente de segurança da informação (secção 13 da norma ISO/IEC 27002).

A análise de riscos pode ser empreendida com diferentes níveis de detalhe, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores.

Uma metodologia para estimativa pode ser qualitativa ou quantitativa ou uma combinação das duas, dependendo das circunstâncias. Na prática, a estimativa qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos. No entanto a posterior poderá ser necessário efetuar uma análise quantitativa ou mais específica, nos grandes riscos. Normalmente é menos complexo e menos oneroso realizar análises qualitativas do que quantitativas.

Recomenda-se que a forma da análise seja coerente com o critério de avaliação de riscos desenvolvida como parte da definição do contexto.

A estimativa qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das potenciais consequências (por exemplo: Pequena, Média e Grande) e a probabilidade dessas consequências ocorrerem. Uma vantagem da estimativa qualitativa é sua facilidade de compreensão por todas as pessoas envolvidas. Por outro lado, uma desvantagem é a dependência à escolha subjetiva da escala.

Estas escalas podem ser adaptadas ou ajustadas para se adequarem às circunstâncias e descrições diferentes podem ser usadas para riscos diferentes. Recomenda-se que a análise qualitativa utilize informações e dados factuais quando disponíveis.

A estimativa quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na estimativa qualitativa) tanto para consequências como para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados. A estimativa quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos de segurança da informação e interesses da organização. Uma desvantagem é a falta de tais dados sobre novos riscos ou sobre fragilidades de segurança da informação e também quando dados factuais e auditáveis não estão disponíveis. Nesse caso, a exatidão da análise/avaliação de riscos e os valores associados tornam-se ilusórios.

A forma como as consequências e a probabilidade são expressas e a forma em que elas são combinadas para fornecer um nível de risco irá variar de acordo com o tipo de risco e do propósito para o qual os resultados da análise/avaliação de riscos serão usados. Convém que a incerteza e a variabilidade tanto das consequências, como da probabilidade, sejam consideradas na análise e comunicadas de forma eficaz.

Muitos métodos fazem uso de tabelas, e combinam medidas empíricas com medições subjetivas. É importante que a organização use um método com o qual ela se sinta confortável, no qual ela acredite, e que produza resultados reproduzíveis. Alguns exemplos de métodos baseados em tabelas (anexo E.2 da norma ISO/IEC 27005[25]) são apresentados a seguir.

- Exemplo 1: Matriz com valores pré-definidos;

De um modo geral este tipo de método de análise/avaliação de riscos, ativos físicos, existentes ou planeados, são valorizados de acordo com os seus custos de reposição ou reconstrução (ou seja, medidas quantitativas) e convertidos para a mesma escala qualitativa usada para a valorização das informações. No final do processo uma matriz mostra a relação entre probabilidade de um cenário de incidente e o impacto estimado, do ponto de vista do negócio. A probabilidade de um cenário de incidente é dada pela probabilidade de uma ameaça vir a explorar uma vulnerabilidade. O risco resultante é medido em uma escada de 0 a 8 e, pode ser avaliado tendo como base os critérios para a aceitação do risco.

- Exemplo 2: Ordenação de Ameaças em função do Risco;

De um modo geral uma tabela ou matriz pode ser utilizada para relacionar as consequências (representadas pelo valor do ativo) à probabilidade de ocorrência de uma ameaça (incluindo assim os fatores ligados às vulnerabilidades). A primeira etapa consiste em avaliar as consequências (através do valor do ativo) numa escala pré-definida. Na segunda etapa, estima-se a probabilidade de ocorrência da ameaça em uma escala pré-definida. Por último, as ameaças podem ser ordenadas em sequência, conforme as suas respetivas medidas de risco.

Este procedimento permite que diferentes ameaças, com consequências e probabilidade de ocorrências distintas, sejam comparadas e ordenadas por

[25] Página 47 a 52 da norma ISO/IEC 27005[51].

prioridade. Em alguns casos, será necessário associar valores monetários às escalas empíricas aqui utilizadas.

- Exemplo 3: Avaliação da probabilidade e as possíveis consequências dos riscos;

Nesse exemplo, a ênfase é dada às consequências dos incidentes de segurança da informação (ou seja: aos cenários de incidentes) e recomenda-se que a atividade determine quais é que são os sistemas prioritários. Pode ser feito estimando-se dois valores para cada par de ativo e risco, os quais, combinados, irão determinar a pontuação para cada ativo. Quando as pontuações de todos os ativos do sistema são somadas, uma medida do risco ao qual o sistema está submetido pode então ser determinada.
Pode ser utilizado para diferenciar os sistemas entre si, e determinar qual o sistema com maior prioridade na proteção.

Cabe à organização escolher ou selecionar para a análise/avaliação de riscos baseado nos objetivos e nas metas definidas o seu próprio método, com o qual se sinta confortável, no qual acredite, e que produza resultados reproduzíveis (secção 8.1, pag.10 e anexo E.2, pag.48 da norma ISO/IEC 27005).

No caso do **MDPSIOS**, de entre as várias abordagens possíveis para este ponto, como por exemplo os métodos anteriormente descritos na sua generalidade, e outros não mencionados, o método adaptado para o MDPSIOS foi o Método simplificado quantitativo de Avaliação de Riscos da Segurança de Informação (**MARSI**), que resultada da adoção e adaptação na íntegra do Método simplificado quantitativo de Avaliação de Riscos de Acidentes de Trabalho (**MARAT**), que apesar de ser uma metodologia muito utilizada (de forma universal) na determinação de acidentes de trabalho pode aplicar-se na determinação da estimativa de riscos de segurança de informação pelas características e adaptação apresentadas, no anexo I (MPDSIOS – Descrição do MARSI adaptada do MARAT), página 249.

Em conclusão, a utilização no MDPSIOS desta metodologia (**MARSI**) apresenta as seguintes vantagens, que a partida são de realçar:

a) É um método simplificado quantitativo de avaliação de riscos;
b) Define Níveis de Deficiência (ND) do ativo, entrado em linha de conta com os controlos existentes ou não;
c) Permite no Nível de Severidade (NS) se for interesse da organização, categorizar o ativo consoante a sua natureza (informação ou material);

d) Para além dos Nível de Risco (NR) obtém também o Nível de Controlo (NC) que é uma ferramenta importante para a monitorização da eficiência das medidas e controlos implementados entre as possíveis iterações do SGSI;
e) A metodologia MARAT do qual é originário o MARSI, é de referência internacional na área de Higiene e Segurança no Trabalho, para a determinação de riscos de acidentes de trabalho que pode envolver danos em pessoas e bens matérias, em que as exigências de segurança a nível das pessoas sobrepõem-se a qualquer bem material, portanto, é um método devidamente testado e otimizado.

- Avaliação das Consequências/Severidade:

  Recomenda-se, que o impacto sobre o negócio da organização, que pode ser causado por incidentes (possíveis ou reais) relacionados à segurança da informação, seja avaliado tendo em conta as consequências de uma violação de segurança da informação, como por exemplo: a perda da confidencialidade, da integridade ou da disponibilidade dos ativos (secção 4.2.1 e) 1) da norma ISO/IEC 27001[26]).

  Depois de identificados todos os ativos relevantes, recomenda-se que os valores atribuídos a esses ativos sejam tidos em consideração durante a avaliação das consequências.

  O valor do impacto no negócio pode ser expresso de forma qualitativa ou quantitativa, porém um método para designar valores monetários geralmente pode fornecer mais informações úteis para a tomada de decisões e, consequentemente permitir que o processo de tomada de decisão seja mais eficiente.

  As consequências podem ser expressas em função dos critérios monetários, técnicos ou humanos, de impacto ou de outro critério relevante para a organização. Em alguns casos, mais do que um valor numérico é necessário especificar as consequências tendo em conta os diferentes momentos, lugares, grupos ou situações.

  É aconselhado, que as consequências expressas em tempo e valor financeiro sejam medidas com a mesma abordagem utilizada para a probabilidade da ameaça e as vulnerabilidades. A consistência deve ser mantida com respeito à abordagem quantitativa ou qualitativa.

[26] Página 5 da norma ISO/IEC 27001 [8].

No caso do **MDPSIOS**, para formalizar este ponto, deve-se preencher o "Documento Inventário de Ativos" – anexo F.2, página 175, o campo associado a este item, na linha do ativo em causa. Deve-se ter em conta o nº da iteração em que se está a trabalhar.

- Avaliação da probabilidade dos incidentes:

  Recomenda-se, que a probabilidade dos cenários de incidentes seja avaliada (secção 4.2.1 e) 2) da norma ISO/IEC 27001[27]).

  Depois de identificar os cenários de incidentes, é necessário avaliar a probabilidade de cada cenário e do impacto correspondente, usando técnicas de estimativa qualitativas ou quantitativas. Convém levar em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas, considerando o seguinte:

  a) A experiência passada e estatísticas aplicáveis referentes à probabilidade da ameaça;

  b) Para fontes de ameaças intencionais:
     A motivação e as competências, que mudam ao longo do tempo, os recursos disponíveis para possíveis atacantes, bem como a perceção da vulnerabilidade e o poder da atração dos ativos para um possível atacante;

  c) Para fontes de ameaças acidentais:
     Fatores geográficos (como por exemplo: proximidade a fábricas e refinarias de produtos químicos e petróleo), a possibilidade de eventos climáticos extremos e fatores que poderiam acarretar erros humanos e o mau funcionamento de equipamentos;

  d) Vulnerabilidades, tanto individualmente como em conjunto;

  e) Os controlos existentes e a eficácia com que eles reduzem as vulnerabilidades;

No caso do **MDPSIOS**, para dar cumprimento a este ponto a metodologia MARSI, calcula o nível de probabilidade (NP), que é em função das medidas preventivas existentes (controlos), isto é nível de deficiência (ND) e do nível de exposição (NE) do ativo ao risco, expresso num produto de ambos os termos (ND x NE). Conforme descrito na apresentação do método, nos anexos I.1, I.2 e I.3 (página 250 a 251).

[27] Página 5 da norma ISO/IEC 27001 [8].

- Estimativa do nível de risco

> Recomenda-se, que o nível de risco seja estimado para todos os cenários de incidentes considerados relevantes (secção 4.2.1 e) 3) da norma ISO/IEC 27001[28]).
>
> A estimativa de riscos designa valores para a probabilidade e para as consequências de um risco. Esses valores podem ser de natureza quantitativa ou qualitativa. A estimativa de riscos é baseada nas consequências e na probabilidade estimadas. Além disso, ela pode considerar o custo-benefício, as preocupações das partes interessadas e outras variáveis, conforme apropriado para a avaliação de riscos. O risco estimado é uma combinação entre a probabilidade de um cenário de incidente e suas consequências.

No caso do **MDPSIOS**, para dar cumprimento a este ponto a metodologia MARSI, calcula o nível de risco (NR), que é o resultado do produto do nível de probabilidade (NP) pelo nível de Severidade/consequências (NS). Conforme descrito na apresentação do método nos anexos I.3, I.4 e I.5 (página 251 a 252).

Nível de Risco (NR) = Nível Probabilidade (NP) x Nível Severidade (NS)

O modelo criado para o MDPSIOS está desenvolvido e implementado em Excel avançado, onde está formalmente suportado todo este processo de Analise/Avaliação de Risco para determinação da estimativa de risco, conforme se pode verificar em anexo F.9 – (Avaliação de Riscos / Definição de Controlos – Global), página 186.

- Avaliação de riscos:

> Recomenda-se que o nível dos riscos seja comparado com os critérios de avaliação de riscos e com os critérios para a aceitação do risco (secção 4.2.1 e) 4) da norma ISO/IEC 27001[28]).
>
> A natureza das decisões relativas à avaliação de riscos e os critérios de avaliação de riscos que devem ser utilizadas para tomar essas decisões teriam sido decididas durante a definição do contexto. Recomenda-se que essas decisões e o contexto sejam revistos detalhadamente neste estágio em que se conhece mais sobre os riscos identificados.

[28] Página 5 da norma ISO/IEC 27001 [8].

Para avaliar os riscos, recomenda-se que as organizações comparem os riscos estimados com os critérios de avaliação de riscos considerados durante a definição do contexto.

As decisões tomadas durante a atividade de avaliação de riscos são baseadas principalmente no nível de risco aceitável. No entanto, convém que as consequências, a probabilidade e o grau de confiança na identificação e análise de riscos também sejam consideradas. A agregação de vários pequenos ou médios riscos pode resultar num risco total mais significativo e que poderá precisar de ser tratada adequadamente.

A avaliação de riscos utiliza o entendimento do risco obtido através da análise de riscos para tomada de decisões sobre ações futuras. Durante esta etapa, para além dos riscos estimados, convém que requisitos contratuais, legais e regulatórios também sejam considerados.

Deste ponto recomenda-se que deve sai uma lista de riscos ordenados por prioridade (de acordo com os critérios de avaliação de riscos) e associados aos cenários de incidentes que os provocam.

No caso do **MDPSIOS**, para dar cumprimento a este ponto a metodologia MARSI, da análise da matriz de níveis de risco apresenta diferentes níveis de intervenção ou de controlo (NC) que dão uma orientação para implementação de programas de eliminação ou redução de riscos atendendo à avaliação do custo – eficácia. Conforme descrito na apresentação do método no anexo I.6, página 253.

5.2.2.3 **MDPSIOS** - tratamento do risco de segurança da informação

Descrição geral do processo de tratamento do risco de segurança da informação exemplificado na figura 28. É de boa prática, que os controlos para reduzir, reter, evitar ou transferir os riscos sejam selecionados e o plano de tratamento do risco seja definido.

Existem quatro opções disponíveis para o tratamento do risco: redução do risco, retenção do risco, evitar o risco e transferência do risco [65][23][69].

- Redução do risco:

É aconselhado, que o nível de risco seja reduzido através da seleção de controlos, para que o risco residual possa ser reavaliado e então considerado aceitável.

Recomenda-se, que controlos apropriados e devidamente justificados sejam selecionados para satisfazer os requisitos identificados através da análise/avaliação de riscos e do tratamento dos mesmos. Convém que essa escolha tenha em conta os critérios para a aceitação do risco assim como requisitos legais, regulatórios e contratuais. Convém que essa seleção também tenha em conta custos e prazos para a implementação de controlos, além de aspetos técnicos, culturais e ambientais. Com frequência, é possível diminuir o custo total de propriedade de um sistema por meio de controlos de segurança da informação devidamente selecionados.

Durante a seleção de controlos, é importante pesar o custo da aquisição, implementação, administração, operação, monitorização e manutenção dos controlos em relação ao valor dos ativos protegidos. Além disso, convém que o retorno do investimento, na forma da redução do risco e da possibilidade de se explorar novas oportunidades de negócio em função da existência de certos controlos, também seja considerado.

Adicionalmente, convém considerar as competências especializadas que possam ser necessárias para definir e implementar novos controlos ou modificar os existentes.

É aconselhado, que as várias restrições (tais como: técnicas, temporais, financeiras, operacionais etc.) sejam consideradas durante a escolha e a implementação de controlos.

- Retenção do risco:

  É de boa prática que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos.

  Se o nível de risco está de acordo com os critérios para a aceitação[29] do risco, não há necessidade de se implementar controlos adicionais e pode haver a retenção do risco.

- Evitar o risco:

[29] "Aceitar o risco consciente e objetivamente, desde de que satisfaçam claramente às políticas da Organização e aos critérios de aceitação de riscos (ver 4.2.1c) 2)) ", refere à ISO/IEC 27001 4.2.1 f 2).

Recomenda-se que a atividade ou condição que dá origem a um determinado risco seja evitada.

Quando os riscos identificados são considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco excederem os benefícios, poderá decidir-se em evitar completamente o risco, através da eliminação de uma atividade planeada ou existente (ou de um conjunto de atividades), ou então através de mudanças nas condições em que a operação da atividade ocorre.

- Transferência do risco:

  É de boa prática, que um determinado risco seja transferido para outra entidade que possa gerir de forma mais eficaz, dependendo da avaliação de riscos.

Convém que as opções do tratamento do risco sejam selecionadas com base no resultado da análise/avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.

Quando uma grande redução do risco envolve uma despesa relativamente pequena propõe-se que seja efetuada. Quando existirem opções de melhoria que são muito dispendiosas, deve ser feita uma análise específica para justificar a sua implementação.

De um modo geral, recomenda-se que as consequências adversas do risco sejam reduzidas ao mínimo possível, independentemente de quaisquer critérios absolutos.

As quatro opções para tratamento do risco não são mutuamente exclusivas. Às vezes, a organização pode beneficiar substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e a transferência ou retenção dos riscos residuais.

É aconselhado, que um plano de tratamento do risco seja definido, identificando claramente a ordem de prioridade em que as formas específicas de tratamento do risco devem ser implementadas, assim como os seus prazos de execução. As prioridades podem ser estabelecidas utilizando algumas técnicas, incluindo a ordenação dos riscos e a análise de custo-benefício. É da responsabilidade dos gestores da organização equilibrar os custos da implementação dos controlos e o orçamento.

A definição do contexto (Critérios de avaliação de riscos) deve fornecer informações sobre requisitos legais e de regulação com os quais a organização deve estar em conformidade. Nesse caso, se o risco para organização é não estar em conformidade,

recomenda-se que sejam implementadas opções de tratamento para limitar essa possibilidade.

É de boa prática, que todas as restrições (organizacionais, técnicas, estruturais etc.) identificadas durante a atividade de definição do contexto, sejam tidas em conta durante o tratamento do risco.

Propõe-se, igualmente, que depois de estar definido o plano de tratamento do risco, os riscos residuais sejam determinados. Esta tarefa envolve uma atualização ou uma repetição da análise/avaliação de riscos, considerando-se os efeitos previstos do tratamento do risco que foi proposto. Caso o risco residual ainda não satisfaça os critérios para a aceitação do risco para a organização, uma nova iteração do tratamento do risco pode ser necessária antes de se prosseguir ou chegar a aceitação do risco.

Deste ponto, deve sair o plano de tratamento do risco e os riscos residuais sujeitos à decisão de aceitação por parte dos gestores da organização.

No caso do **MDPSIOS** a actividade de tratamento de riscos é baseada nos pressupostos descritos nesta secção, e obedece à estrutura funcional representada na figura 28. Esta actividade é suportada formalmente pelos seguintes documentos em anexo:

Anexo F.7 – (Documento de Analise / Avaliação / Monitorização do Risco), página 183;
Anexo F.8 – (Documento de Apoio ao Tratamento do Risco), página 185.

Em cada um dos campos que constitui cada um destes documentos, está especificada a sua finalidade e contexto.

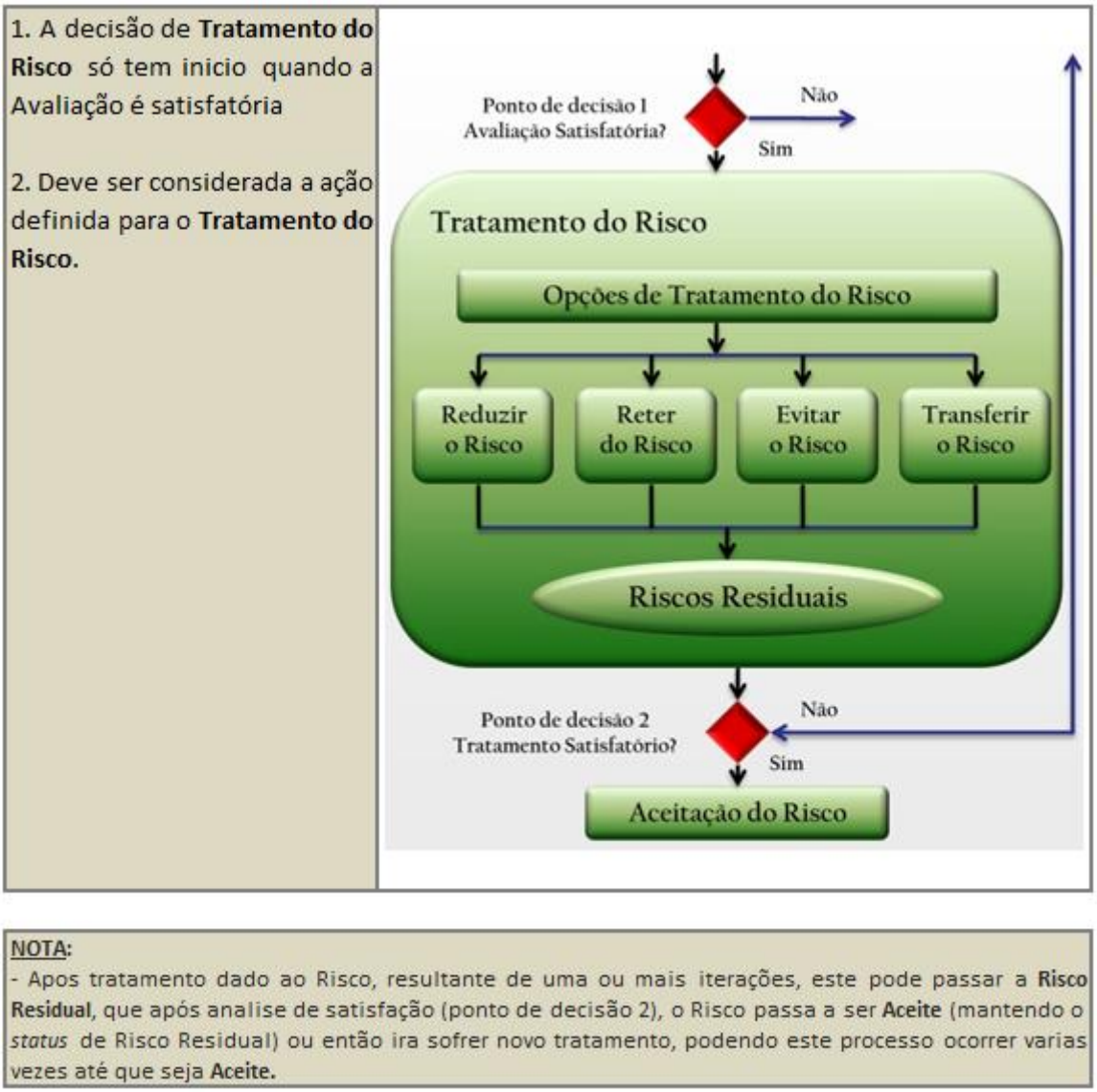


figura 28: - Estrutura funcional do tratamento de risco [51][58].

5.2.2.4 **MDPSIOS** - aceitação do risco de segurança da informação

É aconselhado que a decisão de aceitar os riscos seja feita e formalmente registada, juntamente com a responsabilidade pela decisão ((secção 4.2.1 h) da norma ISO/IEC 27001[30]).

Convém que os planos de tratamento do risco descrevam como os riscos avaliados devem ser tratados para que os critérios de aceitação do risco sejam respeitados ou satisfatórios. É importante que gestores responsáveis façam uma análise crítica e aprovem, se for o caso,

[30] Página 6 da norma ISO/IEC 27001 [8].

os planos propostos de tratamento do risco, os riscos residuais resultantes e que registem as condições associadas a essa aprovação.

Os critérios para a aceitação do risco podem ser mais complexos do que somente a determinação, se o risco residual está, ou não, abaixo ou acima de um limite bem definido.

Em alguns casos, o nível de risco residual pode não satisfazer os critérios de aceitação do risco, pois os critérios aplicados não têm em conta as circunstâncias predominantes no momento. Por exemplo, pode ser válido argumentar a necessidade de se aceitar o risco, porque os benefícios que acompanham essa decisão são mais atraentes ou porque os custos da sua redução são demasiadamente elevados. Tais circunstâncias indicam que os critérios para aceitação do risco são inadequados e convêm que sejam revistos, se possível. No entanto, nem sempre é possível rever os critérios para aceitação do risco em tempo útil. Nesses casos, os gestores terão que aceitar riscos que não satisfaçam os critérios normais para a aceitação. Se isso for necessário, convém que o gestor comente explicitamente sobre os riscos e inclua uma justificativa para a sua decisão de passar por cima dos critérios normais para a aceitação do risco.

No caso do **MDPSIOS**, para dar cumprimento a este ponto e também por forma a otimizar a documentação e facilitar a visualização de vários aspetos num único documento, o mesmo é suportado formalmente pelos seguintes documentos em anexo:

> Anexo F.7 – (Documento de Analise / Avaliação / Monitorização do Risco), página 183;
> Anexo F.8 – (Documento de Apoio ao Tratamento do Risco), página 185.

Em cada um dos campos que constitui cada um destes documentos, está especificada a sua finalidade e contexto.

5.2.2.5 **MDPSIOS** - comunicação do risco de segurança da informação

Recomenda-se que as informações sobre riscos sejam trocadas e/ou compartilhadas entre quem toma a decisão e as outras partes interessadas.

A comunicação do risco é uma atividade que tem por objetivo alcançar um consenso sobre a maneira mais adequada de gerir os riscos, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os gestores e as outras partes envolvidas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitação dos riscos.

A comunicação eficaz entre as partes envolvidas é importante, uma vez que a mesma pode ter um impacto significativo sobre as decisões que devem ser tomadas. A comunicação assegurará que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito, tenham um bom entendimento sobre as decisões que são tomadas e os motivos que tornam certas ações necessárias. A comunicação tem de ser bidirecional.

É particularmente importante garantir que a perceção do risco das partes envolvidas, bem como a perceção dos benefícios, sejam identificadas e documentadas e que as razões subjacentes sejam claramente entendidas e consideradas.

A coordenação entre os principais gestores e as partes envolvidas pode ser obtida mediante a formação de uma comissão em que os riscos, a sua priorização, as formas adequadas de tratá-los e a sua aceitação possam ser amplamente discutidos.

É importante a cooperação com o as relações públicas ou com o grupo de comunicação dentro da organização para coordenar as tarefas relacionadas com a comunicação do risco. Esta cooperação é vital no caso de ações de comunicação durante crises, por exemplo: em resposta a incidentes específicos.

No caso do **MDPSIOS**, para formalizar este ponto, deve ser utilizado o documento que se encontra no anexo F.1 - (Documento Padrão), página 174.

5.2.2.6 **MDPSIOS** - monitorização e análise crítica do risco

- Monitorização e análise crítica dos fatores de risco:

  É de boa prática, que os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorizados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

  Os riscos não são estáticos. As ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar abruptamente, sem qualquer indicação. Portanto, a monitorização constante é necessário para que se detetem essas mudanças. Serviços de terceiros que forneçam informações sobre novas ameaças ou vulnerabilidades podem prestar uma valiosa ajuda.

  É aconselhado, que as organizações assegurem que os seguintes itens sejam monitorizados continuamente:

a) Novos ativos que tenham sido incluídos no objetivo da gestão de riscos;

b) Modificações necessárias dos valores dos ativos, por exemplo: devido à mudança nos requisitos de negócio;

c) Novas ameaças que podem estar ativas tanto fora como dentro da organização e que não tenham sido avaliadas;

d) A possibilidade de que vulnerabilidades novas ou ampliadas venham a permitir que alguma ameaça as possa explorar;

e) Vulnerabilidades já identificadas, para determinar aquelas que estão a ficar mais expostas a ameaças novas ou a ressurgir;

f) As consequências ou impacto ampliado de ameaças, vulnerabilidades e riscos avaliados em conjunto – analisadas em um todo, e que resultem um nível inaceitável de risco;

g) Incidentes relacionados com a segurança da informação.

É de boa prática, que não só as atividades de monitorização de riscos sejam regularmente repetidas, mas também as opções selecionadas para o tratamento do risco sejam periodicamente revistas.

O resultado da atividade de monitoramento de riscos pode fornecer os dados de entrada para as atividades de análise crítica. É aconselhado, que a organização analise crítica e regularmente todos os riscos e sempre que ocorram grandes mudanças (secção 4.2.3) da norma ISO/IEC 27001[31]).

No caso do **MDPSIOS**, para dar cumprimento a este ponto e também por forma a otimizar a documentação e facilitar a visualização de vários aspetos num único documento, o mesmo é suportado formalmente pelos seguintes documentos em anexo:

Anexo F.7 – (Documento de Analise / Avaliação / Monitorização do Risco), página 183;
Anexo F.9 – (Avaliação de Risco / Definição de Controlos – Global), página 186.

Em cada um dos campos que constitui cada um destes documentos, está especificada a sua finalidade e contexto.

Recomenda-se, o recurso a esta parte na aplicação criada para o MDPSIOS, sempre que seja necessário efetuar uma nova analise/avaliação de risco.

[31] Página 7 da norma ISO/IEC 27001 [8]

- Monitorização e análise crítica e melhoria do processo de gestão de risco.

  É de boa prática, que o processo de gestão de riscos de segurança da informação seja continuamente monitorizado, analisado criticamente e melhorado quando for necessário e apropriado.

  A monitorização cotidiana e a análise crítica são necessários para assegurar que o contexto, o resultado da análise/avaliação de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados às circunstâncias.

  É aconselhado, que a organização se certifique que o processo de gestão de riscos de segurança da informação e as suas atividades permanecem apropriadas as circunstâncias presentes e devidamente acompanhadas.

  É importante que a organização verifique regularmente se os critérios utilizados para medir o risco e os seus elementos ainda são válidos e consistentes com os objetivos do negócio, estratégia e políticas e se as mudanças no contexto do negócio são adequadamente consideradas durante o processo de gestão de riscos de segurança da informação.

  Recomenda-se que a organização assegure que os recursos necessários para a análise/avaliação de riscos e o tratamento dos mesmos estejam sempre disponíveis para rever os riscos, para lidar com ameaças ou vulnerabilidades novas ou alteradas e para aconselhar a direção da melhor forma possível.

  Convém que esta atividade de monitorização e análise crítica lide com (mas não seja limitada ao(s)): Contexto legal e do ambiente, Contexto da concorrência, Método de análise/avaliação de riscos, Valor e as categorias dos ativos, Critérios de impacto, Critérios para a avaliação de riscos, Critérios para a aceitação do risco, Custo total de propriedade e Recursos necessários.

  A monitorização da gestão de riscos pode resultar em modificação ou acréscimo da abordagem, metodologia ou ferramentas utilizadas, dependendo:

  a) Das mudanças identificadas;

  b) Da iteração da análise/avaliação de riscos;

  c) Do objetivo do processo de gestão de riscos de segurança da informação (por exemplo: a continuidade de negócio, a resiliência diante dos incidentes, a conformidade);

d) Do objeto de interesse do processo de gestão de riscos de segurança da informação (por exemplo: a organização, a unidade de negócios, o sistema de informação, a sua implementação técnica, a aplicação, a conexão à Internet).

No caso do **MDPSIOS**, para dar cumprimento a este e também por forma a otimizar a documentação e facilitar a visualização de vários aspetos num único documento, o mesmo é suportado formalmente pelos seguintes documentos em anexo:

Anexo F.7 – (Documento de Analise / Avaliação / Monitorização do Risco), página 183;
Anexo F.9 – (Avaliação de Risco / Definição de Controlos – Global), página 186.

Em cada um dos campos que constitui cada um destes documentos, está especificada a sua finalidade e contexto.

Recomenda-se o recurso a esta parte na aplicação criada para o MDPSIOS, sempre que seja necessário efetuar uma nova analise/avaliação de risco.

Este recurso no MDPSIOS, disponibiliza quatro estatísticas (indicadores) em forma de gráficos de monitorização, figura 29 e figura 30.

Estes indicadores para além da monitorização para acompanhamento do processo de implementação, permitem aferir o resultado das decisões, medidas ou controlos implementados relativamente a cada iteração do processo SGSI e desta forma promover melhorias ao processo. Estes disponibilizam a seguinte informação ou resultados:

- Total de Ativos por Nível de Risco:
  Permite visualizar qual é a distribuição de ativos por nível de risco, numa escala de Muito Baixo a Muito Alto.

- Nível de controlo (NC) por Ativo:
  Permite visualizar e aferir qual é o nível de controlo atual de cada um dos Ativos numa escala de 1 a 5, sendo que o ideal seria ter os Ativos todos no nível 5.

- Estado provável de Insegurança / Segurança:
  É uma estimativa meramente indicativa para uma perceção imediata da situação, em que o estado provável de insegurança resulta da percentagem de Ativos posicionados entre o nível de risco, Alto e Muito Alto, e o estado provável de segurança entre o nível de risco Muito Baixo, Baixo e Médio.

Consoante o resultado apresentado pode necessitar de uma avaliação mais profunda.

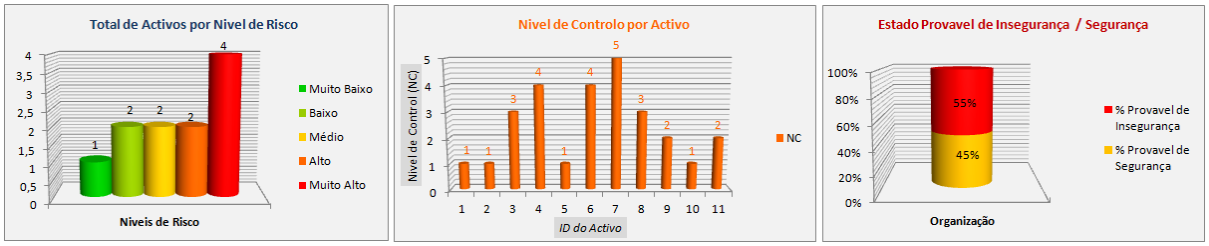
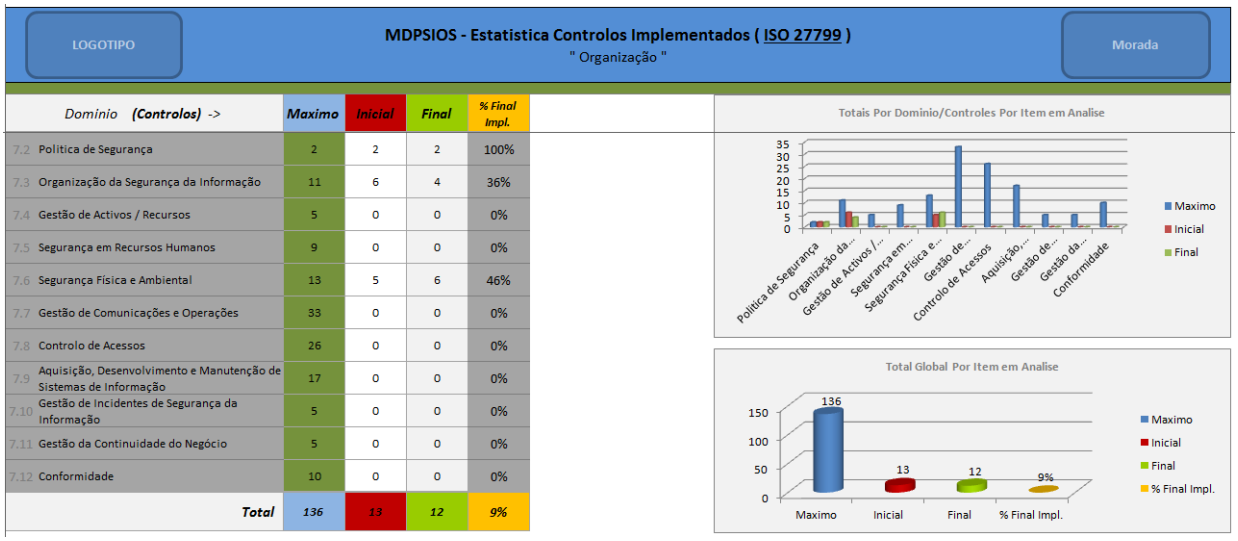


figura 29: - MDPSIOS - Gráficos de monitorização “Indicadores de estimativa de risco”.

- Estatística de Controlos Implementados (norma ISO 27799), figura 30[32] :

  Este indicador permite a visualização imediata e simples de todos os controlos implementados até ao momento (coluna “Final”), os controlos considerados no estado inicial (coluna “Inicial”) e a % de controlos implementados até ao momento relativamente ao máximo de controlos da norma. Este indicador ao ser cruzado com valores de possíveis incidentes permite aferir se as medidas implementadas estão a ser eficazes ou não.

  O MDPSIS disponibiliza também um gráfico idêntico para o caso da implementação da noma ISO 27002.



Dominio (Controlos) ->	Maximo	Inicial	Final	% Final Impl.
7.2 Politica de Segurança	2	2	2	100%
7.3 Organização da Segurança da Informação	11	6	4	36%
7.4 Gestão de Activos / Recursos	5	0	0	0%
7.5 Segurança em Recursos Humanos	9	0	0	0%
7.6 Segurança Física e Ambiental	13	5	6	46%
7.7 Gestão de Comunicações e Operações	33	0	0	0%
7.8 Controlo de Acessos	26	0	0	0%
7.9 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	17	0	0	0%
7.10 Gestão de Incidentes de Segurança da Informação	5	0	0	0%
7.11 Gestão da Continuidade do Negócio	5	0	0	0%
7.12 Conformidade	10	0	0	0%
Total	136	13	12	9%

figura 30: - MDPSIOS – Estatística Controlos Implementados

[32] Figura com maior resolução no anexo F.13 – (Estatística Controlos Implementados), página 190.

5.3 Conclusão

Como indiscutivelmente a melhoria das condições de segurança da informação consiste nas estratégias a definir e a aplicar perante as situações de risco que surgem a partir de vulnerabilidades que podem ser exploradas por ameaças, é importante conhecê-las de modo a que seja possível realizar uma gestão de risco adequada perante o possível impacto ou consequências que a concretização dessas ameaças podem representar para a organização. Assim, a utilização de processos, metodologias e ferramentas adequadas na gestão de risco da segurança da informação é um trunfo muito importante e estratégico a ter em conta num SGSI que se queria implementar numa organização.

O modelo documental MDPSIOS, para resolver este problema usa como modelo para Gestão de Risco a norma ISO/IEC 27005:2008, e como metodologia para a Estimativa de Risco o Método simplificado quantitativo de Avaliação de Riscos de Segurança da Informação (MARSI), de acordo com o que foi apresentado ao longo deste capítulo.

Capítulo 6 - DEFINIÇÃO DO MODELO DOCUMENTAL

Para implementar um SGSI desenvolveu-se um sistema baseado na arquitetura apresentada no capítulo anterior, modelo MDPSIOS. Esta solução tem como objetivo principal, criar um modelo documental que permita a implementação de políticas de segurança da informação através da adoção de um SGSI, cumprindo com as seguintes características e pressupostos:

- Simplificar a implementação de um sistema de SGSI baseando-se na metodologia das normas ISO/IEC 27001, sem fins de certificação numa primeira fase;
- Utilizar a metodologia e as boas práticas disponibilizadas pelas normas ISO/IEC 27002 para qualquer organização e a norma ISO/IEC 27799 para as organizações de saúde;
- Utilizar a metodologia de análise/avaliação de risco disponibilizada pela norma ISO/IEC 27005;
- Utilizar na estimativa de risco uma metodologia simples, acessível, flexível e de linguagem minimamente percetível a todos os possíveis intervenientes no processo sem fugir do objetivo e rigor que este item requer (avaliação da estimativa de risco);
- Disponibilizar documentação mínima para formalização dos processos;
- Fácil instalação, utilização e gestão flexível da informação (emissão de relatórios);
- Utilização de recursos internos na implementação do modelo documental;
- Utilização individual (monoposto);
- Robustez funcional e operacional;
- Manutenção facilitada;
- Interface agradável e intuitivo;
- Segurança (minimamente segura em termos de acessos);
- Outros aspetos a ter em conta durante a realização do trabalho.

Para a implementação, foi escolhido o Microsoft Excel para desenvolver o primeiro protótipo.

A escolha do Microsoft Excel como plataforma base para a aplicação proposta teve como pressuposto ser um *software* amplamente disponível e difundido, que não requer grandes conhecimentos para o seu uso, e que a grande maioria dos potenciais utilizadores da aplicação possuirá. De facto, apesar do Excel ser uma ferramenta paga, existem várias aplicações semelhantes, de uso gratuito, que permitem uma utilização completa dos mesmos recursos e funcionalidades. Além disso, a dependência tecnológica do modelo desenvolvido acaba por ser apenas esse *software* instalado num qualquer computador de secretária, portátil ou até num *tablet*. Desta forma, evita-se a dependência de comunicações móveis ou de rede para ter a aplicação funcional, pois assenta no conceito "*stand-alone*", no qual tanto a aplicação como os dados por ela armazenados estão todos contidos num só ficheiro, que pode ser facilmente transportado e utilizado.

Claro que esta opção tem desvantagens do ponto de vista da segurança dos dados, cabendo ao utilizador estar consciente dessa limitação, devendo aplicar as medidas de proteção necessárias para estas situações prevista na política de segurança da organização.

6.1 Descrição Genérica e Organização Interna

O protótipo desenvolvido apresenta um conjunto de funcionalidades e características relacionadas com o domínio ao qual o mesmo pertence, mas que de uma forma rápida, simples, intuitiva e apelativa ofereça todo um conjunto de informações e facilidades que permitam a qualquer utilizador navegar com facilidade pela aplicação e que possibilitem a inserção de dados e a execução das diversas etapas envolvidas nos diferentes passos a realizar. Conforme representado no anexo F.14 – (MDPSIOS - Estrutura Funcional da Aplicação), página 191.

Deste modo o modelo assenta sobre a normativa ISO/IEC 27001, conforme se pode verificar no menu de entrada, figura 31[33].

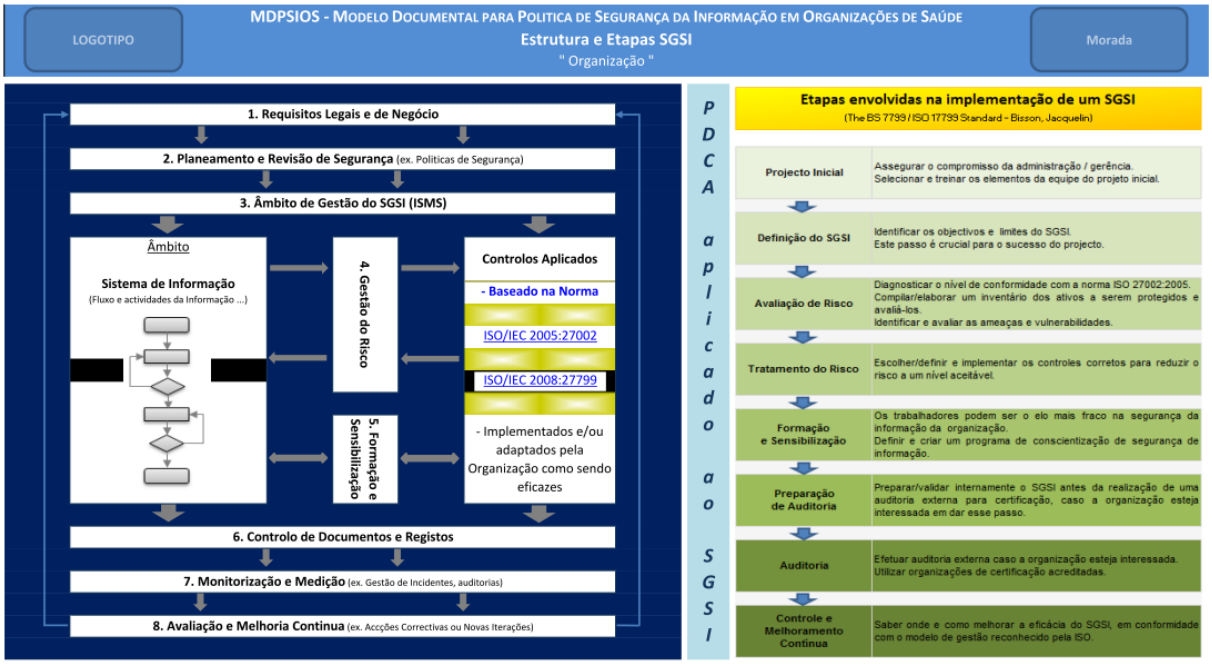


figura 31: - MDPSIOS – Estrutura e Etapas SGSI

No menu de entrada (figura 31) é apresentado ao utilizador o menu principal do MDPSIOS, onde pode-se verificar na parte esquerda as fases envolvidas na implementação de um SGSI, ao centro, o *link* de acesso a informação relacionada com a metodologia PDCA associada e na parte direita, informação sobre as etapas envolvidas na implementação de um SGSI.

[33] Figura com maior resolução no anexo F.15 – (MDPSIOS – Estrutura e Etapas SGSI), página 193.

Está também disponíveis a partir deste menu o acesso a todas as funções que permitem a implementação e gestão do SGSI, conferindo desta forma a centralização do processo a partir deste menu (estrutura do lado esquerdo).

Os *links* existentes neste menu, permitem a navegação para as seguintes funcionalidades do modelo (nestas opções estão definidos e identificados os respetivos documentos a utilizar em cada um dos processos principais):

1. Requisitos Legais e de Negócio
2. Planeamento e Revisão de Segurança
3. Âmbito de Gestão do SGSI
4. Gestão de Risco (totalmente desenvolvida no capitulo 5 deste documento)
5. Formação e Sensibilização
6. Controlo de Documentos e Registos
7. Monitorização e Medição
8. Avaliação e Melhoria Continua

Outros *link's* existentes neste menu:

- *Link* referente a caraterização de um Sistema de Informação e consequente acesso ao documento de inventario de ativos.
- *Link* direto a configuração dos controlos disponibilizados que poderão ser implementados em resposta a analise/avaliação de risco, após decisão do tratamento a dar ao risco:
    - Norma ISO/IEC 27002
    - Norma ISO/IEC 27799

6.1.1 1.Requisitos Legais e de Negócio

Esta opção permite formalmente através do documento, figura 32 (anexo F.16, página 194), definir a finalidade e os limites do SGSI nos termos das características do negócio, da organização, da sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões (secção 1.2 da Norma ISO/IEC 27001[34]).

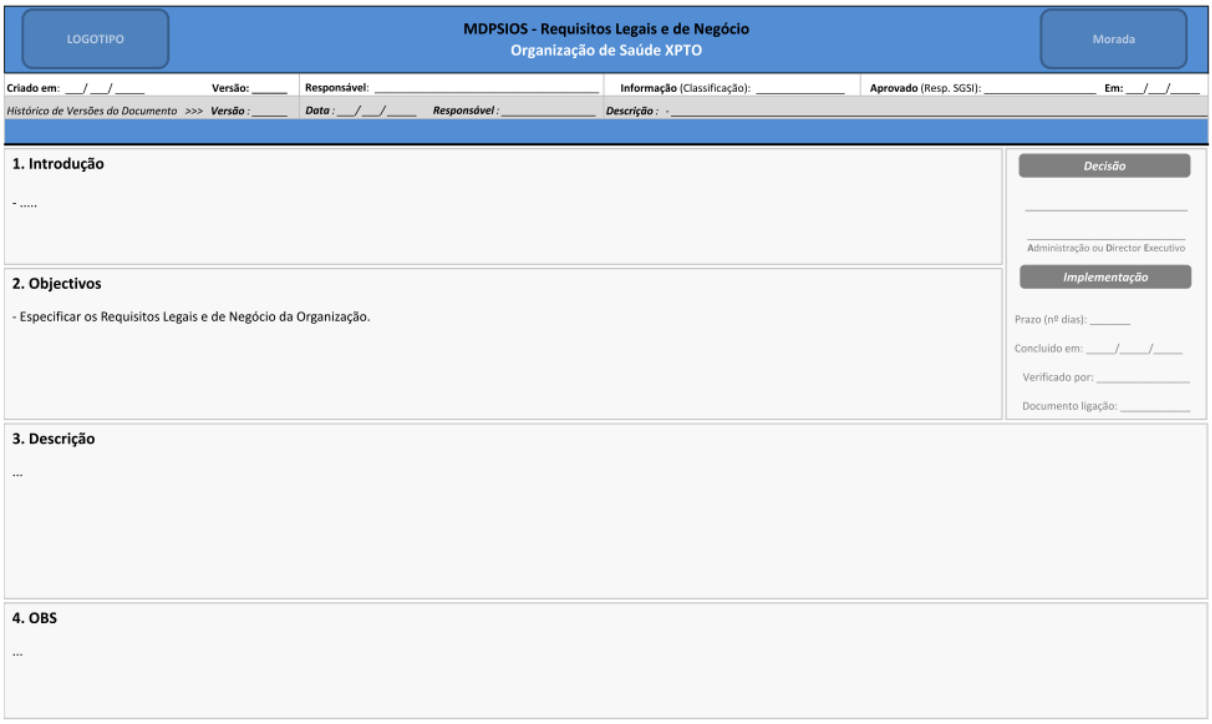


figura 32: - MDPSIOS – Requisitos Legais e de Negócio

6.1.2 2.Planeamento e Revisão da segurança

Esta opção permite formalmente através do documento, figura 33 (anexo F.17, página 195), definir uma política do SGSI nos termos das características do negócio, da organização, da sua localização, ativos e tecnologia que, [8]:

- Inclua uma estrutura para definir objetivos e estabeleça um rumo global e princípios para ações relacionadas com a segurança da informação;
- Considere requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;

[34] Página 1 da norma ISO/IEC 27001 [8].

- Esteja alinhada com o contexto estratégico de gestão de riscos da organização sobre o qual será estabelecido e mantido o SGSI;
- Estabeleça critérios em relação aos quais os riscos devem ser avaliados (secção 4.2.1c) e capitulo 5, da norma ISO/IEC 27001[35]) e que tenham sido aprovados pela direção.

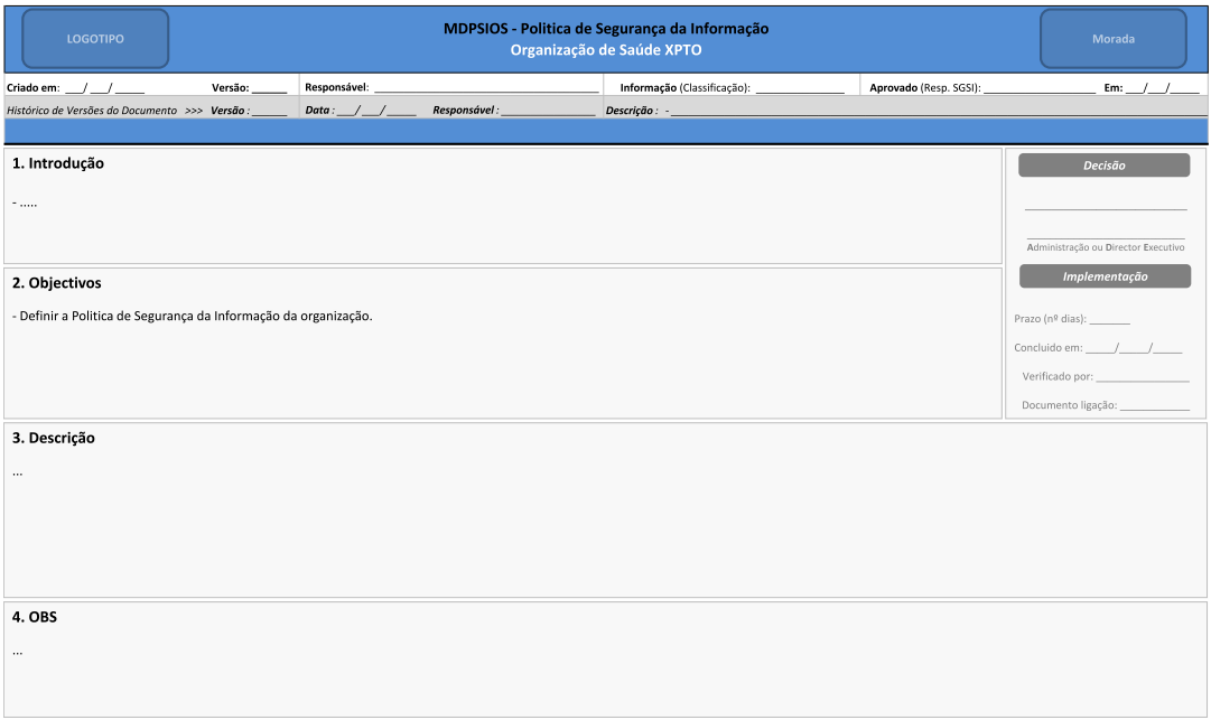


figura 33: - MDPSIOS – Politica da Segurança da Informação

6.1.3 3.Âmbito da Gestão do SGSI

Esta opção permite formalmente através do documento figura 34 (anexo F.18, página 196), definir de forma específica, situações em que seja necessário uma descrição mais detalhada da gestão ou dos processos do SGSI.

[35] Página 4 e 9 da norma ISO/IEC 27001 [8].

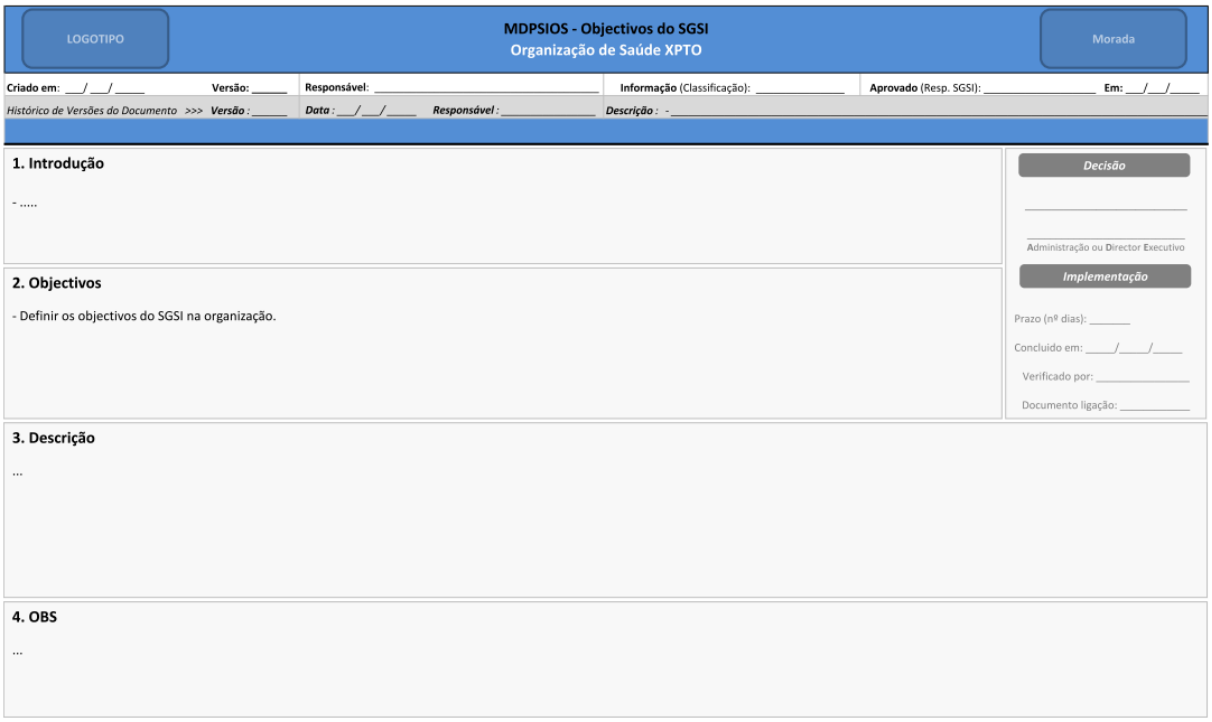


figura 34: - MDPSIOS – Objetivos do SGSI

6.1.4 4.Gestão de Risco

Esta opção permite formalmente através do documento figura 35 (anexo F.9, página 186), definir de forma específica, a abordagem de análise/avaliação de riscos da organização.

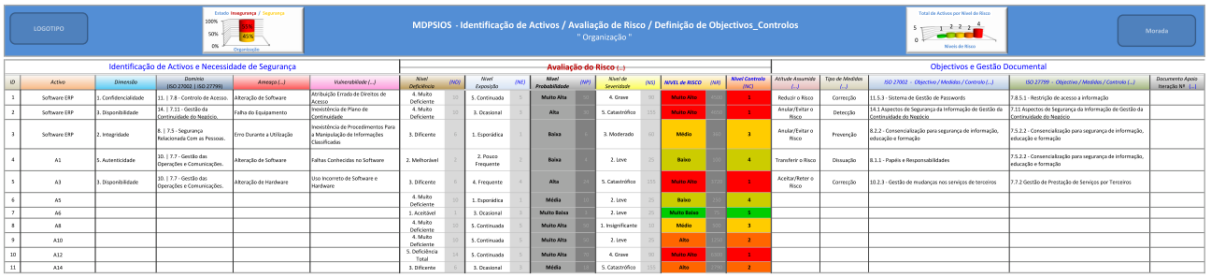


figura 35: - MDPSIOS – Avaliação de Risco / Definição de Controlos - Global

A conceção deste documento baseou-se nos seguintes critérios definidos pela norma ISO/IEC 27001 [8]:

- Identificar uma metodologia de análise/avaliação de riscos que seja adequada ao SGSI e aos requisitos legais, regulamentares e de segurança da informação, identificados para o negócio.

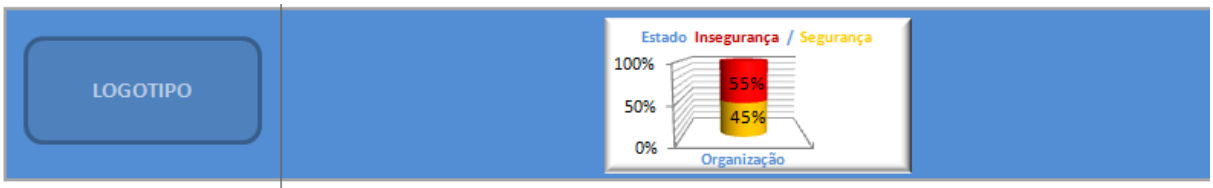
- Desenvolver critérios para a aceitação de riscos e identificar os níveis aceitáveis de risco (secção 5.1.f da norma ISO/IEC 27001[36]).
- A metodologia de análise/avaliação de riscos selecionada deve assegurar que as análises/avaliações de riscos produzam resultados comparáveis e reproduzíveis.

A escolha da metodologia e toda a sua adoção e adaptação para o MDPSIOS está totalmente desenvolvida no capítulo 5 deste documento.

Neste documento estão integradas três áreas/sectores que dependem sempre da conclusão ou preenchimento da anterior:

1ª área: - Identificação dos Ativos e Necessidade de Segurança

Implementa a secção 4.2.1 d) da Norma ISO/IEC 27001[37] - Identificar os riscos, conforme exemplo figura 36 (anexo F.10, página 187).



Identificação de Activos e Necessidade de Segurança

ID	Activo	Dimensão	Dominio (ISO 27002 | ISO 27799)	Ameaça (...)	Vulnerabiliade (...)
1	Software ERP	1. Confidencialidade	11. | 7.8 - Controlo de Acesso.	Alteração de Software	Atribuição Errada de Direitos de Acesso
2	Software ERP	3. Disponibilidade	14. | 7.11 - Gestão da Continuidade do Negócio.	Falha do Equipamento	Inexistência de Plano de Continuidade
3	Software ERP	2. Integridade	8. | 7.5 - Segurança Relacionada Com as Pessoas.	Erro Durante a Utilização	Inexistência de Procedimentos Para a Manipulação de Informações Classificadas
4	A1	5. Autenticidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Software	Falhas Conhecidas no Software
5	A3	3. Disponibilidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Hardware	Uso Incorreto de Software e Hardware
6	A5				
7	A6				
8	A8				
9	A10				
10	A12				
11	A14				

figura 36: - MDPSIOS – Identificação de Ativos e Necessidade de Segurança

Esta figura representa a primeira área do documento global, e permite:

[36] Página 9 da norma ISO/IEC 27001 [8]
[37] Página 4 da norma ISO/IEC 27001 [8]

- Identificar os ativos dentro do objetivo do SGSI e os proprietários[38] destes ativos. Esta identificação resulta da utilização do documento do Anexo F.2 (MDPSIOS - Documento Inventário de Ativos), página 175.
- Identificar os impactos que as perdas de confidencialidade, integridade, disponibilidade e outras dimensões podem causar aos ativos.
- Identificar o Domínio/Cláusula de controlo a considerar para o ativo em causa:
    - Conforme anexo G (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27002 [23]), página 200:
        - 5. – Política de Segurança;
        - 6. – Organização da Segurança da Informação;
        - 7. – Classificação e Controlo de Ativos de Informação;
        - 8. – Segurança em Recursos Humanos;
        - 9. – Segurança Física e Ambiental;
        - 10. – Gestão das Operações e Comunicações;
        - 11. – Controlo de Acesso;
        - 12. – Desenvolvimento e Manutenção de Sistemas;
        - 13. – Gestão de Incidentes de Segurança;
        - 14. – Gestão da Continuidade do Negócio;
        - 15. – Conformidade.
    - Conforme anexo H (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27799 [69]), página 222:
        - 7.2 – Política de Segurança;
        - 7.3 – Organização da Segurança da Informação;
        - 7.4 – Classificação e Controlo de Ativos de Informação;
        - 7.5 – Segurança em Recursos Humanos;
        - 7.6 – Segurança Física e Ambiental;
        - 7.7 – Gestão das Operações e Comunicações;
        - 7.8 – Controlo de Acesso;
        - 7.9 – Desenvolvimento e Manutenção de Sistemas;
        - 7.10 – Gestão de Incidentes de Segurança;
        - 7.11 – Gestão da Continuidade do Negócio;
        - 7.12 – Conformidade.

[38] O termo 'proprietário' neste caso identifica uma pessoa que tenha uma responsabilidade autorizada para controlar o processo, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. Não significa que a pessoa realmente tenha qualquer direito de propriedade sobre o ativo [8].

- Identificar as ameaças associadas aos ativos inventariados. Podendo utilizar o catálogo disponibilizado, conforme anexo F.3 (MDPSIOS - Catálogo de Ameaças mais Comuns “Tipo e Origem”), página 176, ou inserir novas que não constem do catálogo.

- Identificar as vulnerabilidades que podem ser exploradas pelas ameaças. Podendo utilizar o catálogo disponibilizado, conforme anexo F.4 (MDPSIOS - Catálogo de Vulnerabilidades mais Comuns “Tipo e Ex. Ameaças”), página 178, ou inserir novas que não constem do catálogo.

2ª área: - Avaliação de Risco

Implementa a secção 4.2.1 e) da Norma ISO/IEC 27001[39], – Analisar e Avaliar os riscos, conforme exemplo figura 37 (anexo F.11, página 188).

MDPSIOS - Identificação de Activos / Avaliação de Risco / Definição de Controlos

" Organização "

Avaliação do Risco (...)

Nivel Deficiência	(ND)	Nivel Exposição	(NE)	Nivel Probabilidade	(NP)	Nivel de Severidade	(NS)	NIVEL de RISCO	(NR)	Nivel Controlo (NC)
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	4. Grave	90	Muito Alto	4500	1
4. Muito Deficiente	10	3. Ocasional	3	Alta	30	5. Catastrófico	155	Muito Alto	4650	1
3. Dificente	6	1. Esporádica	1	Baixa	6	3. Moderado	60	Médio	360	3
2. Melhorável	2	2. Pouco Frequente	2	Baixa	4	2. Leve	25	Baixo	100	4
3. Dificente	6	4. Frequente	4	Alta	24	5. Catastrófico	155	Muito Alto	3720	1
4. Muito Deficiente	10	1. Esporádica	1	Média	10	2. Leve	25	Baixo	250	4
1. Aceitável	1	3. Ocasional	3	Muito Baixa	3	2. Leve	25	Muito Baixo	75	5
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	1. Insignificante	10	Médio	500	3
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	2. Leve	25	Alto	1250	2
5. Deficiência Total	14	5. Continuada	5	Muito Alta	70	4. Grave	90	Muito Alto	6300	1
3. Dificente	6	3. Ocasional	3	Média	18	5. Catastrófico	155	Alto	2790	2

figura 37: - MDPSIOS – Avaliação do Risco / Estimativa de Riscos

[39] Página 5 da norma ISO/IEC 27001 [8]

Esta figura representa a segunda área do documento global e permite:

- Avaliar os impactos na organização, que podem resultar de falhas de segurança, tendo em consideração as consequências de uma perda de confidencialidade, integridade, disponibilidade ou outra dimensão de segurança que deve ser considerada para os ativos em causa.
- Avaliar a probabilidade real da ocorrência de falhas de segurança, à luz de ameaças e vulnerabilidades prevalecentes, impactos associados a estes ativos e os controlos atualmente implementados.
- Estimar os níveis de riscos e controlo.
- Determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos (secção 4.2.1 c) 2 da norma ISO/IEC 27001[40]).

3ª área: - Objetivos e Gestão Documental

Implementa a secção 4.2.1 f) e g) da Norma ISO/IEC 27001[41] - Identificar e avaliar as opções para o tratamento de riscos, conforme exemplo figura 38 (anexo F.12, página 189).

[40] Página 4 da norma ISO/IEC 27001 [8]
[41] Página 5 da norma ISO/IEC 27001 [8]

Objectivos e Gestão Documental

Atitude Assumida (...)	Tipo de Medidas (...)	ISO 27002 - Objectivo / Medidas / Controlo (...)	ISO 27799 - Objectivo / Medidas / Controlo (...)	Documento Apoio Iteração Nº (...)
Reduzir o Risco	Correcção	11.5.3 - Sistema de Gestão de Passwords	7.8.5.1 - Restrição de acesso a informação	
Anular/Evitar o Risco	Detecção	14.1 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	7.11 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	
Anular/Evitar o Risco	Prevenção	8.2.2 - Consencialização para segurança de informação, educação e formação	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
Transferir o Risco	Dissuação	8.1.1 - Papéis e Responsabilidades	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
Aceitar/Reter o Risco	Correcção	10.2.3 - Gestão de mudanças nos serviços de terceiros	7.7.2 Gestão de Prestação de Serviços por Terceiros	

figura 38: - MDPSIOS – Medidas, Objetivos e Controlos

Esta figura representa a terceira área do documento global, e permite as seguintes ações:

- Aceitar o risco consciente e objetivamente, desde que satisfaçam claramente às políticas da organização e aos critérios de aceitação de riscos (secção 4.2.1 c) 2) da norma ISO/IEC 27001[42]);
- Reduzir, Evitar riscos; e ou
- Transferir os riscos associados ao negócio a outras partes, por exemplo, seguradoras e fornecedores;
- Atitude Assumir e Tipo de medidas; (anexo F.8 - MDPSIOS - Documento de Apoio ao Tratamento do Risco, página 185);
- Escolher os controlos apropriados a aplicar, consoante a norma a ser implementada, ISO 27002 e/ou ISO 27799;

- Preencher nº de iteração do processo SGSI associado ao Documento de Analise / Avaliação / Monitorização do Risco (anexo F.7, página 183) e do Documento de Apoio ao Tratamento do Risco (anexo F.8, página 185).

[42] Página 4 da norma ISO/IEC 27001 [8]

- Selecionar objetivos de controlo e controlos para o tratamento de riscos:
  - Objetivos de controlo e controlos devem ser selecionados e implementados para dar resposta aos requisitos identificados pela análise/avaliação de riscos e pelo processo de tratamento de riscos. Esta seleção deve considerar os critérios para aceitação de riscos (secção 4.2.1 c) 2) da norma ISO/IEC 27001[43]) como também os requisitos legais, regulamentares e contratuais.
  - Os objetivos de controlo e controlos do anexo G.1 a G.11 (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27002) ou anexo H.1 a H.11 (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27799), devem ser selecionados fazendo parte deste processo, como adequados para cobrir os requisitos identificados. A seleção dos objetivos de controlo de uma ou outra norma estará dependente da área em que a organização está inserida, sendo aconselhável para área de saúde a utilização dos objetivos de controlo da norma ISO/IEC 27799.
  - Os objetivos de controlo e controlos presentes nos anexos referidos no ponto anterior não são exaustivos, e objetivos de controlos e controlos adicionais podem ser também selecionados. É importante assegurar que nenhuma opção de controlo importante seja negligenciada ou esquecido, sendo estes anexos o ponto de partida para que tal seja evitado.

Obter aprovação da direção relativamente aos riscos residuais propostos e ou autorização da direção para implementar e operar o SGSI [8]:

- Secção 4.2.1 i) da Norma ISO/IEC 27001[44], implementado através da utilização do documento da figura 39 (anexo F.7 – MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco, página 183).

[43] Página 4 da norma ISO/IEC 27001 [8]
[44] Página 5 da norma ISO/IEC 27001 [8]


LOGOTIPO

MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco

" Organização "

Morada

DATA : ___/___/____ Versão: _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

Histórico do Documento >>> Versão: _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____

Documento AAM nº _____ | Iteração nº _____

Avaliação / Classificação

ID Activo: _____ Dimensão: _____

Norma: _____ Dominio(nº): _____ Secção (nº): _____

Risco não residual (%): _____ Risco Residual (%): _____

Questões ou Riscos identificados:

(As Questões ou Riscos identificados a colocar nesta caixa servem para detectar problemas de segurança da informação e determinar como implementar com sucesso o SGSI). Servirá também para orientação da Administração , Director Executivo ou Responsavel SGSI, na avaliação e decisão sobre as medidas a adoptar)

Decisão

Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: ___/___/___

Verificado por: _____

Documento ligação: _____

Considerações do responsável do SGSI:

(Nesta caixa devem ser colocadas as questões relevantes em termos de negócio que o responsável do SGSI deve ter como preocupação em relação a questão / risco acima colocado)

Fontes e/ou localização da Informação e/ou equipamentos:

(Nesta caixa deve ser colocada a fonte e/ou localização da informação e/ou equipamentos, que estejam dentro ou fora da organização para ajudar o responsável do SGSI na determinação da resposta ou medida relativamente a questão / risco acima colocado)

Critérios de Avaliação e Desempenho:

(Nesta caixa devem ser identificados os critérios que podem ser utilizados pelo responsavel do SGSI para determinar a eficácia da organização e/ou abordar os problemas de segurança em relação a questão / risco acima colocado)

Medidas a Implementar: (ver Documento de Apoio ao Tratamento do Risco)

(Nesta caixa deve-se descrever os passos que a organização deve seguir para fazer face as considerações e situações de segurança acima descritas)

MDPSIOS [Pag. 1 de 2]

LOGOTIPO

MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco

" Organização "

Morada

DATA : ___/___/____ Versão: _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

Histórico do Documento >>> Versão: _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____

Documento AAM nº _____ | Iteração nº _____

Analise Financeira (previsão de perda "Custo" vs Custo Investimento vs resultado a previsto) :

Decisão do CIO: _____ Ass: _____ Data: ___/___/____

(Nesta caixa deve-se descrever a previsão de perda "quanto custa organização a concretização do risco" versos o custo do investimento para metigar o risco versos a previsão do resultado que se obtem mediante o investimento a fazer)

MDPSIOS [Pag. 2 de 2]

figura 39: - MDPSIOS – Documento de Analise / Avaliação / Monitorização do Risco

(Documento predefinido com 2 páginas)

Preparar uma Declaração de Aplicabilidade.

- Uma Declaração de Aplicabilidade[45] deve ser preparada, incluindo o seguinte:
  - Os objetivos de controlo e os controlos selecionados e, as razões para a sua seleção;
  - Os objetivos de controlo e os controlos atualmente implementados; e

[45] A Declaração de Aplicabilidade prevê um resumo das decisões relativas ao tratamento de riscos. A justificação das exclusões permite validar que nenhum controlo foi omitido inadvertidamente.

- A exclusão de quaisquer objetivos de controlo e controlos e a justificativa para sua exclusão.

No caso do **MDPSIOS**, para simplificar e permitir uma visão parcial dos objetivos de controlo, apresenta um documento por cada um dos domínios/cláusulas o que possibilita uma gestão de forma mais controlada e cuidada.

Se a opção de implementação passar pela norma ISO/IEC 27002 esta declaração estará separada pelos seguintes domínios/cláusulas, anexo G.1 a G.11 (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27002):

- 5. – Política de Segurança (anexo G.1, página 203);
- 6. – Organização da Segurança da Informação (anexo G.2, página 204);
- 7. – Classificação e Controlo de Ativos de Informação (anexo G.3, página 206);
- 8. – Segurança em Recursos Humanos (anexo G.4, página 207);
- 9. – Segurança Física e Ambiental (anexo G.5, página 209);
- 10. – Gestão das Operações e Comunicações (anexo G.6, página 211);
- 11. – Controlo de Acesso (anexo G.7, página 214);
- 12. – Desenvolvimento e Manutenção de Sistemas (anexo G.8, página 216);
- 13. – Gestão de Incidentes de Segurança (anexo G.9, página 218);
- 14. – Gestão da Continuidade do Negócio (anexo G.10, página 219);
- 15. – Conformidade (anexo G.11, página 220);

Conforme exemplo representado na figura 40, para a caso dos objetivos de controlo do domínio/clausula, 5. – Política de Segurança:

LOGOTIPO

MDPSIOS - Documento de Objectivos de Controlo / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

*Histórico do Documento >>> **Versão:** _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____*

Dominio: **5.1 - Politica de Segurança**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
5.1	***Política de Segurança da Informação***	***Para proporcionar o apoio necessário e direcção e Administração relativamente a segurança da informação, em conformidade com os requisitos do negócio, as leis e regulamentos relevantes.***								
5.1.1	Documento da Política de Segurança da Informação	O documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado a todos os funcionários e colaboradores externas relevantes.	IMP			27001				Referência: SI-Regulamento Interno
5.1.2	Revisão da Política de Segurança da Informação	A política de segurança da informação deve ser revista em intervalos planificados, ou se ocorrerem mudanças significativas para garantir a sua contínua eficiência, eficácia e adequação.	IEC			27002				Referência: Gestão de Politicas
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

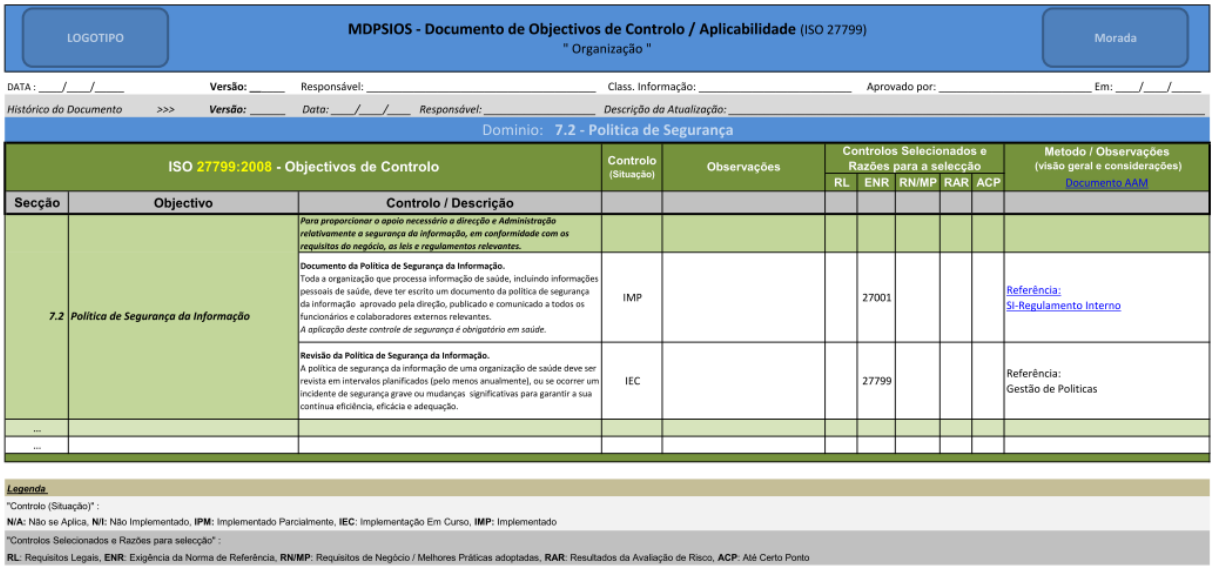
figura 40: - MDPSIOS – Documento de Objetivos de Controlo / Aplicabilidade (ISO 27002)

Se a opção de implementação passar pela norma ISO/IEC 27799 esta declaração estará separada pelos seguintes domínios/cláusulas, anexo H.1 a H.11 (MDPSIOS – Domínios/Cláusulas norma ISO/IEC 27799):

- 7.2 – Política de Segurança (anexo H.1, página 225);
- 7.3 – Organização da Segurança da Informação (anexo H.2, página 226);

- 7.4 – Classificação e Controlo de Ativos de Informação (anexo H.3, página 228);
- 7.5 – Segurança em Recursos Humanos (anexo H.4, página 229);
- 7.6 – Segurança Física e Ambiental (anexo H.5, página 231);
- 7.7 – Gestão de Comunicações e Operações (anexo H.6, página 233);
- 7.8 – Controlo de Acesso (anexo H.7, página 239);
- 7.9 – Desenvolvimento e Manutenção de Sistemas (anexo H.8, página 243);
- 7.10 – Gestão de Incidentes de Segurança (anexo H.9, página 245);
- 7.11 – Gestão da Continuidade do Negócio (anexo H.10, página 246);
- 7.12 – Conformidade (anexo H.11, página 247);

Conforme exemplo representado na figura 41, para a caso dos objetivos de controlo do domínio/clausula, 7.2 – Política de Segurança:



LOGOTIPO

MDPSIOS - Documento de Objectivos de Controlo / Aplicabilidade (ISO 27799)
" Organização "

Morada

DATA : ___/___/___ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

Histórico do Documento >>> **Versão:** _____ *Data:* ___/___/___ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.2 - Politica de Segurança**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.2	***Política de Segurança da Informação***	***Para proporcionar o apoio necessário a direcção e Administração relativamente a segurança da informação, em conformidade com os requisitos do negócio, as leis e regulamentos relevantes.***								
		Documento da Política de Segurança da Informação. Toda a organização que processa informação de saúde, incluindo informações pessoais de saúde, deve ter escrito um documento da política de segurança da informação aprovado pela direção, publicado e comunicado a todos os funcionários e colaboradores externos relevantes. *A aplicação deste controle de segurança é obrigatório em saúde.*	IMP			27001				Referência: SI-Regulamento Interno
		Revisão da Política de Segurança da Informação. A política de segurança da informação de uma organização de saúde deve ser revista em intervalos planificados (pelo menos anualmente), ou se ocorrer um incidente de segurança grave ou mudanças significativas para garantir a sua continua eficiência, eficácia e adequação.	IEC			27799				Referência: Gestão de Politicas
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

figura 41: - MDPSIOS – Documento de Objetivos de Controlo / Aplicabilidade (ISO 27299)

6.1.5 5.Formação e Sensibilização

A organização deve promover e assegurar que todo o pessoal que tem responsabilidades atribuídas e definidas no SGSI tenha as competências necessárias para desempenhar as tarefas requeridas [8]:

- Determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;
- Atribuindo ações de formação ou através de outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;
- Avaliando a eficácia das ações executadas; e
- Mantendo registros de formação, treino, habilidades, experiências e qualificações.

A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI.

No caso do **MDPSIOS**, para formalizar este ponto, disponibiliza o documento da figura 42, anexo F.19 (MDPSIOS - Formação e Sensibilização dos Funcionários e Colaboradores), página 197.

LOGOTIPO

MDPSIOS - Formação e Sensibilização dos Funcionarios e Colaboradores
Organização de Saúde XPTO

Morada

Criado em: 30 / 10 / 2012 **Versão: V.01** **Responsável:** Francisco Carvalho **Informação** (Classificação): Interna **Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 30 / 10 / 2012

*Histórico de Versões do Documento >>> **Versão:** V.01* ***Data:** 30 / 10 / 2012* ***Responsável:** Francisco Carvalho* ***Descrição:** - Aprovação do Documento*

1. Introdução

- A formação e sensibilização dos funcionarios e colaboradores é um factor muito importante para o sucesso de qualquer SGSI.

2. Objectivos

- Definir formas e meios a utilizar para dar formação e promover a sensibilização dos funcionarios e colaboradores da organização.

Decisão

APROVADO

Luís Anibal
~~Administração ou~~ Director Executivo

Implementação

Prazo (nº dias): Imediata

Concluido em: ____/____/____

Verificado por: _____

Documento ligação: _____

3. Descrição

- Todos os funcionarios e colaboradores devem ser devidamente escalrecidos e formados sobre a importância da segurança da informação , independentemente da sua função ou cargo na organização.
- Devem-se encontrar as melhores soluções e formas de fazer chegar ou divulgar as informações sobre segurança a todos, se possivel recorrendo a apresentações, intranet, etc.
- As politicas de segurança adotadas, devem ser de conhecimento geram, assim a abertura paranovas sugestões e ideias que possam surgir por parte de qualquer funcionario.
- Deve-se sempre que necessário realizar novas acções de formação e ou sensibilização para todos ou por areas caso tal justifique.

4. OBS

...

figura 42: - MDPSIOS – Formação e Sensibilização dos Funcionários e Colaboradores

6.1.6 6.Controlo de Documentos e Registo

- Controlo de Documentos

Os documentos requeridos e produzidos pelo SGSI devem ser protegidos e controlados.
Um procedimento devidamente documentado deve ser estabelecido para definir as ações de gestão necessárias:

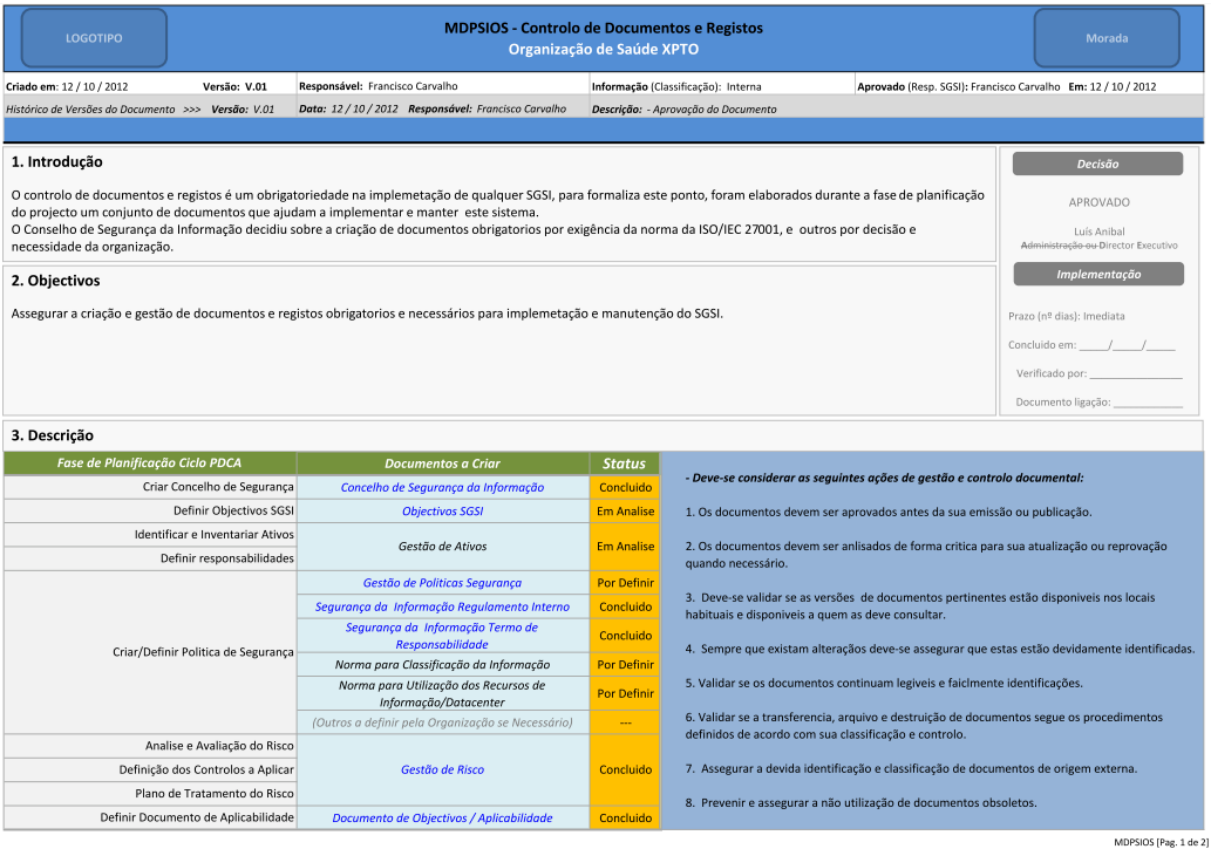
- Os documentos devem ser aprovados antes da sua emissão ou publicação;
- Os documentos devem ser analisados de forma crítica para sua atualização ou reprovação quando necessário;
- Assegurar que as alterações e as situações de revisão dos documentos atuais sejam identificadas;

- Deve-se validar se as versões de documentos pertinentes estão disponíveis nos locais habituais e a quem as deve consultar;
- Assegurar que os documentos permaneçam legíveis e devidamente identificáveis;
- Assegurar que os documentos estejam disponíveis àqueles que deles precisam e sejam transferidos, armazenados e finalmente destruídos conforme os procedimentos aplicáveis à sua classificação;
- Assegurar que documentos de origem externa sejam devidamente identificados e classificados;
- Assegurar que a distribuição de documentos seja controlada;
- Prevenir e assegurar a utilização não intencional de documentos obsoletos;
- Aplicar identificação adequada nos casos em que sejam retidos para qualquer propósito (documentos obsoletos).

- Controlo de Registos

Os registros devem ser definidos e mantidos para fornecer evidências de conformidade com os requisitos e da operação eficaz do SGSI, devem ser protegidos e controlados. O SGSI deve ter em consideração os requisitos legais ou regulamentares pertinentes e obrigações contratuais. Os registros devem permanecer legíveis, prontamente identificáveis e recuperáveis. Os controlos necessários para a identificação, armazenamento, proteção, recuperação, tempo de retenção e a disposição dos registos devem ser documentados e implementados.
Devem ser mantidos registos do desempenho do processo e de todas as ocorrências de incidentes de segurança da informação significativos relacionados com o SGSI.

No caso do **MDPSIOS**, para formalizar este ponto, utiliza o documento da figura 43, anexo F.20 (MDPSIOS - Controlo de Documentos e Registos), página 198.



LOGOTIPO

MDPSIOS - Controlo de Documentos e Registos
Organização de Saúde XPTO

Morada

Criado em: 12 / 10 / 2012 **Versão: V.01**	**Responsável:** Francisco Carvalho	**Informação** (Classificação): Interna	**Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 12 / 10 / 2012
Histórico de Versões do Documento >>> ***Versão:*** *V.01*	***Data:*** *12 / 10 / 2012* ***Responsável:*** *Francisco Carvalho*	***Descrição:*** *- Aprovação do Documento*	

1. Introdução

O controlo de documentos e registos é um obrigatoriedade na implemetação de qualquer SGSI, para formaliza este ponto, foram elaborados durante a fase de planificação do projecto um conjunto de documentos que ajudam a implementar e manter este sistema.
O Conselho de Segurança da Informação decidiu sobre a criação de documentos obrigatorios por exigência da norma da ISO/IEC 27001, e outros por decisão e necessidade da organização.

2. Objectivos

Assegurar a criação e gestão de documentos e registos obrigatorios e necessários para implemetação e manutenção do SGSI.

Decisão

APROVADO

Luís Anibal
~~Administração ou~~ Director Executivo

Implementação

Prazo (nº dias): Imediata

Concluido em: ____/____/____

Verificado por: _____

Documento ligação: _____

3. Descrição

Fase de Planificação Ciclo PDCA	*Documentos a Criar*	*Status*
Criar Concelho de Segurança	*Concelho de Segurança da Informação*	Concluido
Definir Objectivos SGSI	*Objectivos SGSI*	Em Analise
Identificar e Inventariar Ativos	*Gestão de Ativos*	Em Analise
Definir responsabilidades		
Criar/Definir Politica de Segurança	*Gestão de Politicas Segurança*	Por Definir
	Segurança da Informação Regulamento Interno	Concluido
	Segurança da Informação Termo de Responsabilidade	Concluido
	Norma para Classificação da Informação	Por Definir
	Norma para Utilização dos Recursos de Informação/Datacenter	Por Definir
	(Outros a definir pela Organização se Necessário)	---
Analise e Avaliação do Risco	*Gestão de Risco*	Concluido
Definição dos Controlos a Aplicar		
Plano de Tratamento do Risco		
Definir Documento de Aplicabilidade	*Documento de Objectivos / Aplicabilidade*	Concluido

- Deve-se considerar as seguintes ações de gestão e controlo documental:

1. Os documentos devem ser aprovados antes da sua emissão ou publicação.
2. Os documentos devem ser anlisados de forma critica para sua atualização ou reprovação quando necessário.
3. Deve-se validar se as versões de documentos pertinentes estão disponiveis nos locais habituais e disponiveis a quem as deve consultar.
4. Sempre que existam alterações deve-se assegurar que estas estão devidamente identificadas.
5. Validar se os documentos continuam legiveis e faiclmente identificações.
6. Validar se a transferencia, arquivo e destruição de documentos segue os procedimentos definidos de acordo com sua classificação e controlo.
7. Assegurar a devida identificação e classificação de documentos de origem externa.
8. Prevenir e assegurar a não utilização de documentos obsoletos.

MDPSIOS [Pag. 1 de 2]

figura 43: - MDPSIOS – Controlo de Documentos e Registos

6.1.7 7. Monitorização e Medição

A organização deve estar preparada para [8]:

- Executar procedimentos de monitoração e análise crítica e outros controlos para:
  - Prontamente detetar erros nos resultados dos processos e procedimentos;
  - Prontamente identificar tentativas e violações de segurança bem-sucedidas, e incidentes de segurança da informação;
  - Permitir à direção determinar se as atividades de segurança da informação delegadas a pessoas ou implementadas por meio de tecnologias de informação são executadas e obtêm os resultados pretendidos;
  - Ajudar a detetar eventos de segurança da informação e assim prevenir incidentes de segurança da informação através da utilização de indicadores; e
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.

- Realizar análises críticas regulares da eficácia do SGSI (incluindo os requisitos da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), tendo em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas.
- Analisar criticamente as análises/avaliações de riscos a intervalos planeados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados, tendo em consideração mudanças relativas a:
    - Organização; tecnologias; objetivos e processos de negócio; ameaças identificadas; eficácia dos controles implementados; eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social.
- Conduzir auditorias internas[46] do SGSI em intervalos planeados.
- Realizar uma análise crítica do SGSI pela direção em períodos regulares para assegurar que o objetivo permanece adequado e que são identificadas melhorias nos processos do SGSI.
- Atualizar os planos de segurança da informação tendo em consideração os resultados das atividades de monitorização e análise crítica.
- Registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI
- Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos.

No caso do **MDPSIOS**, para formalizar este ponto, utiliza o documento do anexo F.7 (MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco), página 183. Os indicadores de monitorização e medição estão devidamente retratados no capítulo 5 secção 5.2.2.6 “MDPSIOS - monitorização e análise crítica do risco”. No anexo F.9 (MDPSIOS - Avaliação de Risco / definição de Controlos – Global), página 186 e anexo F.13 (MDPSIOS - Estatística Controlos Implementados), página 190, estão representados alguns dos indicadores que este modelo documental disponibiliza.

[46] Auditorias internas, também chamadas de auditorias de primeira parte, são conduzidas por ou em nome da própria organização para propósitos internos [8].

6.1.8 8. Avaliação e Melhoria Continua

A organização deve regularmente tratar de:

- Implementar as melhorias identificadas no SGSI.
- Executar as ações preventivas e corretivas apropriadas.
    - Acção Corretiva:
      A organização deve executar ações para eliminar as causas de não-conformidades com os requisitos do SGSI, de forma a evitar a sua repetição.
    - Acção Preventiva:
      A organização deve determinar ações para eliminar as causas de não-conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência. As ações preventivas tomadas devem ser apropriadas aos impactos dos potenciais problemas.
- Aplicar lições aprendidas de experiências de segurança da informação de outras organizações e da própria organização.
- Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado as circunstâncias e, se relevante, obter a concordância sobre como proceder.
- Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorizados, ações corretivas e preventivas e análise crítica pela direção.

No caso do **MDPSIOS**, para formalizar este ponto, utiliza o documento em anexo F.7 (MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco), página 183.

Capítulo 7 - DISCUSSÃO E CONCLUSÃO

7.1 Discussão

Após o desenvolvimento e conceção do protótipo MDPSIOS, para aferir algumas das opções tomadas, nomeadamente à sua estrutura funcional e de cumprimento dos requisitos funcionais de um Sistema de Gestão de Segurança da Informação (SGSI), foi realizada uma avaliação por peritos da área da segurança da informação.

Entenda-se perito como sendo um profissional com pelo menos 10 anos de experiência[47] a desenvolver, implementar e auditar ou a gerir SGSI.

Para a realização da avaliação critica e construtiva através da apresentação do modelo, recorreu-se a três peritos que são consultores e auditores experientes em implementações, auditorias e monitorização de SGSI, conhecedores da família de normas ISO/IEC 27000, assim como da realidade da segurança da informação nas organizações em geral e em particular no sector da saúde.

Após apresentação do modelo, a avaliação foi efetuada com base num questionário, constituído por um conjunto de 10 perguntas de resposta na forma aberta e uma pergunta de comentário global ao protótipo desenvolvido, conforme anexo J (página 254 a 263).

Apesar de ser desejável um número superior de peritos, mas devido a constrangimentos temporais e de disponibilidade dos próprios peritos, a equipa de peritos foi a seguinte:

- Engenheiro José Casinhas, com a função de *Information Security Manager*, na empresa ONI – Lisboa, com mais de 15 anos na função, licenciado, MBA, CISA, ISO/IEC 27001 LA, ITIL, ISO/IEC 22301 LI.
- Engenheiro Luis Martins, com a função de *Business Unit Manager - Governance, Risk and Compliance,* na empresa GLINTT – Beloura, com mais de 13 anos na função, licenciado, *Information Security*.
- Doutor Rui Gomes, com a função de *Chief Information Officer* (CIO) no Hospital Prof. Doutor Fernando Fonseca E.P.E – Amadora (Hospital Amadora-Sintra), com mais de 15 anos na função, Doutorado em Gestão, Mestre em Informática Médica, Licenciado em Engenharia Eletrotécnica.

[47] Em muitos domínios a estimativa diz que são necessários pelo menos 10 anos de experiência e prática, para ser um perito [83].

O resultado das avaliações realizadas pelos peritos é apresentada nos anexos J.1, J.2 e J.3. Da sua análise qualitativa pode-se afirmar que o protótipo desenvolvido apresenta as principais características que um SGSI tem de cumprir.

Foram também expressas sugestões para melhoramento da solução, que serão consideradas nos trabalhos futuros a realizar, para melhorar e adequar o modelo de forma abrangente a realidade e as necessidades apresentadas com vista ao seu enquadramento numa perspectiva de apoio e suporte para a certificação.

Resumo da Avaliação Critica e Construtiva

Neste ponto é apresentado um resumo geral e a conclusão/discussão, da análise feita a cada uma das questões do questionário da avaliação critica e construtiva, devidamente respondida pelos peritos, conforme anexo J (página 254 a 263).

A. - O Conceito utilizado?

Na resposta a esta questão, os peritos divergem relativamente ao PDCA, no que respeita a evidencia de tarefas já executadas das que faltam, assim como no seu alinhamento em 100% com a ISO/27001, no entanto todos reconhecem que o conceito esta estruturado, adequado ao fim a que se destina e reflete um bom trabalho de investigação.

Conclusão / Discussão:

Na fase em que o modelo foi apresentado/demonstrado, não estava o controlo documental e o alinhamento do PDCA devidamente finalizado, estes pontos, é um dos melhoramentos implementados que resultou desta avaliação.

B. - Estrutura geral do modelo?

Na resposta a esta questão os peritos são unânimes em afirmar que a estrutura geral do modelo esta alinhado com os requisitos da norma ISO/IEC 27001, bem desenhada e aparenta ser flexível e fluida.

Conclusão / Discussão:

Um dos objetivos do modelo é de apresentar uma estrutura que lhe permite ser flexível, suficientemente robusto com fluidez suficiente para se adaptar a qualquer organização que o queira adotar para implementação de um SGSI ou mesmo com vista ao apoio inicial para futura certificação na norma ISO/IEC 27001.

C. - Cumpre com os requisitos necessários e essências de um SGSI?

Na resposta a esta questão os peritos são unânimes em afirmar que no geral cumpre todos os requisitos de um SGSI.
No entanto sugerem que alguns aspetos podem ser melhorados, como a inclusão na Declaração de Aplicabilidade (SoA) dos requisitos regulatórios ou outros que possam influenciar o SGSI, assim como a citação dos objetivos para cada domínio.

Conclusão / Discussão:

O modelo procura implementar de forma ágil e de fácil perceção para o utilizador, todos os requisitos necessários e essenciais de um SGSI. A forma como foi estruturado demonstra a existência dessa preocupação durante a sua conceção. No entanto alguns dos pontos sugeridos pelos peritos nesta questão, já estavam implementados no modelo e faziam parte do documento "MDPSIOS - Documento de Objetivos de Controlo / Aplicabilidade", tendo sido melhorado/aperfeiçoado para melhor enquadramento e resposta as necessidades que podem surgir durante a sua utilização.

D. - Apresentação e Layouts do modelo?

Na resposta a esta questão, os peritos consideram que o modelo tem boa apresentação (grande trabalho de sistematização, maquetes de layout com bom *look & feel*). No entanto ainda podem ser melhorados em termos visuais.

Conclusão / Discussão:

O modelo procura disponibilizar *layouts* que permitam ao utilizar a aplicação, que esta tenha uma navegação agradável e ‘sentida’, e que ao mesmo tempo ajude a diferenciar aspetos mais importantes dos restantes, disponibilize a informação necessária em cada passo. Apesar da ótima opinião dada, sobre o atual *layout* do modelo, também não deixa de ser verdade que o mesmo terá ainda margem para melhoramento.

E. - Apresenta uma abordagem intuitiva na sua utilização?

Na resposta a esta questão os peritos avaliam que, de forma geral existe uma abordagem intuitiva na sua utilização. No entanto, existem *écrans* com muita informação o que pode ser pouco prático, podendo a abordagem ser melhorada.

Conclusão / Discussão:

Nesta fase do modelo existem situações que podem ou terão de ser melhoradas e aperfeiçoadas, algumas serão tidas em conta em versões futuras a medida que o modelo é adotado e utilizado. Sendo a flexibilidade que este apresenta um fator facilitador para crescer e ser adaptado na medida e forma de apresentação que a organização/utilizador pretender.

F. - Funcionalidade do Modelo?

Na resposta a esta questão os peritos acham que o modelo apresenta uma boa funcionalidade com bastante possibilidade de melhoria. Um ponto muito positivo nesta abordagem, é por exemplo a existência no documento "MDPSIOS - Documento de Objetivos de Controlo / Aplicabilidade" dos controlos selecionados e a razões da sua aplicabilidade.

Conclusão / Discussão:

A conceção do modelo suportada no PDCA, na norma ISO/IEC 27001, norma ISO/IEC 27002, norma ISO/IEC 27799 e norma ISO/IEC 27005, confere-lhe uma estrutura solida que lhe permite um enquadramento e alinhado funcional de um SGSI, com possibilidades de melhoria e resposta adequada as necessidades da organização no decurso da sua utilização.

G. - Aspetos positivos?

Na resposta a esta questão os peritos avaliam que um dos aspetos positivos do modelo é o facto de só depender do *Excel*, assim como a congregação da informação pode ser uma ajuda muito significativa para qualquer organização que equacione a implementação de um SGSI. Outros dos aspetos positivos é a excelente recolha de dados que lhe confere um aspeto informativo assim como a documentação desenvolvida (concelho de segurança da informação; segurança da informação regulamento interno; segurança da informação termo de responsabilidade; objetivos do

sistema de segurança; política de segurança da informação; formação e sensibilização das pessoas; inventário dos ativos; etc.).

Conclusão / Discussão:

Para além dos aspetos indicados pelos peritos existe um de extrema importância, que é a utilização na gestão de risco da metodologia do Modelo de Avaliação de Risco de Segurança da Informação (MARSI). Outro aspeto positivo, é o facto de o modelo ter uma abrangência que vai desde a possibilidade de definir o estado T0 de uma organização até a possibilidade de servir de base de partida para a certificação.

H. - Aspetos negativos?

Na resposta a esta questão os peritos definiram como aspetos negativos, a falta de controlo documental (muito importante para a certificação e funcionalidade do sistema documental), assim como alguma imaturidade na apresentação dos *layouts* e falta de uma perspectiva quantitativa que permite ao decisor ter uma noção de dimensão financeira.

Conclusão / Discussão:

Os aspetos definidos pelos peritos neste ponto foram tidos em conta e aplicados, isto é, incluídos de imediato como melhoramentos na versão atual do modelo, tornando-o mais adequado ao objetivo definido para o mesmo.

I. - Têm algo de novo que não conheça, alguma inovação?

Na resposta a esta questão os peritos avaliaram, o facto de utilizar o *Excel* para todos os aspetos e/ou a congregação e organização da informação num único ponto, como inovador.

Conclusão / Discussão:

Para além dos aspetos indicados pelos peritos, existe um aspeto de extrema importância, cuja sua adaptabilidade concebe a este modelo uma característica impar, que é a utilização na gestão de risco do Modelo de Avaliação de Risco de Segurança da Informação (MARSI), adaptada da Modelo de Avaliação de Risco de Acidentes de Trabalho (MARAT).

J. – O modelo apresentado é uma ajuda ou simplifica a implementação de um SGSI em qualquer organização?

Na resposta a esta questão, os peritos são unânimes em considerar que o modelo constitui sem dúvida uma potencial de ajuda para qualquer organização que esteja a equacionar a implementação de um SGSI, posicionando-se como um ferramenta extremamente útil e valiosa.

Conclusão / Discussão:

A unanimidade e consenso na resposta dos peritos relativamente a esta questão, mostra que a versão aplicacional que neste momento o modelo apresenta, cumpre com os objetivos para o qual o mesmo foi proposto e concebido.

K. - Conclusão:

Neste item do questionário os peritos concluíram que:

- Da avaliação realizada o conceito do modelo aponta para um nível de robustez considerável.
- Do ponto de vista da sua especificidade, em organizações de saúde foi bem identificada em capítulos da família de normas ISO/IEC 27000 para este sector, mas para tornar este sistema mais adequado, questões regulamentares do sector deverão ser incorporadas no sistema de gestão pois parece ser um aspeto relevante a ter em conta.
- Em relação à utilização do Microsoft Excel como ferramenta de suporte à implementação, está adequada à fase de protótipo, mas é preciso ter cuidado com as questões de segurança. Por exemplo, a inadequada gestão de controlo de acessos desta ferramenta pode colocar em causa todo um trabalho e um sistema. Isto é um desafio, especialmente se houver intenção de certificação por entidade externa.
- O modelo cumpre, de uma forma geral, com o que foi apresentado enquanto objetivo e com os requisitos de um SGSI.
- O modelo tem clara margem para melhorias, quer a nível da estrutura e organização, quer ao nível da facilidade de uso *layout*.
- É sem qualquer dúvida uma abordagem de valor e meritória de acompanhamento, sempre que possível, com a eventual possibilidade de testar o modelo num contexto empresarial real.

- O trabalho está muito orientado para a documentação, e tal como o nome indica “Modelo Documental para a Política de Segurança da Informação em Organizações de Saúde”.
- É útil, pertinente e matéria essencial para a implementação de um modelo documental de SGSI.

7.1.2 – Discussão

O resultado desta avaliação critica e construtivo foi um ponto de partida para, se perceber se a conceção que o modelo estava a ter ia no sentido da realidade e necessidades que as organizações têm, ao adotarem o modelo como base para análise do seu estado relativamente a segurança da informação, assim como para implementação de um SGSI que pudesse ajudar na resolução dos problemas de segurança da informação.

Permitiu também que fossem efetuados os primeiros melhoramentos ao modelo, de forma a torna-lo mais apto ao fim a que foi proposto com base no *feedback* de profissionais experientes, que sabem que ferramentas são necessários e que podem ajudar na resolução de problemas associados a segurança da informação no dia-a-dia das organizações.

7.2 Conclusão

Os sistemas de informação ligados a área de saúde devem satisfazer exigências únicas para continuarem operacionais mesmo perante situações de desastres naturais, falhas de sistemas e ataques de negação de serviço. Garantir a confidencialidade, a integridade e a disponibilidade da informação de saúde requer um grande esforço a todos os níveis por parte da organização, principalmente por parte de quem gere a segurança da informação.

A confidencialidade da informação de saúde é importante, sendo a informação de carater pessoal e clinico muito importante e essencial, porque deve garantir e manter a privacidade do paciente de acordo com a conformidade legalmente obrigatória.

A integridade da informação de saúde é importante e essencial porque deve ser protegida para garantir a segurança do paciente, e um componente importante desta proteção é assegurar que todo o ciclo de vida da informação seja completamente auditável.

A disponibilidade da informação de saúde, também é crítica no sentido em que é preciso garantir que a informação dos serviços de cuidados de saúde esteja disponível sempre que for precisa.

Para alguns autores esta área é caraterizada por uma natureza específica e às três dimensões consideradas clássicas, deve-se adicionar a dimensão autoria/responsabilidade. Esta dimensão permite conhecer o autor e o responsável por uma determinada informação ou processo e revela-se de importância vital hoje em dia, dada a necessidade de determinar com exatidão onde começa e acaba a responsabilidade de cada profissional de saúde interveniente nos cuidados prestados a um doente.

A efetiva gestão de segurança da informação em saúde torna-se cada vez mais necessária pelo aumento da troca digital de informações pessoais de saúde entre profissionais de saúde, pelo uso crescente de tecnologias de internet no fornecimento de serviços de saúde e utilização de redes sem fio (wireless) entre outras. Se estas tecnologias complexas não forem implementadas corretamente, poderão aumentar os riscos de confidencialidade, integridade, confiabilidade e disponibilidade da informação nestas organizações.

Não obstante o tamanho, a posição e o modelo do fornecimento de serviços, todas as organizações precisam de ter controlos rígidos implantados para proteger a sua informação ou a que lhes é confiada como é o caso particular da área de saúde. Portanto, as organizações de saúde devem ter uma orientação clara, concisa, e específica de saúde na seleção e na implementação de controlos de segurança da informação. Estas orientações

devem ser adaptáveis a qualquer dimensão da organização, localização, e ou tipos diferentes de serviço disponibilizados pelas instituições de saúde.

Constata-se empiricamente que qualquer organização independentemente da sua dimensão e área de atuação, ainda têm um grande caminho a percorrer de forma a tirarem o máximo partido dos seus sistemas de informação, aliás no atual contexto em que vivemos e vivem estas organizações, em que os desafios são cada vez maiores e mais exigentes, a importância do conhecimento da gestão da segurança da informação assume um papel e peso ainda maior e inevitável quando integrado nos processos de gestão da organização de forma flexível e adaptável às suas necessidades e crescimento, garantido continuidade e evolução por parte da organização.

Naturalmente não existe um único modelo capaz de servir todas as organizações.
Para que as organizações possam realmente implementar e adaptar um modelo a sua medida, precisam de se focar na forma como a gestão da segurança da informação pode ser utilizada para gerar competências, capacidades criticas e sobretudo proteger o ativo mais importante do seculo XXI (a informação), sendo também muito importante que haja um acompanhamento da cultura organizacional e dos comportamentos individuas para que o resultado seja eficaz e eficiente.

O MDPSIOS, está concebido de forma a servir de ponto de partida ou mesmo de guia prático para desenvolver os procedimentos de segurança da informação da organização e ajudar na integração das eficientes práticas de gestão da segurança da informação, permitindo desta forma a criação de confiança nas atividades internas e externas da organização ou instituição, através da implementação de um sistema de gestão da segurança da informação que o mesmo incorpora, baseado em normas internacionais da família ISO 27000 que definem aspetos e as boas práticas que se deve ter em consideração ao elaborar e implementar políticas de segurança da informação.

No início requer um contínuo e constante melhoramento, que ao longo da sua utilização possivelmente se revelariam necessários, de forma a torna-lo cada vez mais otimizado.
Indo, desta forma ao encontro de diversas necessidades e possíveis soluções, apresentando uma maior eficácia e eficiência em futuras implementações ou revisões do Sistemas de Gestão de Segurança da Informação (SGSI).
A escolha do caminho a seguir para elaboração deste modelo documental, foi extremamente difícil de definir devido ao grande e variado leque de processos e sistemas que podem estar relacionados, do qual o SGSI depende e tem de intervir numa organização.
Este modelo de documentos para implementação de um SGSI, ao estar estruturado desta forma, apresenta um conjunto de vantagens a ter em conta, das quais se destacam:

- Simplicidade;
- Versatilidade;
- Ecológico (evita a utilização de papel);
- Fácil partilha e distribuição entre os intervenientes;
- Pode crescer em itens de critérios (domínios, dimensões, objetivos, controlos) e informação de apoio em função das necessidades, de forma simples;
- Facilidade em reescrever uma política de segurança.

Em conclusão, a segurança da informação acaba por ser um problema 'mais' organizacional do que tecnológico.

O que faz com que a implementação de um SGSI tenha que ser um compromisso entre o risco, o grau de proteção desejado e o custo dos mecanismos de controlo.

7.3 Trabalhos Futuros

Sendo o MDPSIOS um modelo documental destinado a gestão de segurança da informação, área que nos tempos atuais é vista como complexa ou com alguma complexidade, e que é em diferentes formas muito dependente das necessidades distintas de cada organização, em que os sistemas de informação estão em constante evolução assim como as próprias organizações, em que as possíveis ameaças são cada mais sofisticada, terá o modelo muito por onde crescer e melhorar. Tal como o sistema (SGSI) que o próprio modelo tenta implementar, ele próprio também terá de incorporar o princípio que é estar sujeito a uma melhoria continua e sistemática.

Os trabalhos futuros previstos passam pelas sugestões desde já apresentadas pelos peritos que avaliaram nesta fase este modelo. Este modelo poderá evoluir de forma diferente ou diferenciada de organização para organização, pelo facto das necessidades, em princípio não serem iguais de umas para as outras e o modelo ser flexível e ajustável.

Os possíveis trabalhos futuros são:

- Avaliar e implementar sugestões, apresentadas pelos peritos;
    - Melhorar o modelo com *inputs* de profissionais da indústria com experiência de implementação e de gestão de sistemas de segurança;
    - Melhor o *output* da valorização financeira que possa enquadrar e ajudar em termos de decisão nas iterações com a gestão;
    - Revisão do grafismo e cores usadas em alguns casos.
- Implementar em organizações, acompanhar e recolher informação útil para melhorias;
- Adicionar outras funcionalidades ou alterações sugeridas pelos utilizadores finais da aplicação, que melhorem a sua usabilidade e desempenho;
- Avaliação da eficácia do modelo através da definição de métricas e meios de medição propostos pela norma ISO/IEC 27004;
- Preparar o modelo para fins de certificação da organização, na norma ISO/IEC 27001;
- Noutro enquadramento temporal, desenvolver o modelo numa plataforma aplicacional que permite funcionar em ambiente multiposto e partilhado.

Capítulo 8 - Referências Bibliográficas

[1] A. M. R. C. dos Santos, “Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação,” Universidade do Minho, 2007.

[2] D. A. REZENDE and A. F. ABREU, *Tecnologia da informação aplicada a sistemas de informações empresariais*. 2000.

[3] H. KATZAM JR, *Segurança de Dados em Computação*. 1977.

[4] M. SÊMOLA, *Gestão da Segurança da Informação – Uma visão Executiva*. 2003.

[5] C. DIAS, *Segurança e Auditoria da Tecnologia da Informação*. 2000.

[6] Promon Business & Technology Review, “Segurança da Informação Um diferencial determinante na competitividade das corporações,” 2005.

[7] M. Aurelio and P. Laureano, “Gestão de segurança da informação,” 2005.

[8] I. STANDARD, *INTERNATIONAL STANDARD ISO / IEC FDIS 27001*, 1º Ed. 2005.

[9] T. WADLOW, *Segurança em Redes*. 2000.

[10] J. Carlos, P. Ferreira, E. M. Neto, and R. A. C. Leite, “Classificação da Informação de acordo com normal ISO / IEC 17799 : 2005,” pp. 1–5, 2005.

[11] O. LabSpace, “An introduction to information security - Why is information security important?” [Online]. Available: http://labspace.open.ac.uk/mod/resource/view.php?id=343885. [Accessed: 27-Jul-2012].

[12] S. Loh, “Sistemas de Informação.” [Online]. Available: http://paginas.ucpel.tche.br/~loh/sist-inf.htm. [Accessed: 18-May-2012].

[13] P. Silva, H. Carvalho, and C. B. Torres, *Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial*. 2003.

[14] C. Marçalo, “Negocios: Segurança da Informação,” *Semana Informática*, p. 22, Apr-2012.

[15] A. F. Cristina, “Estratégia: Segurança escapa à crise,” *Semana Informática*, p. 14, Nov-2010.

[16] C. EUROPEIA, “Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade.” Bruxelas, p. COM(2012) 140 final, 2012.

[17] SGS Portugal - Sociedade Geral de Superintendência S.A., “Portugal pela positiva,” 2004.

[18] I. I. U. G. (IUG)., “International Register of ISMS Certificates,” 2012. [Online]. Available: http://iso27001certificates.com/. [Accessed: 15-Apr-2012].

[19] I. I. U. G. (IUG)., “Internacional Register of ISMS Certificates,” 2012. [Online]. Available: http://iso27001certificates.com/. [Accessed: 04-Aug-2012].

[20] D. VASILE, “PENTEST Romania Security Design, Implementation & Audit,” 2012. [Online]. Available: http://www.pentest.ro/iso-27001-certification-statistics/. [Accessed: 30-Jul-2012].

[21] Eurostat, “Statistics in focus 7/2011,” 2011. [Online]. Available: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-11-007/EN/KS-SF-11-007-EN.PDF. [Accessed: 28-Jul-2012].

[22] PTPrime, “Serviço Segurança TIC,” 2012. [Online]. Available: http://www.ptprime.pt/ServicosESolucoes/informacao_conhecimento/Documents/VideoseDemonstracoes/Serv_seguranca/Serv_Seguranca.swf. [Accessed: 08-Aug-2012].

[23] I. Standard, “ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security management,” *Security*, 2005.

[24] R. J. M. M. C. GOMES, “UMA ABORDAGEM RELACIONAL E PLANEADA PARA A APLICAÇÃO DE MODELOS DE GESTÃO DA SEGURANÇA NA SAÚDE,” Universidade do Porto, 2010.

[25] J. P. Serra, *Manual de Teoria da Comunicação*. Covilhã: , 2007, p. 203.

[26] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication*. 1949, p. 117.

[27] D. Salomon, *Data Compression: The Complete Reference*, 2 ed. [S.l. 2000, p. 279.

[28] L. Niemeyer, *Elementos de Semiótica Aplicados ao Design*, 2ª ed. Rio de Janeiro: , 2007.

[29] P. Beynon-Davies, *Information Systems: an introduction to informatics in Organisations*. Basingstoke, UK: , 2002.

[30] P. Beynon-Davies, *Business Information Systems*. Basingstoke, UK: , 2009.

[31] M. Oliveira, *Ciência da Informação e Biblioteconomia: Novos Conteúdos e Espaços de Atuação.* Belo Horizonte: , 2005.

[32] A. M. Gadomski, *Supporto intelligente alle decisioni: acquisizione informazioni e conoscenze*. 1993.

[33] D. E. Knuth, *Selected Papers on Computer Science*. Cambridge: , p. 274 p.p. 1–2.

[34] C. D. Ortega, “INFORMÁTICA DOCUMENTÁRIA : ESTADO DA ARTE,” Universidade de São Paulo, 2002.

[35] C. D. Ortega, “Do princípio monográfico à unidade documentária : exploração dos fundamentos da Catalogação,” no. 31, pp. 43–60, 2011.

[36] V. P. da Silva and A. M. Costa, “Sistema de gestão de segurança e saúde ocupacional,” vol. 2, pp. 229–248, 2012.

[37] L. S. Matos, “© DICIONÁRIO DE FILOSOFIA MORAL E POLÍTICA.”

[38] J. M. Pinho, “Auditoria e Análise de Segurança da Informação Segurança Física e Lógica da Informação,” 2009.

[39] P. J. M. S. Pinheiro, “Auditoria e Análise de Segurança da Informação - Segurança Física e Lógica,” 2009.

[40] P. W. A. C. Peixoto and P. H. Moura, “Curso de Gestão da Segurança nas Organizações - Segurança Física,” 2004.

[41] E. e T. da I. Inside-Factis, “Segurança da Informação Para Além das Boas Intenções,” Lisboa, p. 3, 2011.

[42] . De, Associação Brasileira de Normas Técnicas, “NBR ISO/IEC 17799 – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação.,” 2003.

[43] R. Shirey, “RFC 2828 – Internet Security Glossary,” 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2828.txt?number=2828. [Accessed: 29-Nov-2012].

[44] T. R. Peltier, J. Peltier, and J. Blackley, *Information security fundamentals*. Auerbach Publications, 2005.

[45] N. M. Martel, *“Medical Records Security,” in Handbook of Information Security - Threats, Vulnerabilities, Prevention, Detection, and Management*, Vol. 3. 2006.

[46] P. J. Brusil and D. Harley, *“Medical Records Security,” in Computer Security Handbook, S. Bosworth and M. E. Kabay*, 4º ed. 2002.

[47] G. J. Annas, *“HIPAA - Regulations - A New Era of Medical-Record Privacy ?,” New England Journal of Medicine*, Vol. 348(1. 2003, pp. 1486 – 1490.

[48] 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. 2004, pp. 297– 303.

[49] P. White, *“Privacy and security issues in teleradiology,” Seminars in Ultrasound, CT, and MRI*, Vol. 25. pp. 391-395, 2004.

[50] J. F. Weege, “Gestão de Risco – Segurança da Informação. 1.”

[51] I. Standard, *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management*, 1ª Ed. 2008.

[52] R. G. Johnston, “Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities,” vol. 4, no. 2, pp. 30–34, 2010.

[53] K. C. LAUDON and J. P. LAUDON, *Sistemas de informações gerenciais*, 5. ed. 2004.

[54] V. Management, “GUIDE 73 Risk management — Vocabulary Management du risque —,” 2009.

[55] G. DAWEL, *A Segurança da Informação nas Empresas*. Rio de Janeiro: Editora Ciência Moderna, 2005.

[56] A. BEAL, *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação das organizações*. São Paulo: Editora Atlas, 2005.

[57] E. Necessita, “Abnt nbr iso/iec 27002:2005,” 2007.

[58] F. Fonseca, “ISO / IEC 27005 Exemplificada,” *Apresentação*.

[59] M. Dey, *Information security management - a practical approach. In: Africon 2007 - 8th IEEE Africon Conference*. 2007, pp. p.1–6.

[60] A. A. Fernandes and V. F. Abreu, *Implantando a Governança de TI - da Estatégia à Gestão dos Processos e Serviços*, 2ª Ed. 2008.

[61] ISO, “ISO -International Organization for Standardization,” 2012. [Online]. Available: http://www.iso.org/iso/home/search.htm?qt=+27001&published=on&active_tab=standards&sort_by=rel. [Accessed: 30-Nov-2012].

[62] T. G. . Ngqondi, “The ISO / IEC 27002 and ISO / IEC 27799 Information Security Management Standards : A Comparative Analysis from a Healthcare Perspective,” Nelson Mandela Metropolitan University, 2009.

[63] C. E. Ribas, “Sistema de gestão de segurança da informação em organizações da área da saúde,” Faculdade de Medicina da Universidade de São Paulo, 2010.

[64] R. S. Rodrigues, “Estudo de um Processo Estruturado de Segurança da Informação em Sistemas de Informação do sector de Saúde com base na Norma ISO 27799:2008,” Centro Estadual de Educação Tecnológica Paula Souza, 2010.

[65] N. Brasileira, *ABNT NBR ISO / IEC 27001*, 1º Ed. 2006.

[66] Comunidade ISMS Portugal, “Comunidade Portuguesa de Segurança da Informação - Vantagens da certificação ISO 27001.” [Online]. Available: http://ismspt.blogspot.pt/2005/11/vantagens-da-certificao-iso-27001.html. [Accessed: 30-Nov-2012].

[67] I. Standard, “INTERNATIONAL STANDARD management in health using ISO 27799,” *Information Security*, vol. 2008, 2008.

[68] E. Kowask, *Gestão de Riscos de TI NBR 27005*. Rio de Janeiro: Escola Superior de Redes, 2011.

[69] I. Standard, “ISO/IEC 27799 - Health informatics — Information security management in health using ISO/IEC 27002,” 2008.

[70] R. Norton Cybercrime, “2012 NORTON CYBERCRIME REPORT,” 2012.

[71] T. Figueiró, “Vulnerabilidades diminuem, mas riscos aumentam,” *Computerworld*.

[72] C. P. Amador, *Natureza e perigosidade - Fichas de controlo de riscos ou prevenção*. .

[73] C. G. DE OLIVEIRA, “Doutoramento em Higiene , Segurança e Saúde no Trabalho Doctorado en Higiene , Salud y Seguridad en el Trabajo,” UNIVERSIDAD DE LEÓN, 2010.

[74] R. Pedro, “Métodos de Avaliação e Identificação de Riscos nos Locais de Trabalho,” *TECNOMETAL n.º 167 (Novembro/Dezembro de 2006)*, vol. 167, TECNOMETAL n.º 167 (Novembro/Dezembro de 2006), pp. 1–8, 2006.

[75] L. Ricogest, “Fornecimento de Serviços Externos para : Organização de Higiene e Segurança no Trabalho.” 2011.

[76] M. Colli, *Cibercrimes - Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos*. 2010, p. 208.

[77] A. Ambrosi, V. Peugeot, and D. Pimienta, *Desafios de Palavras: Enfoques Multiculturais sobre as Sociedades da Informação*. 2005.

[78] I. G. Institute, *Cobit 4.1 Modelo, Objectivos de Controle, Directrizes de Gestão e Modelos de Maturidade*. 2009, p. 212.

[79] I. Macfarlane, *An Introductory Overview of ITIL ® V3 An Introductory Overview of ITIL ® V3*. 2007.

[80] A. I. M. Pires, “Impacto da lei sarbanes-oxley no sistema de controlo interno das empresas cotadas nos eua o caso português,” p. 214, 2008.

[81] P. C. Fulgencio, *Glossário Vade Mecum: administração pública, ciências contábeis, direito, economia, meio ambiente*. 2007, p. 64.

[82] A. Martins, *Introdução à Análise Financeira de Empresas*, 2ª-edição ed. 2004, pp. 26–28.

[83] A. K. Ericsson, N. Charness, P. Feltovich, and R. R. Hoffman, *Cambridge handbook on expertise and expert performance*. Cambridge, UK: , 2006.

[84] L. Seguros, “SEGURANÇA NA INTERNET - ‘NAVEGAR EM SEGURANÇA’,” 2012. [Online]. Available: http://www.libertyseguros.pt/Tips.aspx?tabId=1859. [Accessed: 02-Nov-2012].

ANEXOS

Anexo A - Cibercriminalidade

1. Cibercrime

Pricewaterhouse Coopers (PwC)

Patrique Fernandes, Partner da PwC de Forensic Services em Portugal, salienta que:
"O crime económico continua a ser generalizado, afectando tanto as grandes como as pequenas organizações, em todo o mundo. Nenhuma empresa ou indústria é imune ao impacto causado pela fraude".
"Num mundo onde a maioria das empresas depende da tecnologia, há uma cada vez maior exposição ao risco de actividade criminosa, através de qualquer lugar do planeta desde que haja um computador, um smartphone ou qualquer outro dispositivo com acesso à internet. O aumento do número de incidentes de perda e roubo de dados, vírus, hackers e outras formas de crime económico demonstra a necessidade de uma abordagem mais pró-activa na prevenção de fraudes."

Cibercrime
No relatório da PwC, o cibercrime é classificado como um dos quatro crimes económicos mais frequentes. A percepção do cibercrime como uma ameaça predominantemente externa está a mudar, estando agora as organizações a reconhecer que o risco de cibercrime pode também surgir dentro da organização. Os inquiridos referem que o departamento de tecnologias da informação é a fonte interna mais provável de cibercrime. O departamento de TI foi assim citado por 53% dos inquiridos, seguido pelas Operações (39%), Vendas e Marketing (34%) e departamento Financeiro (32%).

Apesar da maioria dos inquiridos referir uma maior sensibilidade para a ameaça de cibercrime, a maioria deles refere que não tem, nem planeia ter, uma plano de combate ao cibercrime nas suas organizações. Além disso, 60% dos inquiridos referem que a sua organização não monitoriza as redes sociais.

A pesquisa da PwC permite ainda definir o perfil típico do defraudador interno que pratica cibercrime. De acordo com os inquiridos, são colaboradores juniores ou gestores de nível médio (85%), com idade inferior a 40 anos (65%) e colaboradores da organização há menos de cinco anos (50%).

A nível externo, os inquiridos apontam Hong Kong, China, Índia, Nigéria, Rússia e Estados Unidos da América como os países que constituem a maior ameaça na perpetração de cibercrimes.

Outras conclusões do survey:
• O crime económico é mais comum nas grandes organizações. 54% dos entrevistados, pertencentes a organizações com mais de 1000 colaboradores, relataram incidentes nos últimos 12 meses, comparativamente com 29% dos que pertencem a organizações com menos de 1000 colaboradores e 17% com menos de 200.
• A fraude atinge todos os tipos de organizações. 45% das vítimas foram entidades governamentais ou empresas do sector público, 40% estavam cotadas em bolsa e 12% eram outras empresas do sector privado.
• A fraude contabilística diminuiu acentuadamente desde 2009. A percentagem de inquiridos que relataram este tipo de fraude diminuiu 37% desde 2009, retomando os níveis apresentados em 2005.
• A maioria dos crimes económicos é cometida por indivíduos no interior das organizações (56%). 40% dos inquiridos relataram fraudes externas.
• A eficácia da detecção de crime económico tem vindo a diminuir desde 2007. As auditorias internas, os sistemas de gestão de risco e de denúncia, diminuíram a sua eficácia como meios para descobrir fraudes. O único método de detecção de fraude que aumentou a sua eficácia foi a monitorização de transacções suspeitas.
• Aqueles que procuram o crime económico encontram-no. As organizações que implementaram avaliações de risco de fraude detectaram e reportaram mais fraudes.

Retirado de:

http://www.pw□.□om/pt/pt/press-releases/2011/gloobale□onomi□rime-07-12-2011.jht... 30-03-2012

14. Dezembro 2011 - 08:10

Cada vez mais empresas vítimas de cibercrimes

Web, terreno fértil para as atividades criminais. (Keystone)

SOBRE O MESMO ASSUNTO

- Uma clínica para os "doentes" da comunicação
- Suíça se arma contra guerra cibernética
- Piratas devassam site do Forum de Davos
- Hackers atacam Ministério suíço das Relações Exteriores

Por **Matthew Allen**, swissinfo.ch

As empresas suíças tomam lentamente consciência de que seus negócios podem ser profundamente afetados pelos criminosos da internet. É o que revela uma pesquisa da consultoria PricewaterhouseCoopers (PwC).

Em 2011, o cibercrime foi o segundo delito mais frequente nas empresas suíças. Em 2012, poderá ser o primeiro.

As empresas suíças não estão mais expostas a ataques criminosos pela internet do que em outros países desenvolvidos. No entanto, a Suíça à um dos destinos mais sensíveis devido a importância de sua praça financeira e ao compromisso de sigilo bancário que tem com seus clientes.

Uma sondagem corporativa feita pela consultoria internacional PricewaterhouseCoopers (PwC) revelou que 18% das empresas na Suíça foram vítimas de algum tipo de fraude cibernética este ano. Assim, o chamado cibercrime é o segundo maior risco de fraude enfrentado atualmente pelas empresas.

De acordo com o estudo, mais de um terço dos 140 entrevistados suíços consideram que em 2012 o cibercrime será o delito mais frequente nas empresas, acima do desvio de dinheiro.

Controles insuficientes

A sofisticação técnica e a rápida evolução dos delitos cometidos através da web – através da pirataria de dados ou o *phising*, quer dizer, a fraude cibernética – deixam perplexos muitos altos executivos, o que complica os esforços institucionais para impor controles mas estritos.

"Entendem que o problema existe, porém a implementação de controles eficazes está no início", explica à swissinfo.ch Gianfranco Mautone, chefe do departamento jurídico da PwC.

De fato, atualmente, um em cada cinco ciberataques a empresas é detectado por acaso devido à intervenção de algum tipo de controle externo, afirma a PwC em seu relatório.

Comparados aos seus homólogos europeus, os executivos suíços perdem em tomada de consciência e de decisões em relação a esse problema. A pesquisa da PwC revela que metade das empresas suíças vê crescer o risco de ciberataques este ano, frente à média de 39% das empresas em escala mundial.

O certo é que muitas companhias só estão dispostas a fechar a porteira do estábulo quando o cavalo escapou. O roubo de CDs com dados bancários mostra como é fácil obter informações confidenciais, ignorando todo tipo de controle de segurança.

"Só quando os CDs roubados na Suíça começaram a ser vendidos em outros países é que os bancos começaram a se preocupar", acrescenta Mautone. Por vezes, "é preciso de problemas maiores para que as coisas mudem", continua.

Estragos em todos os níveis

O ciberataque de que foi objeto a bolsa de valores de Nova York (NYSE) há algumas semanas a obrigou a suspender temporariamente suas operações. Essa experiência deveria servir como advertência clara do dano quer pode causar o cibercrime, sublinha Mautone.

Porém, não somente os gigantes financeiros correm o risco de ser vítimas de delitos cometidos através da web, afirma o relatório da PwC. Na Suíça, milhares de pequenas e médias empresas (PME) poderiam ser presas fáceis e comprometer seriamente seu futuro.

"O cerne de muitas pequenas empresas são seus projetos e produtos inovadores que constituem suas vantagens competitivas. Perder esses ativos pode representar um desastre para as PME", adverte o especialista.

Na prática, as cifras demostram que o ciberdelito não é um problema somente das empresas, mas também de pessoas físicas, indivíduos. Todo ano são denunciados entre 6 e 7500 delitos cibernéticos às autoridades suíças, conforme dados do governo.

□grande maioria está ligada à pornografia, porém a Unidade Suíça de Coordenação para o Controle do Cibercrime recebeu em 2010 um total de 370 denúncias de delitos ligados à economia. Entre eles está o roubo de dados para aceder a contas bancárias. Um ano antes, haviam sido denunciados 254 casos.

Medid□s r□dic□s

Em todas as suas variantes, o cibercrime provocou perdas na Suíça de 924 milhões de francos em 2010, segundo estimativas da Symantec, empresa especializada na comercialização de *software* de segurança.

Com o intento de combater os riscos derivados do aumento deste tipo de delitos, as autoridades suíças elaboraram uma nova lei que entrará em vigor em 2012.

Será intensificada a troca de informação entre a Suíça e outros países, com penas mais severas para os *hackers* e uma linha telefônica aberta 24 horas por dia e 365 dias por ano para denunciar atividades suspeitas na matéria. Essas mudanças fazem a Suíça avançar em seu objetivo de firmar o Convênio Sobre Cibercriminalidade do Conselho da Europa.

O governo também prevê controlar os serviços postais e de telecomunicações, o que muitos consideram a criação de um potencial Big Brother público.

Enquanto a vigilância é destinada a pegar delinquentes de tráfico humano ou pedofilia, os opositores afirmam que esse tipo de medidas pode limitar também os direitos do indivíduo à privacidade.

Matthew □len, swissinfo.ch
□daptação: Claudinê Gonçalves

Retirado de:

http://www.swissinfo.ch/por/economia/Cada vez mais empresas vitimas de ciberc... 30-03-2012

2. Criminalidade

Manual de crimes para gente séria

António Freitas de Sousa
13/12/11 14:30

O crime económico não abranda. Pelo contrário. E até desenvolveu um novo campo de interesses: o cibercrime.

A *PricewaterhouseCoopers* (PwC) tem um estudo que evidencia essa nova realidade global. E propõe um guião de combate.

Desemprego, austeridade, recessão, quebra do PIB, quebra do consumo, quebra de confiança e as ruas escuras mesmo com as luzes do Natal, como se, com o plano de resgate da *'troika'*, o país tivesse também sido obrigado a usar o véu em tons cinzentos da tristeza mais funda que a Europa nos conseguiu entregar. E agora, juntando a isto tudo, o crime económico.

Muitos anos depois de iniciar a monitorização global do crime económico, a consultora PWC chegou a essa conclusão – teoricamente óbvia, mas que carecia de prova numérica: em cenário de crise económica, a incidência do crime económico tende a aumentar. Pior: a profundidade e a consistência da crise são diretamente acompanhadas pelo crescimento daquele tipo de crimes.

Patrique Fernandes é, na PwC Portugal, o responsável pelo gabinete de *'Forensic Services'* – que agrega cinco colaboradores dedicados ao aconselhamento, acompanhamento, monitorização e investigação (entre outras valias) do crime económico. Para ele, a evidência é clara: "O tempo de crise é um tempo de grande aumento do crime económico". Por duas razões principais, que se unem como um torniquete maligno: por um lado, "aumenta a propensão do defraudador para cometer crimes"; e, por outro, "as organizações baixam os seus orçamentos na área da prevenção".

No caso português, está, portanto, aberta a porta à disseminação do crime económico. Com uma agravante sociológica que Patrique Fernandes também deteta no território nacional: "Num país onde, por exemplo, fugir ao fisco não tem quaisquer repercussões sociais negativas" – de facto, fugir ao fisco tem laivos de heroicidade e não contornos de criminalidade – "está tudo dito".

Ou, se calhar, há mesmo duas agravantes sociológicas: àquela, junta-se também o facto de, "por razões que possivelmente se prendem com o regime anterior a 1974", a denúncia de ilícitos ser uma prática em relação à qual a generalidade das pessoas tem grande reserva. "Muitas das nossas entrevistas começam com os visados a informarem que nada dirão que possa ser usado contra pessoas concretas", conta Patrique Fernandes.

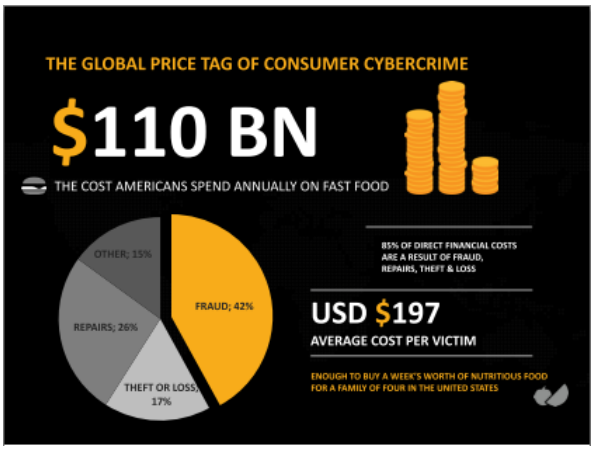
No ano passado, as organizações que recorreram aos serviços da PwC permitiram a deteção de crimes que agregaram uma estimativa de danos da ordem dos dez milhões de euros, sendo de supor que, no final do presente exercício, esse montante venha a crescer.

Norton Cybercrime Report 2012

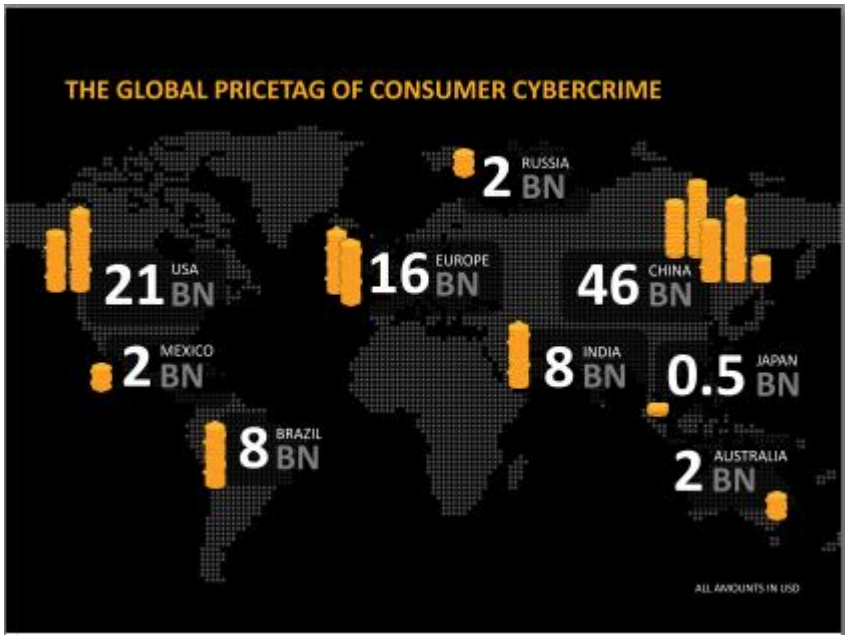
No estudo anual sobre o cibercrime realizado pela *Symantec* da qual resultou o relatório "Norton *Cybercrime Report* 2012" documento que analisa a evolução das atividades criminosas virtuais e seu impacto [70].

O relatório abrange diferentes tecnologias, incluindo e redes sociais e dispositivos móveis, relatando o impacto do cibercrime nos clientes em termos econômicos. O relatório envolveu 13.018 participantes em 24 países, com idades entre 18-64 e um conjunto de colaboradores especializados.

No conteúdo das imagens que se seguem, retiradas do relatório "Norton *Cybercrime Report* 2012" é elucidativo a dimensão mundial deste problema que todos os dias tornam vítimas mais de um milhão de pessoas e organizações [70].



O impacto do cibercrime está a ser muito preocupante, estando com 556 milhões de vítimas por ano, aproximadamente 1,5 milhões de vítimas por dia e 18 vítimas por segundo, com uma perda econômica total de 110 bilhões de dólares e um custo médio por vítima de US $197.



A região da Ásia é a mais afetada por crimes cibernéticos, com um valor global de cibercrime verificado na China de 46 bilhões, seguido pelos EUA com 21 bilhões e a Europa, com 16 bilhões de dólares. O valor mais baixo verifica-se no Japão com 0,5 biliões de dólares.
O maior número de vítimas de cibercrime verificou-se na Rússia (92 %), China (84 %) e África do Sul (80 %).

Embora estes dados devam ser considerados com alguma cautela, pois as diferentes abordagens do conceito de cibercriminalidade podem fazer variar as estimativas dos custos, é geralmente reconhecido que esta forma de criminalidade é altamente rentável e apresenta riscos reduzidos, o que a torna cada vez mais comum e nociva. Numa altura em que temos urgentemente de promover o crescimento económico, a intensificação da luta contra a cibercriminalidade pode permitir manter a confiança dos cidadãos e das empresas na segurança das comunicações e do comércio *online* [16].

3. Portugal em linha com o resto do mundo

A PWC acaba de editar o seu mais recente *'Global Economic Crime Survey'* (GECS, resultante de entrevistas a 3.877 responsáveis por organizações de 78 países diferentes), uma atualização a Novembro deste ano do que de mais relevante se passa no tendencialmente circunspecto mundo do crime económico - e a que o *Outlook* teve acesso em primeira mão. O estudo - que é 'refrescado' de dois em dois anos - revela um dado novo que deve ser devidamente ponderado pelas organizações: a cibercriminalidade chegou ao topo da lista dos crimes económicos mais difundidos e praticados a nível global.

De facto, e pela primeira vez, o cibercrime (palavra que há dez anos nem sequer fazia parte do léxico do 'economês') surge na quarta posição do GECS, logo a seguir à apropriação indevida de ativos, fraude contabilística e suborno e corrupção. O cibercrime é, além do mais, um campo de muito vasta atuação. Definamo-lo, por isso: segundo a PwC, compreende-se por cibercrime a utilização de plataformas informáticas e tecnológicas para a conclusão de crimes económicos, espionagem (muito usada na área da propriedade intelectual), terrorismo, ativismo (dando-se como exemplo a *Wikileaks*) e guerra (informática, entre Estados ou entre um Estado e uma organização privada).

O crescimento do cibercrime está diretamente relacionado com dois vetores: a confidencialidade de que o defraudador consegue usufruir se souber manejar devidamente as plataformas utilizadas; e o facto de os potenciais defraudados multiplicarem as possibilidades de ataque, ao usarem cada vez mais computadores portáteis, agendas eletrónicas, '*tablets*' '*smartphones*' e tudo o mais que está prestes a ser inventado, e que são de muito fácil invasão. A PwC faz esse alerta: um quadro superior de uma empresa tende a trazer no bolso do casaco um manancial de informações confidenciais sobre a sua organização que estão à distância de um 'clique' para qualquer *'hacker'* em início de carreira.

Portugal assistiu a semana passada, boquiaberto e razoavelmente impotente, à exemplificação no terreno do que isto quer dizer: Departamento Central de Acção e Investigação Penal, PSP, SIS, Portal das Finanças, Hospital da Cruz Vermelha, PS, PSD e CDS foram algumas das instituições que viram os seus *'sites'* devassados por alguém que provavelmente ninguém irá conhecer e estará neste momento cheio de vontade de rir.

Quando esta onda de assaltos teve início, a procuradora Maria José Morgado chamou a atenção para o facto de o orçamento nacional para combate ao crime informático ser ridículo, de tão baixo. Paralelamente, nos Estados Unidos, o combate ao cibercrime tem a maior dotação financeira logo a seguir ao terrorismo.

Entretanto, o GECS releva dados preocupantes: 40% do universo do estudo alega não ter forma, nas suas organizações, de controlar o cibercrime; 20% diz nunca ter tido qualquer treino específico no seu combate; 25% das organizações afirmam não estarem sequer despertas para o problema; 48% dos inquiridos teve a perceção de ter sido atingido por uma situação de cibercrime; 40% considera que este tipo de crime pode fazer enormes rombos na reputação de uma organização; e 46% das ocorrências vem de fora das organizações.

Ora, como tudo indica que o cibercrime tem tendência para crescer - como o próprio estudo indica - *Patrique* Fernandes propõe uma espécie de guião contra a sua ocorrência. Que incide, como é evidente, muito mais a montante que a jusante do problema. "É preciso definir, dentro de uma organização, aquilo a que se chama o triângulo da fraude: motivação, oportunidade e racionalização do ato" (quando o potencial defraudador considera ultrapassada a barreira da auto-inibição). Depois disso, é necessária uma avaliação do risco de fraude - nomeadamente através da sistematização das fraudes que podem ocorrer em determinada organização. E finalmente é preciso definir o que fazer em caso de ataque: a organização de um plano de contingência que minimize os danos e permita detetar os fautores.

Como não é nada provável que as organizações regressem aos velhos tempos da economia analógica – com faxes, máquinas de escrever, papel químico e pombos-correio – e, por outro lado, é igualmente improvável que a crise dê sinais certos de abrandamento nos próximos tempos, o mais acertado parece ser que cada organização se convença que o cibercrime não acontece só aos outros. Porque, de facto, nunca nada acontece até acontecer.

Retirado de:
http://economico.sapo.pt/noticias/manual-de-crimes-para-gente-seria_133337.html em 29-03-2012

4. CIBERCRIMES: Comissão Europeia propõe Centro Europeu de Cibercrime

A Comissão Europeia está a propor uma nova força de combate ao cibercrime integrada na Europol. Deverá chamar-se **Centro Europeu de Cibercrime** e deverá ficar sedeada em Haia, na Holanda.

A instituição deverá ser integrada na Europol, focada no desmantelamento de redes de cibercrime e não no controlo da partilha ilegal de ficheiros

A nova estrutura deverá custar cerca de 3,6 milhões de euros no primeiro ano, e pode iniciar as suas operações em Janeiro de 2012: a proposta ainda precisa de ser aprovada pela autoridade orçamental da Europol.

A Comissão Europeia parece querer endurecer as suas ações contra a cibercriminalidade. O centro terá uma administração autónoma, encarregue de identificar redes organizadas de cibercriminosos. Teria como função dar apoio operacional.

A Europol ajuda as forças da lei da União Europeia a trocarem informações sobre actividade criminal, mas não tem poderes executivos. Ele tem como alvo principalmente o tráfico de pessoas, drogas e veículos, o terrorismo, a contrafação de euros, e a lavagem de dinheiro.
Mas já tem um mandato para monitorizar actividades e ocorrências de cibercrime. O centro proposto deverá expandir essa responsabilidade adicionando poderes e capacidades de investigação forense digital e outros recursos, de acordo com um comunicado da Europol.
A comissária europeia para os assuntos internos, Cecilia *Malmström*, faz questão de sublinhar que o centro não abordará situações de partilha ilegal de ficheiros. Em vez disso, a comissária pretende que o centro neutralize grupos de crime organizado, focados em obter grandes margens de lucro.
Considerando dados da *PricewaterhouseCoopers* há muito trabalho a ser feito. A consultora descobriu que os ataques de cibercrime são responsáveis por 38% de todos os incidentes de crimes económicos que afetaram as empresas financeiras durante 2011.
Malmström citou também dados segundo os quais o impacto global do cibercrime está entre os 114 mil milhões de dólares e 388 mil milhões de dólares por ano. Só na Alemanha, os casos de *phishing* na banca online cresceram dois mil em número (2008), para cinco mil (2010).

EU proposes elite cybercrime unit (BBC)
Comissão Europeia propõe Centro Europeu de Cibercrime (*Computerworld* Portugal 28 de Março de 2012)

Retirado de:
http://estudosdeterrorismo2012.blogspot.pt/ em 29-03-2012

Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade. COM(2012) 140 final de 28.03.2012 [16]**.**

Todos os dias mais de um milhão de pessoas são vítimas da cibercriminalidade em todo o mundo. As atividades criminosas *online* vão desde a venda de cartões de crédito furtados por valores irrisórios, a usurpação de identidade e o abuso sexual de crianças, até aos ciber-ataques em grande escala contra as instituições e as infraestruturas. Os custos globais da cibercriminalidade para as nossas sociedades são consideráveis. Um relatório recente de 2011 revelou que as vítimas do cibercrime perdem anualmente cerca de 388 mil milhões de dólares em todo o mundo, o que torna este tipo de crime mais rentável que o conjunto do tráfico mundial de marijuana, cocaína e heroína.
Em resposta a estes desafios, a Comissão anunciou a sua intenção de criar um Centro Europeu da Cibercriminalidade, enquanto uma das prioridades da Estratégia de Segurança Interna. Após ter realizado um estudo de viabilidade para a criação de um organismo desse tipo a pedido do Conselho, a Comissão propõe que seja criado um Centro Europeu da Cibercriminalidade (EC3), que fará parte da Europol e deverá tornar-se o futuro ponto de convergência da luta contra a cibercriminalidade na EU [16].

Anexo B – Proteção de Dados

1. Falha na Proteção de Dados

14 | PORTUGAL | PÚBLICO, SEX 18 MAI 2012

Dados pessoais de 220 mil estudantes estiveram acessíveis no *site* da DGES

Erro da plataforma de candidatura a bolsas de estudo permitia conhecer nomes e números do BI e contribuinte de alunos e pais. Sistema deixou ontem de estar acessível, depois de detectado o problema

Ensino Superior
Samuel Silva

Os dados pessoais de 220 mil estudantes bolseiros do ensino superior estiveram acessíveis durante várias semanas no *site* da Direcção-Geral do Ensino Superior (DGES). A situação foi ontem corrigida pela empresa responsável pelo desenvolvimento da plataforma, mas vai ser investigada pela Comissão Nacional de Protecção de Dados (CNPD).

Os nomes completos e os números dos bilhetes de identidade e de identificação fiscal dos mais de 220 mil alunos candidatos a bolsas de estudo podiam ser consultados sem grandes dificuldades numa área específica do *site* da DGES. O sistema permitia também aceder aos mesmos dados pessoais dos pais e restantes elementos do agregado familiar destes estudantes do ensino superior.

O problema prendia-se com o acesso à área reservada do *site* a bolseiros, que era feita através de um endereço inseguro, que podia ser manipulado. O *link* à vista no *browser* (programa de navegação na Internet) de qualquer computador mostrava os parâmetros de acesso "ID" preenchidos com vários X. Substituindo os X pelos números de contribuinte ou de BI dos estudantes era possível aceder a essa zona do *site*. Uma vez ultrapassada a barreira, os dados pessoais estavam inteiramente disponíveis.

Uma denúncia anónima fez com que o portal pplware.com, associado à rede Sapo Tek, tivesse detectado o problema, dando origem a uma publicação naquele *site* feita anteontem. A forma como a notícia se começou a espalhar levou também o Ministério da Educação e Ciência (MEC) e a DGES a olhar para o caso e, a meio do dia de ontem, já havia uma solução, ainda que temporária.

O endereço de acesso à zona "reservada" a candidatos foi desactivado, o que impede agora o acesso à área onde os dados pessoais estavam acessíveis. A solução não corrige, todavia, o problema em definitivo. Numa nota escrita enviada ao PÚBLICO, o MEC garante que "têm vindo e estão a ser desenvolvidos os procedimentos normais nestas circunstâncias, designadamente em matéria de auditoria informática".

A situação só ontem foi corrigida e será investigada pela Comissão Nacional de Protecção de Dados

"O endereço já não se encontrava acessível através da plataforma de candidatura, onde tinha sido substituído, na sequência da adopção de um método diferente de geração de formulários", informa o gabinete de Nuno Crato. Segundo o ministério, "nunca esteve em risco a divulgação de qualquer informação acerca, designadamente, dos rendimentos e património dos candidatos e do seu agregado familiar". Além disso, a consulta da informação através do endereço em causa "não era possível por engano ou casualidade", obrigando a uma "deliberada e intencional" manipulação de dados, uma prática que é ilegal, explica o MEC.

Comissão em campo

O caso foi também detectado no início desta semana pela CNPD, dando origem a um procedimento interno que deverá motivar um processo de averiguações por parte daquele organismo. De acordo com a CNPD, nenhuma queixa relativa a esta situação deu até agora entrada nos seus serviços.

A plataforma de acesso a bolsas de estudo foi desenvolvida pela empresa Brightpartners, com quem a DGES tem quatro contratos registados no portal da contratação pública. Desde 2010, a firma recebeu mais de 400 mil euros relativos a quatro serviços de "manutenção e assistência técnica de *software* informático de suporte" ao concurso de atribuição de bolsas de estudo. Os contratos são renovados anualmente e o último foi lançado no portal em Fevereiro deste ano, com um valor de 76 mil euros.

O *site* está activo há cerca de dois anos e foi a solução encontrada para uniformizar as candidaturas dos estudantes às bolsas de estudo. A inovação nunca foi, porém, imune a críticas, tendo sido criticada por alguns responsáveis dos serviços de acção social devido à sua complexidade. Essa questão terá também contribuído para os atrasos verificados na análise das candidaturas no início do ano lectivo passado. De resto, a única instituição de ensino superior que não usa a plataforma da DGES, preferindo um sistema informático próprio, é a Universidade do Minho, que, nos últimos dois anos, foi a primeira a terminar o processo de atribuição dos apoios aos estudantes.

Retirado de: Jornal o Público, 18.Mai.2012

Anexo C – Estatística sobre Segurança Hospitais e Empresas

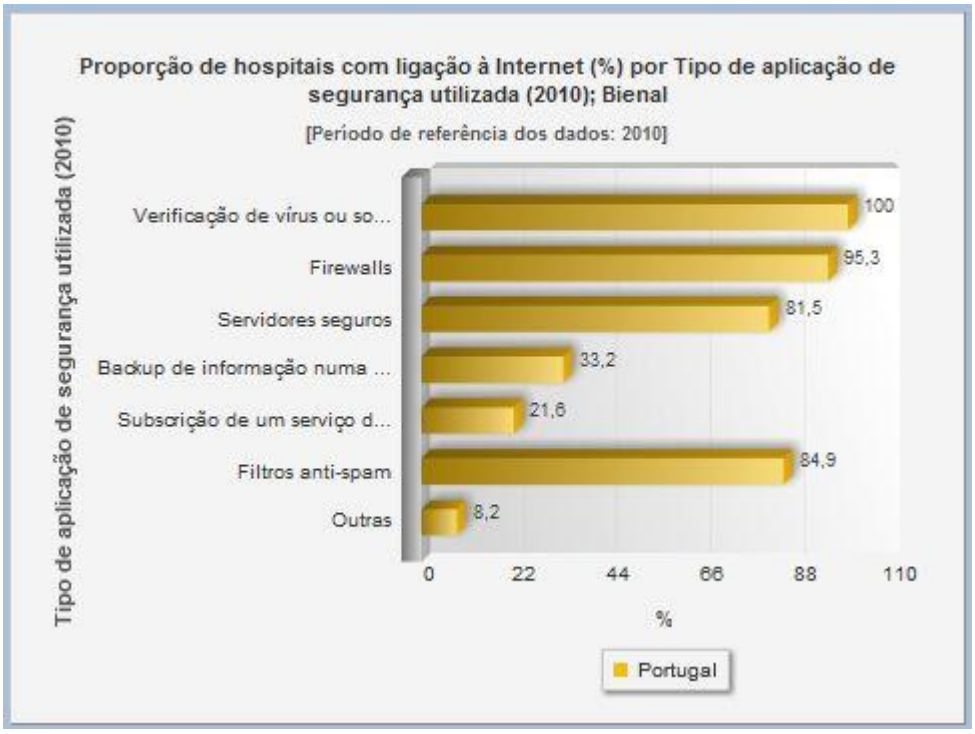
1. Hospitais (alguns dados estatísticos sobre segurança)

Internet – Estatística por tipo de Aplicação de segurança utilizada (2010)

Período de referência dos dados	Tipo de aplicação de segurança utilizada (2010)	Proporção de hospitais com ligação à Internet (%) por Tipo de aplicação de segurança utilizada (2010); Bienal
		Localização geográfica
		Portugal
		%
2010	Verificação de vírus ou software de segurança	100,0
	Firewalls	95,3
	Servidores seguros	81,5
	Backup de informação numa localização externa ao estabelecimento	33,2
	Subscrição de um serviço de segurança	21,6
	Filtros anti-spam	84,9
	Outras	8,2

Proporção de hospitais com ligação à Internet (%) por Tipo de aplicação de segurança utilizada (2010); Bienal - INE, Inquérito à Utilização das Tecnologias de Informação e de Comunicação nos Hospitais

Última atualização destes dados: 04 de março de 2011



Retirado de: www.ine.pt - em 04-05-2012

Tabela V.6 **Hospitais por tipo de equipamentos e serviços informáticos utilizados**
(%) Hospitais

	2004	2006	2008	2010
Redes				
LAN (*Local Area Network*)	88	90	92	91
Intranet	70	77	78	74
Wireless LAN	17	34	45	62
WAN (Wide Area Network)	37	42	44	59
Redes virtuais privadas (VPN)	x	21	37	52
Extranet	36	36	38	40
Aplicações				
Correio electrónico	87	93	93	97
Software médico	x	55	64	78
Videoconferência	21	22	20	22
Segurança				
Software anti-vírus	93	98	99	100
Firewall	66	83	92	95
Filtros *anti-spam*	x	62	77	85
Servidores seguros	x	x	x	82
Backup de informação numa localização externa ao hospital	x	x	x	33
Subscrição de um serviço de segurança	x	x	x	22

Fonte(s): INE/UMIC, Inquérito à Utilização de Tecnologias da Informação e da Comunicação nos Hospitais.

Tabela V.7 **Hospitais por tipo de actividades informatizadas**
(%) Hospitais

	2004	2006	2008	2010
Actividades gerais				
Gestão financeira e administrativa	94	92	94	93
Gestão de *stocks* farmacêuticos	81	86	84	88
Gestão de recursos humanos	84	88	89	87
Marcação de tratamentos e consultas	79	84	84	86
Gestão de fornecedores	x	x	x	86
Troca interna de ficheiros	74	75	79	85
Gestão de *stocks*	84	87	81	80
Gestão de meios complementares	x	70	69	79
Gestão de listas de espera	x	55	58	65
Troca interna de imagens médicas	x	30	44	60
Planeamento e calendarização de actividades	30	43	47	54
Gestão de correspondência	38	42	46	47
Comunicação interna	37	49	60	x
Gestão de serviços de hotelaria	23	33	36	x
Gestão documental / Centros de comunicação	18	23	28	x
Actividades médicas				
Serviço de internamento	x	76	77	86
Serviço de consulta externa	67	71	73	83
Base de dados da informação clínica dos pacientes	39	46	48	75
Base de dados da informação relativa ao corpo médico	40	42	43	63
Bloco operatório	52	52	47	62
Processo clínico electrónico	42	30	36	60
Serviço de urgência	48	44	46	53

Fonte(s): INE/UMIC, Inquérito à Utilização de Tecnologias da Informação e da Comunicação nos Hospitais.

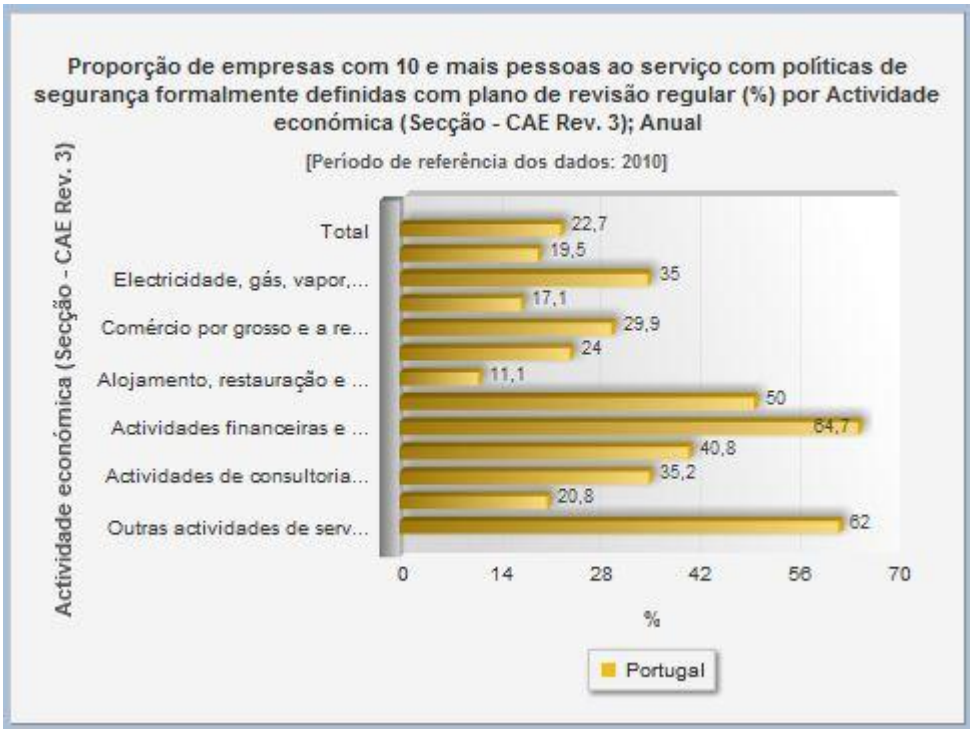
Universo de hospitais em (**2004**: 203 ; **2006**: 198 ; **2008**: 194 ; **2010**: 235)
Retirado de: A sociedade da informação em Portugal 2010 - em 04-05-2012

2. Empresas (alguns dados estatísticos sobre segurança)

Período de referência dos dados	Actividade económica (Secção - CAE Rev. 3)	Proporção de empresas com 10 e mais pessoas ao serviço com políticas de segurança formalmente definidas com plano de revisão regular (%) por Actividade económica (Secção - CAE Rev. 3); Anual
		Localização geográfica
		Portugal
		%
2010	Total	22,7
	Indústrias transformadoras	19,5
	Electricidade, gás, vapor, água quente e fria e ar frio. Captação, tratamento e distribuição de água; saneamento, gestão de resíduos e despoluição	35,0
	Construção	17,1 §
	Comércio por grosso e a retalho; reparação de veículos automóveis e motociclos	29,9
	Transportes e armazenagem	24,0 §
	Alojamento, restauração e similares	11,1 §
	Actividades de informação e de comunicação	50,0
	Actividades financeiras e de seguros (grupos/classes 64.19, 64.92, 65.1, 65.2, 66.12, 66.19)	64,7
	Actividades imobiliárias	40,8
	Actividades de consultoria, cientificas, técnicas e similares (divisão 69-74)	35,2
	Actividades administrativas e dos serviços de apoio	20,8
	Outras actividades de serviços (grupo 95.1)	62,0

Proporção de empresas com 10 e mais pessoas ao serviço com políticas de segurança formalmente definidas com plano de revisão regular (%) por Actividade económica (Secção - CAE Rev. 3); Anual - INE, Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas

Última atualização destes dados: 04 de novembro de 2011

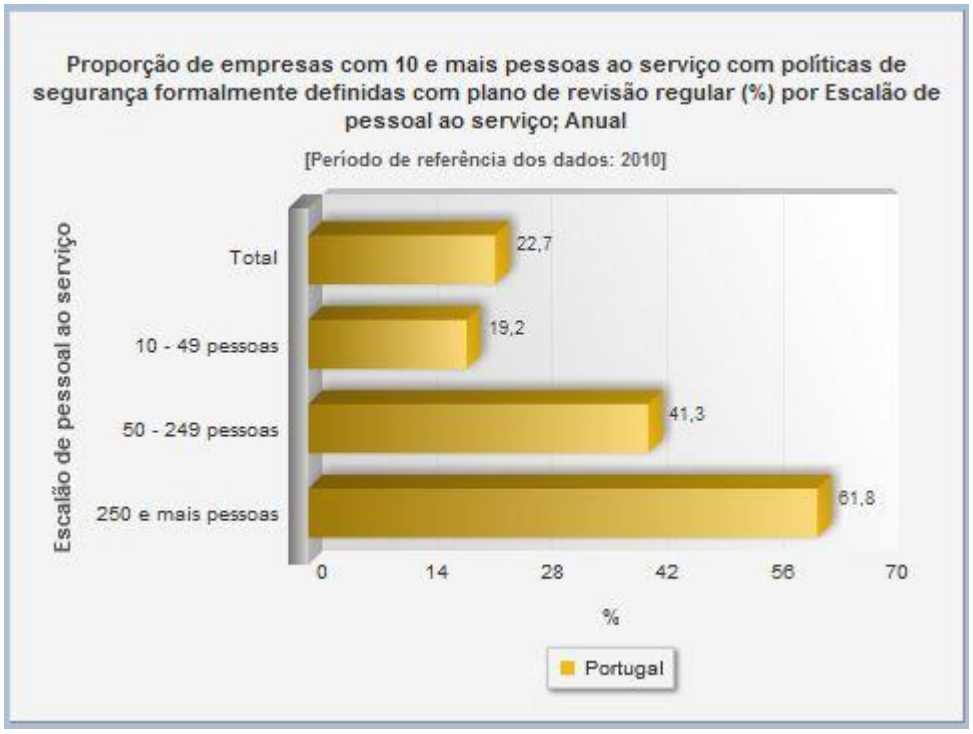


Retirado de: www.ine.pt - em 04-05-2012

Período de referência dos dados	Escalão de pessoal ao serviço	Proporção de empresas com 10 e mais pessoas ao serviço com políticas de segurança formalmente definidas com plano de revisão regular (%) por Escalão de pessoal ao serviço; Anual
		Localização geográfica
		Portugal
		%
2010	Total	22,7
	10 - 49 pessoas	19,2
	50 - 249 pessoas	41,3
	250 e mais pessoas	61,8

Proporção de empresas com 10 e mais pessoas ao serviço com políticas de segurança formalmente definidas com plano de revisão regular (%) por Escalão de pessoal ao serviço; Anual - INE, Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas

Última atualização destes dados: 04 de novembro de 2011



Retirado de: www.ine.pt - em 04-05-2012

1.8 Segurança

Tabela VI.60 Empresas com política de segurança das TIC formalmente definida e com um plano de revisão regular

(%) Empresas com 10 ou mais pessoas ao serviço e com actividade económica em Portugal

	2010
Empresas com política de segurança das TIC formalmente definida e com um plano de revisão regular	23

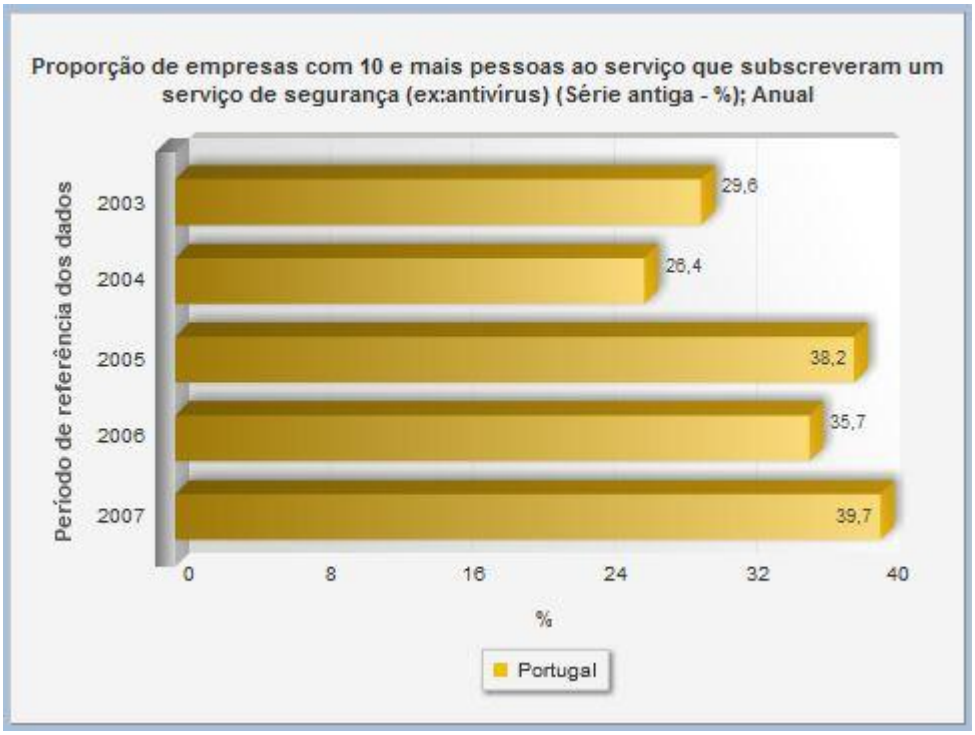
Fonte(s): INE/UMIC, Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas.

Universo de empresas em (**2004**: 2 809 ; **2006**: 2 529 ; **2008**: 2 751 ; **2010**: 2 843)
Retirado de: A sociedade da informação em Portugal 2010 - em 04-05-2012

Período de referência dos dados	Proporção de empresas com 10 e mais pessoas ao serviço que subscreveram um serviço de segurança (ex:antivírus) (Série antiga - %); Anual
	Localização geográfica
	Portugal
	%
2007	39,7
2006	35,7
2005	38,2
2004	26,4
2003	29,6

Proporção de empresas com 10 e mais pessoas ao serviço que subscreveram um serviço de segurança (ex:antivírus) (Série antiga - %); Anual - INE, Utilização de tecnologias da informação e da comunicação nas empresas

Última atualização destes dados: 30 de abril de 2008



Retirado de: www.ine.pt - em 04-05-2012

Anexo D - Vulnerabilidades e Ataques

1. Internet e a implicação nas vulnerabilidades dos sistemas e ataques.

A Internet foi concebida de forma a ser utilizada facilmente por organizações e pessoas com sistemas de informação diferentes. Atualmente está muito popularizada por todo o mundo e é cada vez mais, utilizada como meio de comunicação. Milhões de utilizadores de todas as fachas etárias, culturas, estratos sociais, crenças, etc., usam diariamente a Internet, e apesar de ser um meio versátil e uma fonte inesgotável de recursos, apresenta problemas especiais e muitos perigos associados, isto é vulnerabilidades, algumas das quais descritas nos parágrafos que se seguem.

Das muitas funcionalidades ou serviços disponibilizados na Internet, o correio eletrónico[48] um dos mais utilizados pode apresentar os seus perigos. Um dos perigos mais comuns é a propagação de vírus e consequente infeção dos computadores de utilizadores domésticos e empresariais.

As mensagens instantâneas[49] e sala de conversação[50] podem ser locais perigosos para crianças e jovens, nunca se tem a certeza de quem é o cibernauta que se encontra do outro lado. Os *chatrooms* são um local privilegiado para os pedófilos angariarem crianças desprevenidas, pelo que é importante preparar e educar os mais novos acerca dos potenciais perigos (ameaças) existentes nestes meios.

As redes sociais virtuais[51] devido a sua grande implementação e popularidade é de extrema importância que o utilizador conheça as formas de se proteger contra possíveis ameaças resultantes das vulnerabilidades que este tipo de serviço suportado pela Internet apresenta.

Uma das conclusões do relatório anual de riscos e tendências da IBM, dizia que [71]:

> "O número global de vulnerabilidades detetadas em aplicações de *software* caiu em 2009, mas por outro lado a quantidade de erros em leitores de documentos e aplicações de multimédia cresceu cerca de 50 por cento."

[48] Correio eletrónico (e-mail de "*electronic mail*"): - consiste num meio de enviar mensagens escritas pela Internet e que tem a vantagem de ser recebido quase instantaneamente pelo destinatário [84].

[49] Mensagens Instantâneas (IM de *"Instant Messaging"*): - é uma forma fácil de manter contacto com alguém sem ter que esperar por um e-mail. Exemplo *Skype*, MSM *Messeger* [84].

[50] Sala de Conversação (chat de *"chatroom"*): - é um local *online* destinado a juntar várias pessoas para conversarem. Este local pode ser de índole generalista, ou pode destinar-se à discussão de um tema em particular [84].

[51] Redes Sociais Virtuais: - é um reflexo da necessidade de comunicar aplicado às redes *Web*. É deste modo que o sujeito se apresenta aos restantes internautas, quer seja através de páginas pessoais ou através de blogues, mostrando-se ao mundo dos mais diversos modos: por fotografias, pela escrita, por vídeos [84].

A investigação foi feita pelo grupo X-Force, da IBM, que recolheu registos de vulnerabilidades e outros dados de ataques realizados através da *Web*[52]. Em 2009, a equipa do X-Force registou 6,6 mil novas vulnerabilidades, 11 por cento menos do que o registado em 2008. No que se refere às falhas de segurança, a IBM conta que o número de vulnerabilidades reportadas em leitores de documentos, editores e aplicações de multimédia subiu 50 por cento. A empresa classifica estas vulnerabilidades estando elas do lado do cliente, categoria que também inclui vulnerabilidades que afetam navegadores (*browsers)* e sistemas operativos. Das cinco falhas mais exploradas na *Web*, três envolvem arquivos PDF. Os ciber-criminosos têm tido muito sucesso na procura de vulnerabilidades no *software* da Adobe e conduzidos os seus ataques através de campanhas de spam e sites maliciosos.

Mas são os *browsers* os que possuem a maior parte das vulnerabilidades detetadas, sendo que o *Firefox* registou o dobro das falhas críticas do Internet Explorer em 2009. Nenhum destes erros, no entanto, ficou por corrigir até ao final do ano. Mais de metade das vulnerabilidades críticas diz respeito a quatro fabricantes em específico: Microsoft, Adobe, Mozilla e Apple. Enquanto, em média, a maioria dos fornecedores corrigiu 66 por cento dessas falhas, a Apple mostrou ser a pior neste ponto, corrigindo apenas 38 por cento das suas vulnerabilidades.

Outras vulnerabilidades observadas pela X-Force incluem as aplicações *Web*, algo que é particularmente perigoso para os *sites* e que pode resultar na perda de dados e outros danos. E os números aqui não são bons: cerca de 67 por cento dos problemas com aplicações *Web* não foram corrigidos até o fim de 2009. O *cross-site scripting*[53] superou a *SQL injection*[54] como principal vulnerabilidade na *Web*, disse a IBM. O número de *SQL injections* observado pela IBM em 2008 foi de cerca de 5 mil por dia. Em 2009, o grupo X-Force observou cerca de um milhão de ataques por dia, com os atacantes a usar sobretudo ferramentas especialmente concebidas para descobrir *sites* vulneráveis [71].

Pode-se concluir que a vulnerabilidade é a maior fraqueza ou lacuna que requer por parte das organizações, os maiores esforços de proteção possível, para que não esteja exposta,

[52] *WEB* (WWW de "*World Wide Web*") é a parte multimédia da Internet, que permite que sejam exibidas páginas de hipertexto, ou seja, documentos que podem conter todo o tipo de informação: textos, fotos, animações, trechos de vídeo e sons e programas e, especialmente, que permite conexões entre documentos (links). Na Internet a informação é colocada em documentos denominados páginas *Web* que estão sitiados em "*sites*".

[53] *Cross-site Scripting*: - é um ataque no qual um *script* ganha permissão para ser executado onde não deve, recurso que pode ser usado pelos *hackers* para roubarem informação [71].

[54] *SQL Injection*: - ocorre quando determinados comandos são validados e executados numa base de dados, que pode revelar as suas informações e ser usada para fins maliciosos [71].

isto é, esteja devidamente salvaguardada de qualquer potencial ameaça, de modo a evitar qualquer hipótese de ataque, e consequentemente concretização do risco.

A norma ISO/IEC 27005:2008 tipifica no seu anexo D, o exemplo de vulnerabilidades mais comuns que estão associados aos Sistemas de Informação, transcritas neste documento no anexo F.4 (Catálogo Vulnerabilidades mais comuns “Tipos e Ex. Ameaças”), página 178.

Se analisarmos o que acontece na Internet, verificamos que os ataques acontecem permanentemente, à uma razão de vários ataques por minuto sobre qualquer máquina que esteja liga a internet. Estes ataques são, na sua maior parte, lançados automaticamente a partir de máquinas infetadas por (vírus, cavalo de troia, *trojans*, etc.), na maior parte das vezes sem o conhecimento do seu proprietário, situações em que, nem sempre se trata da ação de piratas informáticos. Nos parágrafos anteriores foram referidos alguns dados estatísticos e exemplos de ataques realizados através da *Web.*

Quando se está perante um ataque, não significa que este terá o sucesso desejado por quem o está a efetuar, o nível de sucesso de um ataque dependerá da vulnerabilidade do sistema, isto é dos seus ativos, da atividade e eficácia das contramedidas existentes.

Anexo E – Questionário sobre SGSI

1. Questionário sobre Implementação de SGSI

Estudo sobre a Implementação de Sistemas de Gestão de Segurança da Informação (SGSI)

Exmo(s). Senhor(es),

Encontro-me a realizar um Projecto de Dissertação/Tese sobre o Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde, na Escola Superior de Tecnologia da Saúde de Coimbra (ESTeSC) / Instituto Superior de Engenharia de Coimbra (ISEC) do Instituto Politécnico de Coimbra, sob a orientação do Doutor António Manuel Rodrigues Carvalho dos Santos e coorientação do Mestre João Nuno Freitas de Almeida.
Neste âmbito, estou a realizar uma investigação que permitira determinar qual o grau de implementação de um SGSI atualmente no mercado nacional, utilizando como universo de estudo 500 organizações nacionais das diversas áreas de actividade.
As respostas são estritamente confidenciais e têm meramente um objetivo estatístico para estudo académico.
A sua resposta é importante para a real valorização do inquérito e do meu estudo, peço-lhe apenas 5 minutos do seu tempo para responder de forma sucinta (um click por questão) a 12 questões.

Se pretender, terei todo o gosto em enviar-lhe o resultado deste estudo, bastando para tal colocar o seu e-mail no final do questionário.
No entanto se tiver qualquer duvida agradeço que envie um e-mail para: frvilhena@iol.pt ou a9705057@alunos.isec.pt ou que ligue para 91 87 100 82.

Antecipadamente, Muito Obrigado.

Francisco Carvalho

Questões colocadas no Questionário

1. A Segurança de Informação têm grande relevância para a sua organização ?

- Sim
- Não

2. Acha que a forma mais adequada de o fazer é através de um processo, que resultante de:

- Medidas isolados e informais
- Medidas conjuntas, integradas e monitorizadas
- Implementação de um SGSI (Sistema de Gestão de Segurança da Informação)
- Outra:

3. Conhece a norma ISO/IEC 27001?

- Sim
- Não

4. Conhece a norma ISO/IEC 27002?

- Sim
- Não

5. Conhece a norma ISO/IEC 27799?

- Sim
- Não

6. Têm implementado algum SGSI ?

- Sim, baseada na norma ISO/IEC 27001
- Sim, baseada na norma ISO/IEC 27002
- Sim, baseada na norma ISO/IEC 27799
- Não
- Outra:

7. Gostaria de implementar um SGSI ?

- Sim, baseada na norma ISO/IEC 27001
- Sim, baseada na norma ISO/IEC 27002
- Sim, baseada na norma ISO/IEC 27799
- Não
- N/A (Não se Aplica)
- Outra:

8. Com que obejctivo gostaria de implementar um SGSI ?

- Garantir a melhor solução para segurança da informação
- Garantir a melhor solução para segurança da informação + Certificação
- Certificação
- N/A (Não se Aplica)
- Outra:

9. Esta satisfeito com a solução que têm implementada ?

- Sim
- Não
- N/A (Não se Aplica)
- Outra:

10. Que valor atribui a dificuldade de implementação de um SGSI ?

Escolha uma das opções de 1 a 5.

	1	2	3	4	5	
Facil						Dificil

11. Qual é a área de actividade da empresa ?

- Comércio
- Distribuição
- Ensino
- Estado
- Financeira
- Serviços
- Industria
- Saúde (sector público)
- Saúde (sector privado)
- Outra:

12. Quantos trabalhadores tem a empresa ?

Escolha uma das opções.

< 21

Endereço de e-mail:

Se pretender receber o resultado do estudo.

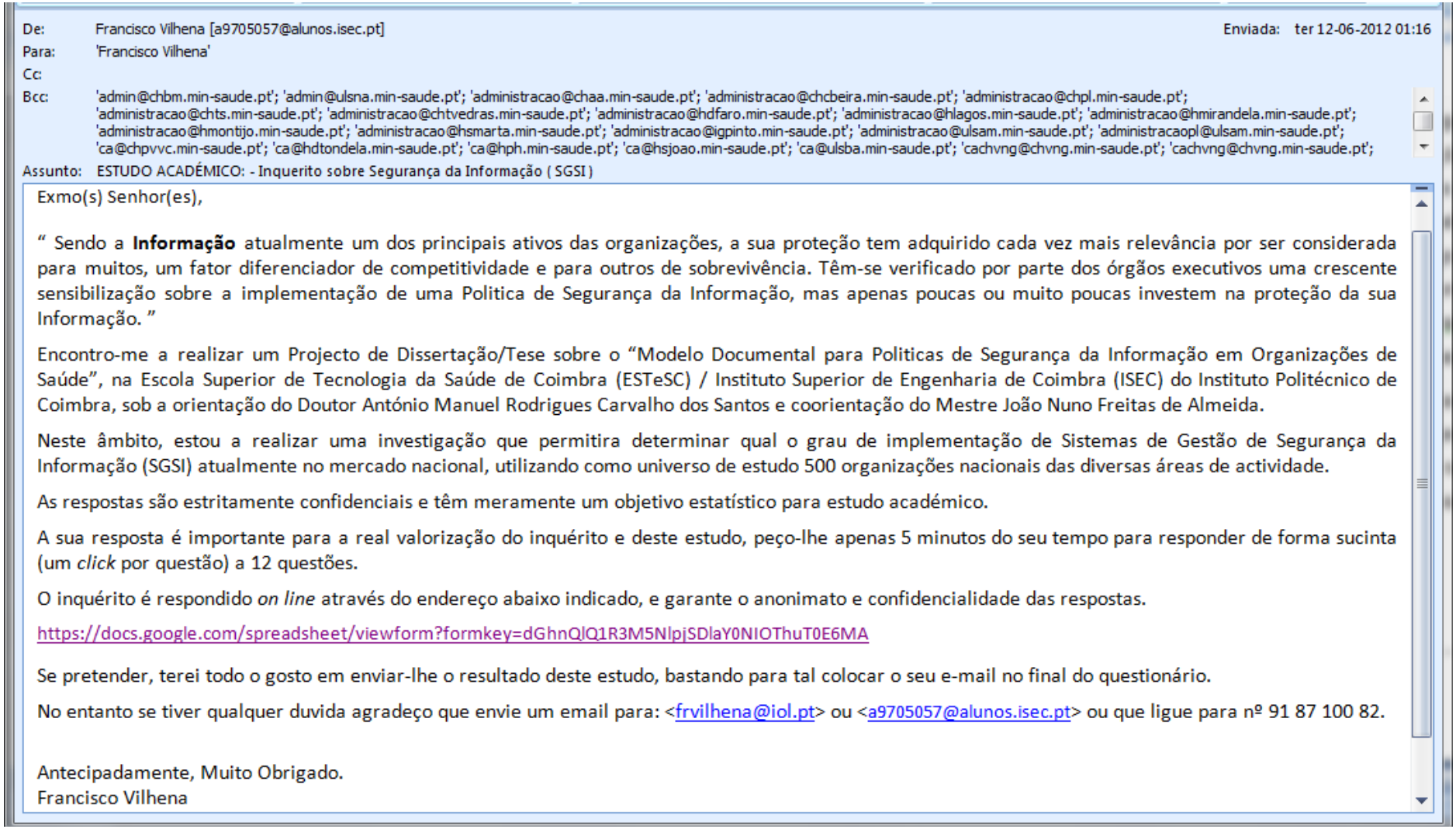
Comentário / OBS:

Caso queira acrescentar algum registo importante para este estudo.

Enviar

2. Email Enviado

***Email* Enviado**



De: Francisco Vilhena [a9705057@alunos.isec.pt] Enviada: ter 12-06-2012 01:16

Para: 'Francisco Vilhena'

Cc:

Bcc: 'admin@chbm.min-saude.pt'; 'admin@ulsna.min-saude.pt'; 'administracao@chaa.min-saude.pt'; 'administracao@chcbeira.min-saude.pt'; 'administracao@chpl.min-saude.pt'; 'administracao@chts.min-saude.pt'; 'administracao@chtvedras.min-saude.pt'; 'administracao@hdfaro.min-saude.pt'; 'administracao@hlagos.min-saude.pt'; 'administracao@hmirandela.min-saude.pt'; 'administracao@hmontijo.min-saude.pt'; 'administracao@hsmarta.min-saude.pt'; 'administracao@igpinto.min-saude.pt'; 'administracao@ulsam.min-saude.pt'; 'administracaopl@ulsam.min-saude.pt'; 'ca@chpvvc.min-saude.pt'; 'ca@hdtondela.min-saude.pt'; 'ca@hph.min-saude.pt'; 'ca@hsjoao.min-saude.pt'; 'ca@ulsba.min-saude.pt'; 'cachvng@chvng.min-saude.pt'; 'cachvng@chvng.min-saude.pt';

Assunto: ESTUDO ACADÉMICO: - Inquerito sobre Segurança da Informação (SGSI)

Exmo(s) Senhor(es),

" Sendo a **Informação** atualmente um dos principais ativos das organizações, a sua proteção tem adquirido cada vez mais relevância por ser considerada para muitos, um fator diferenciador de competitividade e para outros de sobrevivência. Têm-se verificado por parte dos órgãos executivos uma crescente sensibilização sobre a implementação de uma Politica de Segurança da Informação, mas apenas poucas ou muito poucas investem na proteção da sua Informação. "

Encontro-me a realizar um Projecto de Dissertação/Tese sobre o "Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde", na Escola Superior de Tecnologia da Saúde de Coimbra (ESTeSC) / Instituto Superior de Engenharia de Coimbra (ISEC) do Instituto Politécnico de Coimbra, sob a orientação do Doutor António Manuel Rodrigues Carvalho dos Santos e coorientação do Mestre João Nuno Freitas de Almeida.

Neste âmbito, estou a realizar uma investigação que permitira determinar qual o grau de implementação de Sistemas de Gestão de Segurança da Informação (SGSI) atualmente no mercado nacional, utilizando como universo de estudo 500 organizações nacionais das diversas áreas de actividade.

As respostas são estritamente confidenciais e têm meramente um objetivo estatístico para estudo académico.

A sua resposta é importante para a real valorização do inquérito e deste estudo, peço-lhe apenas 5 minutos do seu tempo para responder de forma sucinta (um *click* por questão) a 12 questões.

O inquérito é respondido *on line* através do endereço abaixo indicado, e garante o anonimato e confidencialidade das respostas.

https://docs.google.com/spreadsheet/viewform?formkey=dGhnQlQ1R3M5NlpjSDlaY0NIOThuT0E6MA

Se pretender, terei todo o gosto em enviar-lhe o resultado deste estudo, bastando para tal colocar o seu e-mail no final do questionário.

No entanto se tiver qualquer duvida agradeço que envie um email para: <frvilhena@iol.pt> ou <a9705057@alunos.isec.pt> ou que ligue para nº 91 87 100 82.

Antecipadamente, Muito Obrigado.
Francisco Vilhena

3. Lista de Organizações ou Empresas

Lista de Organizações ou Empresas

Relação de e-mail's enviados - HOSPITAIS (ambito nacional SNS)			
Nº	***Organização***	***Endereço de e-mail***	***Resultado Envio***
	Hospital dos Marmeleiros		Não enviado
	Hospital Dr. Nélio Mendonça		Não enviado
1	Hospital Nossa Senhora do Rosário (Centro Hospitalar Barreiro Montijo, EPE)	admin@chbm.min-saude.pt	enviado - 12.06.2012
2	Hospital Dr. José Maria Grande - Portalegre (Unidade Local de Saúde do Norte Alentejano, EPE)	admin@ulsna.min-saude.pt	enviado - 12.06.2012
	Hospital Santa Luzia de Elvas (Unidade Local de Saúde do Norte Alentejano, EPE)	admin@ulsna.min-saude.pt	Não enviado
3	Unidade Hospitalar de Fafe (Centro Hospitalar do Alto Ave, EPE)	administracao@chaa.min-saude.pt	enviado - 12.06.2012
	Unidade Hospitalar de Guimarães (Centro Hospitalar do Alto Ave, EPE)	administracao@chaa.min-saude.pt	Não enviado
4	Hospital Pêro da Covilhã (Centro Hospitalar Cova da Beira, EPE)	administracao@chcbeira.min-saude.pt	enviado - 12.06.2012
	Unidade Hospitalar de Santo Tirso (Centro Hospitalar do Médio Ave, EPE)	administracao@chma.min-saude.pt	Não enviado
	Unidade Hospitalar de Famalicão (Centro Hospitalar do Médio Ave, EPE)	administracao@chma.min-saude.pt	Não enviado
5	Hospital Júlio de Matos (Centro Hospitalar Psiquiátrico de Lisboa)	administracao@chpl.min-saude.pt	enviado - 12.06.2012
6	Hospital Padre Américo, Vale do Sousa (Centro Hospitalar Tâmega e Sousa, EPE)	administracao@chts.min-saude.pt	enviado - 12.06.2012
7	Hospital Distrital Torres Vedras (Centro Hospitalar de Torres Vedras)	administracao@chtvedras.min-saude.pt	enviado - 12.06.2012
8	Hospital de Faro, EPE	administracao@hdfaro.min-saude.pt	enviado - 12.06.2012
9	Hospital Distrital de Lagos (Centro Hospitalar do Barlavento Algarvio, EPE)	administracao@hlagos.min-saude.pt	Não Entregue - 12.06.2012
10	Unidade Hospitalar de Mirandela (Centro Hospitalar do Nordeste, EPE)	administracao@hmirandela.min-saude.pt	enviado - 12.06.2012
11	Hospital Distrital do Montijo (Centro Hospitalar Barreiro Montijo, EPE)	administracao@hmontijo.min-saude.pt	Não Entregue - 12.06.2012
12	Hospital Santa Marta (Centro Hospitalar Lisboa Central)	administracao@hsmarta.min-saude.pt	enviado - 12.06.2012
13	Instituto de Oftalmologia Dr. Gama Pinto	administracao@igpinto.min-saude.pt	enviado - 12.06.2012
14	Hospital Santa Luzia de Viana do Castelo (Unidade Local de Saúde do Alto Minho, EPE)	administracao@ulsam.min-saude.pt	enviado - 12.06.2012
15	Hospital Conde de Bertiandos - Ponte de Lima (Unidade Local do Alto Minho, EPE)	administracaopl@ulsam.min-saude.pt	enviado - 12.06.2012

Relação de e-mail's enviados - HOSPITAIS (ambito nacional SNS)			
Nº	**Organização**	**Endereço de e-mail**	**Resultado Envio**
16	Unidade Hospitalar da Póvoa de Varzim (Centro Hospitalar Póvoa de Varzim Vila do Conde, EPE)	ca@chpvvc.min-saude.pt	enviado - 12.06.2012
17	Hospital Cândido de Figueiredo - Tondela (CHTV, EPE)	ca@hdtondela.min-saude.pt	enviado - 12.06.2012
18	Hospital Pedro Hispano (Unidade Local de Saúde de Matosinhos, EPE)	ca@hph.min-saude.pt	Não Entregue - 12.06.2012
19	Hospital São João (Centro Hospitalar de São João, EPE)	ca@hsjoao.min-saude.pt	enviado - 12.06.2012
20	Hospital José Joaquim Fernandes - Beja (Unidade Local de Saúde do Baixo Alentejo, EPE)	ca@ulsba.min-saude.pt	Não Entregue - 12.06.2012
21	Centro Hospitalar de Vila Nova de Gaia/Espinho, EPE - Unidade II (antigo Hospital Distrital Vila Nova de Gaia)	cachvng@chvng.min-saude.pt	enviado - 12.06.2012
22	Centro Hospitalar de Vila Nova de Gaia/Espinho, EPE - Unidade I (antigo Hospital Eduardo Santos Silva)	cachvng@chvng.min-saude.pt	enviado - 12.06.2012
23	Centro Hospitalar de Vila Nova de Gaia/Espinho, EPE - Unidade III (antigo Hospital Nossa Senhora da Ajuda - Espinho)	cachvng@chvng.min-saude.pt	enviado - 12.06.2012
24	Hospital Curry Cabral (Centro Hospitalar de Lisboa Central, EPE)	cadm@hccabral.min-saude.pt	enviado - 12.06.2012
	Hospitais da Universidade de Coimbra (Centro Hospitalar e Universitário de Coimbra, EPE)	casec@huc.min-saude.pt	Não enviado
25	Unidade Hospitalar de Vila do Conde (Centro Hospitalar Póvoa de Varzim Vila do Conde, EPE)	cavc@chpvvc.min-saude.pt	enviado - 12.06.2012
26	Hospital Santa Cruz (Centro Hospitalar de Lisboa Ocidental, EPE)	chlo@chlo.min-saude.pt	enviado - 12.06.2012
27	Hospital São Francisco Xavier (Centro Hospitalar de Lisboa Ocidental, EPE)	chlo@chlo.min-saude.pt	enviado - 12.06.2012
28	Centro Medicina de Reabilitação da Região Centro Rovisco Pais	cmrrc@roviscopais.min-saude.pt	enviado - 12.06.2012
29	Hospital Pulido Valente (Centro Hospitalar de Lisboa Norte, EPE)	consadm@hpv.min-saude.pt	Não Entregue - 12.06.2012
30	Hospital Geral de Santo António (Centro Hospitalar do Porto, EPE)	consadmn@hgsa.min-saude.pt	enviado - 12.06.2012
31	Hospital Geral - Centro Hospitalar e Universitário de Coimbra, E.P.E.	correio@chc.min-saude.pt	enviado - 12.06.2012
32	Hospital Pediátrico de Coimbra (Centro Hospitalar e Universitário de Coimbra, EPE)	correio@hpc.chc.min-saude.pt	enviado - 12.06.2012
33	Unidade Hospitalar de Lamego (Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE)	critianacb@chtmad.min-saude.pt	Não Entregue - 12.06.2012
34	Hospital do Fundão (Centro Hospitalar Cova da Beira, EPE)	direccao.hf@chcbeira.min-saude.pt	enviado - 12.06.2012
35	Instituto Português Oncologia do Porto Francisco Gentil, EPE	diripo@ipoporto.min-saude.pt	enviado - 12.06.2012

Relação de e-mail's enviados - HOSPITAIS (ambito nacional SNS)			
Nº	**Organização**	**Endereço de e-mail**	**Resultado Envio**
36	Hospital Dr. Manoel Constâncio - Abrantes (Centro Hospitalar Médio Tejo, EPE)	geral@chmt.min-saude.pt	enviado - 12.06.2012
	Hospital Nossa Senhora da Graça - Tomar (Centro Hospitalar Médio Tejo, EPE)	geral@chmt.min-saude.pt	Não enviado
	Hospital Rainha Santa Isabel - Torres Novas (Centro Hospitalar Médio Tejo, EPE)	geral@chmt.min-saude.pt	Não enviado
37	Centro Hospitalar Psiquiátrico de Coimbra - Unidade Sobral Cid	geral@chpc.min-saude.pt	enviado - 12.06.2012
	Centro Hospitalar Psiquiátrico de Coimbra - Unidade Lorvão	geral@chpc.min-saude.pt	Não enviado
	Centro Hospitalar Psiquiátrico de Coimbra - Unidade Arnes	geral@chpc.min-saude.pt	Não enviado
38	Hospital Ortopédico Sant'Iago do Outão (Centro Hospitalar de Setúbal, EPE)	geral@chs.min-saude.pt	enviado - 12.06.2012
	Hospital São Bernardo (Centro Hospitalar de Setúbal, EPE)	geral@chs.min-saude.pt	Não enviado
39	Hospital Dom Luiz I - Peso da Régua (Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE)	geral@chtmad.min-saude.pt	enviado - 12.06.2012
	Hospital São Pedro de Vila Real (Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE)	geral@chtmad.min-saude.pt	Não enviado
40	Hospital São Gonçalo - Amarante (Centro Hospitalar Tâmega e Sousa, EPE)	geral@chts.min-saude.pt	Não Entregue - 12.06.2012
41	Unidade Hospitalar de Portimão (Centro Hospitalar do Barlavento Algarvio, EPE)	geral@hbalgarvio.min-saude.pt	enviado - 12.06.2012
42	Hospital Beatriz Ângelo	geral@hbeatrizangelo.pt	enviado - 12.06.2012
43	Hospital Distrital de Águeda (Centro Hospitalar do Baixo Vouga, EPE)	geral@hdagueda.min-saude.pt	enviado - 12.06.2012
	Hospital Arcebispo João Crisóstomo - Cantanhede	geral@hdcantanhede.min-saude.pt	Não enviado
44	Hospital Garcia de Orta, EPE	geral@hgo.min-saude.pt	Não Entregue - 12.06.2012
45	Hospital Litoral Alentejano, EPE	geral@hlalentejano.min-saude.pt	enviado - 12.06.2012
46	Hospital São Pedro Gonçalves Telmo - Peniche (Centro Hospialar do Oeste Norte)	geral@hpeniche.min-saude.pt	Não Entregue - 12.06.2012
47	Hospital Nossa Senhora da Assunção - Seia (Unidade Local de Saúde da Guarda, EPE)	geral@hseia.min-saude.pt	Não Entregue - 12.06.2012
48	Hospital São Teotónio, EPE - Viseu (CHTV, EPE)	geral@hstviseu.min-saude.pt	Não Entregue - 12.06.2012
49	Hospital Visconde de Salreu - Estarreja (Centro Hospitalar do Baixo Vouga, EPE)	geral@hvsalreu.min-saude.pt	enviado - 12.06.2012
50	Hospital Amato Lusitano (Unidade Local de Saúde de Castelo Branco, EPE)	geral@ulscbl.min-saude.pt	Não Entregue - 12.06.2012

Relação de e-mail's enviados - HOSPITAIS (ambito nacional SNS)			
Nº	***Organização***	***Endereço de e-mail***	***Resultado Envio***
51	Hospital Bernardino Lopes de Oliveira - Alcobaça (Centro Hospitalar Oeste Norte)	hablo@halcobaca.min-saude.pt	enviado - 12.06.2012
52	Unidade Hospitalar de Chaves (Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE)	hchaves@hchaves.min-saude.pt	Não Entregue - 12.06.2012
53	Hospital José Luciano de Castro - Anadia	hdanadia@hdanadia.min-saude.pt	enviado - 12.06.2012
54	Hospital Distrital Figueira da Foz, EPE	hdff@hdfigueira.min-saude.pt	Não Entregue - 12.06.2012
55	Hospital Dr. José Maria Antunes Júnior - Torres Vedras (Centro Hospitalar de Torres Vedras)	hdjmaj@hdjmaj.min-saude.pt	Não Entregue - 12.06.2012
56	Unidade Hospitalar de Macedo de Cavaleiros (Centro Hospitalar do Nordeste, EPE)	hdmc@hmcavaleiros.min-saude.pt	enviado - 12.06.2012
57	Hospital Distrital Pombal (Centro Hospitalar de Leiria-Pombal, EPE)	hdp@hdpombal.min-saude.pt	enviado - 12.06.2012
58	Hospital de Santarém, EPE	hdsca@hds.min-saude.pt	enviado - 12.06.2012
59	Hospital Egas Moniz (Centro Hospitalar de Lisboa Ocidental, EPE)	hem@chlo.min-saude.pt	Não Entregue - 12.06.2012
60	Hospital Dr. Francisco Zagalo - Ovar	hfzovar@hovar.min-saude.pt	enviado - 12.06.2012
61	Hospital Doutor João D'Almada	hja@srs.pt	enviado - 12.06.2012
62	Hospital Joaquim Urbano (Centro Hospitalar do Porto, EPE)	hju@hjurbano.min-saude.pt	enviado - 12.06.2012
63	Hospital de Magalhães Lemos, EPE	hml@hmlemos.min-saude.pt	enviado - 12.06.2012
64	HPP Hospital de Cascais Dr. José de Almeida	hppcascais@hpphospitaldecascais.pt	enviado - 12.06.2012
65	Hospital Distrital São João da Madeira (Centro Hospitalar de Entre Douro e Vouga, EPE)	hsjm@chedv.min-saude.pt	enviado - 12.06.2012
66	Hospital Santa Maria (Centro Hospitalar de Lisboa Norte, EPE)	hsm.casns@hsm.min-saude.pt	Não Entregue - 12.06.2012
67	Hospital de Braga	hsm.geral@hsmbraga.min-saude.pt	Não Entregue - 12.06.2012
68	Hospital São Miguel - Oliveira de Azeméis (Centro Hospitalar Entre Douro e Vouga, EPE)	hsm@chedv.min-saude.pt	Não Entregue - 12.06.2012
69	Hospital Sousa Martins - Guarda (Unidade Local de Saúde da Guarda, EPE)	hsmguarda@hsmguarda.min-saude.pt	enviado - 12.06.2012
70	Hospital São Sebastião, EPE (Centro Hospitalar de Entre Douro e Vouga, EPE)	hssebastiao@chedv.min-saude.pt	enviado - 12.06.2012
71	Hospital de Vila Franca de Xira	hvfxira@hvfxira.min-saude.pt	Não Entregue - 12.06.2012
72	Centro de Medicina Física de Reabilitação do Sul - São Brás de Alportel	info.cmrsul@gpsaude.pt	enviado - 12.06.2012
73	Unidade Hospitalar de Bragança (Unidade Local de Saúde do Nordeste, EPE)	infor.hdb@hbraganca.min-saude.pt	enviado - 12.06.2012

Relação de e-mail's enviados - HOSPITAIS (ambito nacional SNS)			
Nº	***Organização***	***Endereço de e-mail***	***Resultado Envio***
74	Instituto Português Oncologia de Lisboa Francisco Gentil, EPE	ipofg@ipolisboa.min-saude.pt	enviado - 12.06.2012
75	Hospital São Paulo - Serpa (Unidade Local de Saúde do Baixo Alentejo, EPE)	joao.bule@ulsba.min-saude.pt	enviado - 12.06.2012
76	Hospital Santo António dos Capuchos (Centro Hospitalar Lisboa Central)	sec.adm.capuchos@chlc.min-saude.pt	enviado - 12.06.2012
77	Hospital Dona Estefânia (Centro Hospitalar Lisboa Central)	sec.adm.hde@chlc.min-saude.pt	enviado - 12.06.2012
78	Hospital São José (Centro Hospitalar Lisboa Central)	sec.ca@chlc.min-saude.pt	enviado - 12.06.2012
79	Hospital Espírito Santo, EPE - Évora	sec.ca@hevora.min-saude.pt	enviado - 12.06.2012
	Hospital Professor Doutor Fernando Fonseca, EPE	sec.geral@hff.min-saude.pt	Não enviado
80	Instituto Português Oncologia de Coimbra Francisco Gentil, EPE	secad@ipocoimbra.min-saude.pt	enviado - 12.06.2012
81	Hospital Santa Maria Maior, EPE - Barcelos	secadm@hbarcelos.min-saude.pt	enviado - 12.06.2012
82	Hospital de Santo André - Leiria (Centro Hospitalar de Leiria-Pombal, EPE)	secca@hsaleiria.min-saude.pt	enviado - 12.06.2012
83	Hospital Infante D. Pedro - Aveiro (Centro Hospitalar do Baixo Vouga, EPE)	sec-geral@hdaveiro.min-saude.pt	enviado - 12.06.2012
84	Hospital Termal Rainha D. Leonor (Centro Hospitalar Caldas da Rainha)	secretariado.ca@chcrainha.min-saude.pt	enviado - 12.06.2012
	Hospital Distrital Caldas da Rainha (Centro Hospitalar do Oeste Norte)	secretariado.ca@chcrainha.min-saude.pt	Não enviado
85	Hospital Nossa Senhora da Conceição de Valongo (Centro Hospitalar de São João, EPE)	secretariado@hvalongo.min-saude.pt	enviado - 12.06.2012
86	Hospital do Divino Espírito Santo de Ponta Delgada, EPE	SRES-HDES@azores.gov.pt	enviado - 12.06.2012
87	Hospital da Horta, EPE	SRES-HH@azores.gov.pt	enviado - 12.06.2012
88	Hospital de Santo Espírito de Angra do Heroísmo, EPE	SRES-HSEAH@azores.gov.pt	enviado - 12.06.2012

Resumo de e-mail's Enviados	
88	Total e-mail's enviados 12.06.2012
20	Não entregues
68	Entregues

Relação de e-mail's enviados - HOSPITAIS (ambito nacional publico ou privado)			
Nº	**Organização**	**Endereço de e-mail**	**Resultado Envio**
1	HPP - Hospital dos Lusíadas	contact.center@hppsaude.pt	Enviado - 12.06.2012
2	Hospital Particular Algarve - Gambelas	sigicfaro@hpalg.com	Enviado - 12.06.2012
3	HPP Norte - Hospital da Boavista	marisa.mendes.guerra@hppsaude.pt	Não Entregue - 12.06.2012
4	Hospital da Arrábida - Gaia	aalves@hospitaldaarrabida.pt	Enviado - 12.06.2012
5	Venerável Ordem Terceira de São Francisco	ffreitas-osf@mail.telepac.pt	Enviado - 12.06.2012
6		mpintado-osf@mail.telepac.pt	Enviado - 12.06.2012
7	Venerável Irmandade de Nossa Senhora da Lapa	geral@hospitaldalapa.com	Enviado - 12.06.2012
8		secretariado@hospitaldalapa.com	Enviado - 12.06.2012
9	Santa Casa da Misericórdia de Riba d'Ave - H. Narciso Ferreira	hnf.ribadave@mail.telepac.pt	Não Entregue - 12.06.2012
10	Santa Casa da Misericórdia de Póvoa do Lanhoso - H. António Lopes	sigic@scmpl.pt	Enviado - 12.06.2012
11	Santa Casa da Misericórdia de Felgueiras - H. Agostinho Ribeiro	sigic_scmf_har@mail.telepac.pt	Enviado - 12.06.2012
12	Santa Casa da Misericórdia de Esposende - H. Valentim Ribeiro	argemirapedrosa.hvr@gmail.com	Enviado - 12.06.2012
13	HOSPOR - CLIPÓVOA - Póvoa do Varzim	jacintasilva@hospor.pt	Enviado - 12.06.2012
14	Hospital Particular de Viana do Castelo	hospart@mail.pt	Enviado - 12.06.2012
15	Hospital do Terço - Venerável N.ª Sr.ª do Terço e Caridade	pmartins.vinst@mail.ptprime.pt	Não Entregue - 12.06.2012
16	Hospital da Misericórdia de Valpaços	hospital_valpacos@sapo.pt	Enviado - 12.06.2012
17	Hospital de Santa Maria - Porto	hsm@hsmporto.pt	Enviado - 12.06.2012
18	Hospital da Trofa	nuno.maia@hospitaldatrofa.pt	Não Entregue - 12.06.2012
19		geral@hospitaldatrofa.pt	Enviado - 12.06.2012
20	Hospital da Misericórdia de Vila Verde	aloisia_araujo@hospital-vilaverde.com	Enviado - 12.06.2012
21	Hospital da Misericórdia de Vila do Conde	geral@scmvc.pt	Enviado - 12.06.2012
22	Hospital da Misericórdia de Lousada	hospital@scmlousada.pt	Enviado - 12.06.2012
23	Hospital da Misericórdia de Fão	scmfao@mail.telepac.pt	Enviado - 12.06.2012
24	CUF - Porto	helena.lopes@jmellosaude.pt	Enviado - 12.06.2012
25	Celestial Ordem Terceira da Santíssima Trindade	gabsigic@ordemtrindade.pt	Enviado - 12.06.2012
26	Casa de Saúde de Guimarães	sigic@casasaudeguimaraes.pt	Enviado - 12.06.2012
27	Casa de Saúde da Boavista	leandro@csaudeboavista.com	Enviado - 12.06.2012
28		csb@csaudeboavista.com	Enviado - 12.06.2012
29	Santa Casa da Misericórdia de Leiria - Hospital Dom Manuel de Aguiar	nuno.rama@misericordiadeleiria.pt	Enviado - 12.06.2012
30		geral@misericordiadeleiria.pt	Enviado - 12.06.2012
31	Santa Casa da Misericórdia do Entroncamento - H. S. João Baptista	sigic@scment.pt	Enviado - 12.06.2012
32	HOSPOR - Hospital de Santiago	filiparodrigues@hospor.pt	Enviado - 12.06.2012
33	Hospital de S. Louis	hslouis@hslouis.webside.pt	Não Entregue - 12.06.2012

Relação de e-mail's enviados - HOSPITAIS (ambito nacional publico ou privado)			
Nº	***Organização***	***Endereço de e-mail***	***Resultado Envio***
34	Hospital da Ordem Terceira de S. Francisco da Cidade	hot.sigic@mail.telepac.pt	Enviado - 12.06.2012
35	Hospital de Jesus - Venerável Ordem Terceira da Penitência de São Francisco a Jesus	sigic@hospitaldejesus.pt	Enviado - 12.06.2012
36	Hospital da Cruz Vermelha Portuguesa	mhaettich@hcvp.com.pt	Enviado - 12.06.2012
37	British Hospital	jmarfa@british-hospital.pt	Não Entregue - 12.06.2012
38	Hospital da Misericórdia da Mealhada	sigic@hmmealhada.com	Enviado - 12.06.2012
39	Fundação Nossa Senhora da Guia - Hospital de Avelar	hospitalavelar@mail.telepac.pt	Não Entregue - 12.06.2012
40	CLIRIA - Hospital Privado de Aveiro, SA	pneves@cliria.pt	Enviado - 12.06.2012
41	Hospital da Confraria de Nossa Senhora da Nazaré	mesa.admin@cnsn.pt	Enviado - 12.06.2012
42	Centro Hospitalar de S. Francisco	sigic.chsf@gpsaude.pt	Não Entregue - 12.06.2012
43		elinef@chsf.pt	Não Entregue - 12.06.2012
44	HPP Sul - H. Privado Santa Maria de Faro	sigic@hppsaude.pt	Enviado - 12.06.2012
45	HPP Sul - H. Privado S. Gonçalo de Lagos	otilia.silva.dias@hpphospprivados.pt	Não Entregue - 12.06.2012
46	Hospital de Sant'Ana	secretariado-hosa@scml.pt	Enviado - 12.06.2012
47	Hospital Particular do Algarve	sigic@hpalg.com	Enviado - 12.06.2012
48	Hospital São Camilo	sigic@saocamilo.pt	Enviado - 12.06.2012
49	Hospital São João de Deus - Montemor-o-Novo	hospital.montemor@isjd.pt	Enviado - 12.06.2012
50	Hospital da Misericórdia de Évora	sigic@hmevora.pt	Enviado - 12.06.2012
51	IDEALMED, SA	uhc@idealmed.pt	Enviado - 12.06.2012

Resumo de e-mail's Enviados	
51	Total enviados 12.06.2012
9	Não entregues
42	Entregues

Relação de e-mail's enviados - CLINICAS e OUTRAS ORGANIZAÇÕES DE SAÚDE				
	Área Actividade	*Organização / Empresa*	*e-mail*	*Resultado Envio*
1		CLÍNICA CARDIOLÓGICA DE DIAGNÓSTICO E TERAPÊUTICA ANTÓNIO A. MONTEIRO, LDA.	a.monteiro@mail.telepac.pt	Não entregue - 12.06.2012
2		PEDRO MANUEL GONÇALVES ABREU LOUREIRO	abreuloureiro@clix.pt	Não entregue - 12.06.2012
3	Analise Clinicas	Maria Joana F. S. Rocha de Sousa - Análises Clínicas, Lda	actualab@portugalmail.pt	enviado - 12.06.2012
4		MARIA JOANA F. S. ROCHA DE SOUSA - ANÁLISES CLÍNICAS, LDA.	actualab@portugalmail.pt	enviado - 12.06.2012
5	Analise Clinicas	Labeto - Centro de Análises Bioquímicas, SA	adm@beatrizgodinho.pt	enviado - 12.06.2012
6	Analise Clinicas	Laboratório de Análises Clínicas José Manuel Chau, SA	adm@beatrizgodinho.pt	enviado - 12.06.2012
7	Dialise	BEIRODIAL - Centro Médico e Diálise de Mangualde, Lda	administrativo@beirodial.pt	enviado - 12.06.2012
8		Clínica Europa	administrativo@clinicaeuropa.pt	enviado - 12.06.2012
9	Analise Clinicas	Laboratório Aeminium, Lda	aeminium@mediservicos.pt	enviado - 12.06.2012
10	Cardiologia	Centro Médico São Silvestre da Lousã, Lda	aeminium@mediservicos.pt	enviado - 12.06.2012
11		LABORATÓRIO AEMINIUM, LDA.	aeminium@mediservicos.pt	enviado - 12.06.2012
		CENTRO MÉDICO DE S. SILVESTRE DA LOUSÃ, LDA	aeminium@mediserviços.pt	enviado - 12.06.2012
12	Dialise	DV - Diálises do Vouga, Lda	agueda@diaverum.pt	Não entregue - 12.06.2012
13		Clinialba	aldir.alba@clinialba.com	enviado - 12.06.2012
14	Dialise	Nephrocare Portugal, SA	alexandra.seabra@fmc-ag.com	enviado - 12.06.2012
15		AMETIC - Apoio Móvel Especial à Terceira Idade e Convalescentes	ametic.sigic@netcabo.pt	enviado - 12.06.2012
16	Cardiologia	Narciso Pinheiro - Cardiologia Clínica, Lda	anpinheiro@netcabo.pt	enviado - 12.06.2012
17	Especialidades Médico-cirurgicas	António Boaventura Figueiredo	antonio.bfigueiredo@hotmail.com	Não entregue - 12.06.2012
18	Medicina Física e de Reabilitação	ARCIL - Associação de Recuperação de Cidadãos Inadaptados da Lousã	arcil@mail.telepac.pt	enviado - 12.06.2012
19		CARLOS MANUEL ARMAS SILVEIRA GONÇALVES	armasgoncalves@mail.telepac.pt	Não entregue - 12.06.2012
20		ASMECL - Associação de Socorros Mútuos dos Empregados do Comércio de Lisboa	asmecl@mail.telepac.pt	Não entregue - 12.06.2012
21	Analise Clinicas	Avelab - Laboratórios Médicos de Análises Clínicas, Lda	avelab@netcabo.pt	enviado - 12.06.2012
22		ANTÓNIO LUIS ZAMITH CERVEIRA DE MOURA	azamith1@sapo.pt	enviado - 12.06.2012
23		BECKER - ANÁLISES CLÍNICAS, LDA.	becker@mail.telepac.pt	Não entregue - 12.06.2012
24	Cardiologia	Centro de Cardiologia de Coimbra, Lda	c.cardiologiacoimbra@gmail.com	enviado - 12.06.2012
25		CENTRO DE MEDICINA FÍSICA E REABILITAÇÃO DE TOMAR DE SANTOS & IRMÃO, LDA.	c.m.fr.tomar@sapo.pt	Não entregue - 12.06.2012
26		CENTRO MEDICO DR. SIMAS ABRANTES, LDA	c.m.simas.abrantes@clix.pt	Não entregue - 12.06.2012
27		Clínica de Montes Claros	c.montesclaros@oninet.pt	Não entregue - 12.06.2012
28	Cardiologia	António Camões Sobral	camoessobral@gmail.com	enviado - 12.06.2012
29		JOSÉ EMÍDIO VIEIRA CAMPOS COROA	campos.coroa@hotmail.com	enviado - 12.06.2012
30	Especialidades Médico-cirurgicas	José Emílio Vieira Campos Coroa	camposcoroa@hotmail.com	Não entregue - 12.06.2012
31	Cardiologia	CARDIOALBI - Centro de Cardiologia, Lda	cardioalbi@gmail.com	enviado - 12.06.2012
32	Medicina Física e de Reabilitação	Cáritas Diocesana de Coimbra	caritas.crsi.isabel@mail.telepac.pt	enviado - 12.06.2012
33	Radiologia	ECOGRAFE - Sociedade Médica, Lda	catarina.ecografe@gmail.com	enviado - 12.06.2012
34	Analise Clinicas	Cavadas, Almeida & Cia, Lda	cavadas@cavadas.com	enviado - 12.06.2012
35		CLÍNICA DO CORAÇÃO DO ALENTEJO, SA	ccalentejo@gmail.com	enviado - 12.06.2012
36	Radiologia	CEDIR - Centro de Diagnóstico Raios X, Lda	cedir@cedir.pt	enviado - 12.06.2012
37	Pneumologia e Imunoalergologia	CEDRA II - Consultas de Pneumologia e Alergologia, Lda	cedra.coimbra@sapo.pt	enviado - 12.06.2012
38	Radiologia	CEMEDICAL - Centro Médico de Diagnósticos e Recuperação, Lda	cemedical@gmail.com	enviado - 12.06.2012
39	Endoscopia Gastrenterológica	Dinis Freitas, Lda	centrocirurgico@ccci.pt info@ccci.pt	enviado - 12.06.2012

Relação de e-mail's enviados - CLINICAS e OUTRAS ORGANIZAÇÕES DE SAÚDE				
	Área Actividade	*Organização / Empresa*	*e-mail*	*Resultado Envio*
40	Medicina Física e de Reabilitação	CEPOMEL - Centro Polivalente de Medicina e Enfermagem de Leiria, Lda	cepomel@mail.telepac.pt	enviado - 12.06.2012
41	Radiologia	Cimacon - Clínica de Imagiologia, Lda	cimacon@geralmail.com	Não entregue - 12.06.2012
42		CIRE - CENTRO DE IMAGENS RADIOLÓGICAS E ECOGRÁFICAS, LDA	cirelda@iol.pt	Não entregue - 12.06.2012
43	Radiologia	CLIMAG - Clínica de Diagnóstico e Imagem, Lda	climag@via.nw.pt	Não entregue - 12.06.2012
44	Medicina Física e de Reabilitação	CLINAGUE - Clínica de Medicina Física e de Reabilitação de Águeda, Lda	clinague@clinague.pt	enviado - 12.06.2012
45	Medicina Física e de Reabilitação	Clínica de Medicina Física e Reabilitação de Semblano & Teixeira, Lda	clinica.semblano@iol.pt	enviado - 12.06.2012
46	Cardiologia	Clínica Cardiológica de Diagnóstico e Terapêutica António A. Monteiro, Lda	clinicaamonteiro@gmail.com	enviado - 12.06.2012
47	Clínica	Clínica de Paços de Ferreira - Paços Ferreira	clinicadepacos@hospitaldatrofa.pt	enviado - 12.06.2012
48	Cardiologia	Ernesto Alberto Theile	clinicadofundao@gmail.pt	Não entregue - 12.06.2012
49	Cardiologia	Associação de Beneficiência Popular de Gouveia	clinicamfr@abpg.pt abpgouveia@abpg.pt	enviado - 12.06.2012
50	Medicina Física e de Reabilitação	Associação de Beneficiência Popular de Gouveia	clinicamfr@abpg.pt abpgouveia@abpg.pt	enviado - 12.06.2012
51		CLÍNICA PEDIÁTRICA CENTRAL DO PORTO, LDA.	clinicapediatrica@mail.telepac.pt	enviado - 12.06.2012
52	Radiologia	Clínica Médica de Santo António, Lda	clinvar@gmail.com	enviado - 12.06.2012
53	Medicina Física e de Reabilitação	Maria Angelina Pedrosa & Filho, Lda	cmfr.leiria@gmail.com	enviado - 12.06.2012
54	Medicina Física e de Reabilitação	APPACDM Coimbra	cmfrsilvestre@hotmail.com	enviado - 12.06.2012
55	Analise Clinicas	Santa Casa da Misericórdia do Porto - Hospital da Prelada (IPSS)	consger@hospitaldaprelada.pt	enviado - 12.06.2012
56	Analise Clinicas	Soares & Figueiredo, Lda	contacto@soaresefigueiredo.pt	enviado - 12.06.2012
57		Clínica Particular de Barcelos	cpbarcelos@sapo.pt	enviado - 12.06.2012
58	Radiologia	CRA - Centro de Radiologia, Lda	cra.agueda@mail.telepac.pt	enviado - 12.06.2012
59		FEGAMAR - ANÁLISES EQUIPAMENTOS E REAGENTES, SA	crcomaut.coimbra@dgrn.mj.pt	enviado - 12.06.2012
60		CENTRO MÉDICO D.DINIS, LDA	d.dinis.fisio@netcabo.pt	enviado - 12.06.2012
61	Medicina Física e de Reabilitação	Diagnosticum - Clínica de Diagnóstico da Figueira da Foz, Lda	diagnosticum@netcabo.pt	enviado - 12.06.2012
62	Dialise	DIAVERUM - Investimentos e Serviços, Lda	dialave@gambro.com	Não entregue - 12.06.2012
63	Radiologia	DIMAG - Diagnóstico Médico pela Imagem, SA	dimagsa@gmail.com	enviado - 12.06.2012
64	Clínica	Instituto de Radiologia Dr. Pinto Leite - Porto	drpintoleite@drpintoleite.com	Não entregue - 12.06.2012
65		DRA. ELISABETH AZEDO BARRETO, LDA.	ebarreto@mail.telepac.pt	Não entregue - 12.06.2012
66	Analise Clinicas	EGILAB - Centro de Diagnóstico Laboratorial, Lda	egilab@sapo.pt	Não entregue - 12.06.2012
67	Endoscopia Gastrenterológica	Endoscopia Digestiva - Allen Camacho, Lda	ernestinacamacho@hotmail.com	enviado - 12.06.2012
68	Radiologia	J. Gil Agostinho, Lda	exames@gilagostinho.com	enviado - 12.06.2012
69		Fundação Aurélio Amaro Diniz - IPSS	faadipss@iol.pt	enviado - 12.06.2012
70		FERNANDO SOTTO MAYOR COELHO SOUSA	fcoelhodesousa@hotmail.com	enviado - 12.06.2012
71	Analise Clinicas	Virgílio M. Roldão, Lda	filomena.lencastre@mail.tele	Não entregue - 12.06.2012
72		CANCHO, LDA.	fmcportugal@fmc-ag.com	enviado - 12.06.2012
73	Especialidades Médico-cirurgicas	Santa Casa da Misericórdia de Alvaiázere	geral.hsc@mail.telepac.pt admin.hsc@mail.telepac.pt	enviado - 12.06.2012
74		ICIL - INSTITUTO CLINICO E IMUNOLOGICO DE LISBOA, LDA.	geral.lisboa@medicil.pt	enviado - 12.06.2012
75	Medicina Física e de Reabilitação	Fundação ADFP - Assistência, Desenvolvimento e Formação Profissional	geral@adfp.pt	enviado - 12.06.2012

Relação de e-mail's enviados - CLINICAS e OUTRAS ORGANIZAÇÕES DE SAÚDE				
	Área Actividade	*Organização / Empresa*	*e-mail*	*Resultado Envio*
76	Radiologia	Briosa & Gala, Lda	geral@briosaegala.pt	enviado - 12.06.2012
77	Medicina Física e de Reabilitação	Irmandade da Santa Casa da Misericórdia de Batalha	geral@centrohospitalarbatalha.com	enviado - 12.06.2012
78	Cardiologia	Duarte João & Jorge - Centro Médico de Castelo Branco, Lda	geral@centromedico-cb.com	Não entregue - 12.06.2012
79	Medicina Física e de Reabilitação	Jorge Manuel dos Santos Fontes, Lda	geral@centromedicodamurtosa.com	enviado - 12.06.2012
80	Medicina Física e de Reabilitação	Centro de Reabilitação de Coimbra, Lda	geral@centroreabilitacaocoimbra.pt	enviado - 12.06.2012
81	Medicina Física e de Reabilitação	Maria Luiza Leão, Lda	geral@clinicaluisaleao.com	enviado - 12.06.2012
82		Clínica Central de Oiã	geral@clinica-oia.com	Não entregue - 12.06.2012
83	Especialidades Médico-cirurgicas	Cândido Manuel Pereira Monteiro Ferreira	geral@eurodial.pt	enviado - 12.06.2012
84	Analise Clinicas	FAAD - Fundação Aurélio Amaro Dinis	geral@faad.online.pt	enviado - 12.06.2012
85	Cardiologia	Fundação de Nossa Senhora da Guia	geral@fnsg-avelar.com	enviado - 12.06.2012
86	Cardiologia	Santa Casa da Misericórdia da Mealhada	geral@hmmealhada.com	enviado - 12.06.2012
87		I.M.I. - IMAGENS MÉDICAS INTEGRADAS, SA.	geral@imi.pt	enviado - 12.06.2012
88	Radiologia	Luís Lourenço, SA	geral@luislourenco.pt	enviado - 12.06.2012
89	Cardiologia	MEDICIR - Sociedade Médico Cirúrgica, Lda	geral@medicir.pt	enviado - 12.06.2012
90	Endoscopia Gastrenterológica	MEDICIR - Sociedade Médico Cirúrgica, Lda	geral@medicir.pt	enviado - 12.06.2012
91	Cardiologia	Santa Casa da Misericórdia de Leiria	geral@misericordiadeleiria.pt	enviado - 12.06.2012
92	Medicina Física e de Reabilitação	Associação de Socorros Mútuos Rainha D. Leonor	geral@montepio-rdl.pt	enviado - 12.06.2012
93	Radiologia	Associação de Socorros Mútuos Rainha D. Leonor	geral@montepio-rdl.pt	enviado - 12.06.2012
94	Cardiologia	Policlínica Central da Figueira da Foz, Lda	geral@policlinicadafigueira.pt	enviado - 12.06.2012
95	Medicina Física e de Reabilitação	Santa Casa da Misericórdia de Arganil	geral@scmarganil.pt	enviado - 12.06.2012
96	Radiologia	Santa Casa da Misericórdia de Vouzela	geral@scmvouzela.com.pt	enviado - 12.06.2012
97	Radiologia	Valle e Ruas, SA	geral@valleruas.pt	enviado - 12.06.2012
98	Cardiologia	Clínica Cardiológica A. Moreira da Silva, Lda	gina.carlos@mail.telepac.pt	Não entregue - 12.06.2012
99	Cardiologia	Clisacor - Clínica do Coração Gina Alves/Carlos Lopes, Lda	gina.carlos@mail.telepac.pt	enviado - 12.06.2012
100		CLÍNICA MÉDICA BAIRRO NOSSA SENHORA DA PIEDADE, LDA.	gravidus.clinicabairro@gmail.com	enviado - 12.06.2012
101	Radiologia	Gabinete de Radiodiagnóstico do Centro, Lda	grcc@iol.pt	enviado - 12.06.2012
102	Medicina Física e de Reabilitação	Hellman, Lda	hellman.fisio@hotmail.com	enviado - 12.06.2012
103	Medicina Física e de Reabilitação	Santa Casa da Misericórdia de Castelo de Paiva	hospitalsmcp@clix.pt	Não entregue - 12.06.2012
104		HELENA QUEIROZ-GABINETE DE ENDOSCOPIA DIGESTIVA, LDA	hq.gabend@gmail.com	enviado - 12.06.2012
105		INSTITUTO DO CORAÇÃO	igeral@incor.pt	enviado - 12.06.2012
106	Medicina Nuclear	Universidade de Coimbra (ICNAS)	icnas-lmn@uc.pt fcalves@gmail.com joao.oliveira@uc.pt	enviado - 12.06.2012
107	Radiologia	IMACENTRO - Clínica de Imagiologia Médica do Centro, Lda	imacentro@imacentro.pt	Não entregue - 12.06.2012
108	Radiologia	IMAGRAN - Laboratório de Imagiologia da Marinha Grande, Lda	imagran@chsf.pt	enviado - 12.06.2012
109	Especialidades Médico-cirurgicas	APCV - Associação de Paralisia Cerebral de Viseu	info@apcviseu.org.pt	enviado - 12.06.2012
110		CIL-CLÍNICA DE IMAGIOLOGIA DA LAPA, LDA	info@clinica-radiodiagnostico.com	Não entregue - 12.06.2012
111	Radiologia	CIL - Clínica de Imagiologia da Lapa, Lda	info@clinica-radiodiagnostico.com	enviado - 12.06.2012
112	Radiologia	Clínica Radiológica Peito Cruz & Associados, Lda	info@clinicaradiologica.com.pt	enviado - 12.06.2012
113	Medicina Nuclear	DIATON - Centro de Tomografia Computorizada, SA	info@diaton-coimbra.com.pt	enviado - 12.06.2012
114	Telemedicina	ITM - Instituto Telemedicina	info@i-telemedicina.pt	enviado - 12.06.2012
115		LIFECLINIC - HEALTH CARE	info@lifeclinic.pt	enviado - 12.06.2012
116	Clínica	Planicare Porto	info@planicare.pt	enviado - 12.06.2012
117		RIME - RADIOLOGIA E IMAGIOLOGIA MÉDICA, LDA.	info@rime.pt	enviado - 12.06.2012
118	Radiologia	Rui Branco & Miguel Ferreira, Lda	info@ruibranco.pt	enviado - 12.06.2012
119	Pneumologia e Imunoalergologia	Clínica Alergológica Dr. Celso Chieira, Lda	jgchieira@netcabo.pt	enviado - 12.06.2012
120	Endoscopia Gastrenterológica	Medicina e Gastrenterológica de Medeiros & Marques, Lda	jmedeiros@fmed.uc.pt	enviado - 12.06.2012

Relação de e-mail's enviados - CLINICAS e OUTRAS ORGANIZAÇÕES DE SAÚDE				
	Área Actividade	*Organização / Empresa*	*e-mail*	*Resultado Envio*
121	Endoscopia Gastrenterológica	Clínica de Gastroenterologia e Endoscopia Digestiva Dr. Pontes, Lda	jmpontes@sapo.pt	enviado - 12.06.2012
122	Dialise	NMC - Centro Médico Nacional, SA	jp.oliveira@fmc-ag.com	enviado - 12.06.2012
123	Radiologia	CENTAC-Centro de Tomografia Computorizada de Aveiro, Lda	jpm.lda@iol.pt	Não entregue - 12.06.2012
124	Endoscopia Gastrenterológica	Júlio Barbosa, Lda	juliobarbosa@net.novis.pt	enviado - 12.06.2012
125	Analise Clinicas	Costa Monteiro & Fernandes, Lda	lab.costa.monteiro@sapo.pt	enviado - 12.06.2012
126	Analise Clinicas	Costa Monteiro & Fernandes, Lda	lab.costa.monteiro@sapo.pt	enviado - 12.06.2012
127	Analise Clinicas	Laboratório de Análises Clínicas Maria de Lourdes Beja Cachulo, SA	lab.figueira@gmail.com	enviado - 12.06.2012
128	Analise Clinicas	Fátima Pimentel & Zulmira Cipriano, Lda	labbeiras@mail.telepac.pt	Não entregue - 12.06.2012
129	Analise Clinicas	Centro de Diagnóstico Laboratorial D. Dinis, Lda	labdiniz@interacesso.pt	enviado - 12.06.2012
130	Analise Clinicas	LabLeiria - Laboratório de Análises Clínicas, Lda	lableiria@mediservicos.pt	enviado - 12.06.2012
131		LABORATÓRIO DE ANÁLISES CLÍNICAS RIBEIRO DOS SANTOS, LDA.	labmedcentro@netcabo.pt	enviado - 12.06.2012
132		MARIA MANUELA GOUVEIA DUARTE E C.ª, LDA	labmoncorvo@clix.pt	Não entregue - 12.06.2012
133		ALVES & DUARTE, LDA.	laboratorioalvesduarte@oninet.pt	Não entregue - 12.06.2012
134	Analise Clinicas	Laboratório de Análises Clínicas Dr. Joaquim Rodrigues, Lda	laboratorioluisafrazao@gmail.pt	Não entregue - 12.06.2012
135		LABORATÓRIO SANTA COMBA ANÁLISES CLÍNICAS, LDA.	labsantacomba@mail.telepac.pt	enviado - 12.06.2012
136	Analise Clinicas	Laboratório de Análises Clínicas Silva & Monteiro, Lda	labsmgina@netcabo.pt	enviado - 12.06.2012
137	Analise Clinicas	Laboratório de Análises Clínicas Santo Estêvão, Lda	labsteste vao9@gmail.com	enviado - 12.06.2012
138		SUSANA PEREIRA ROSAS, LDA.	lac.spr@iol.pt	enviado - 12.06.2012
139		LABORATÓRIO PATOLOGIA CLÍNICA PROFESSOR PARREIRA, LDA.	lappparreira@netcabo.pt	Não entregue - 12.06.2012
140	Pneumologia e Imunoalergologia	Lino Chieira, Lda	lchieira@hotmail.com	enviado - 12.06.2012
141	Cardiologia	CHSF - Centro de Cardiologia S. Francisco, Lda	leiria@chsf.pt	enviado - 12.06.2012
142	Radiologia	IMALIS - Meios de Diagnóstico de Imagiologia de Leiria, Lda	luis.marinho@imi.pt	enviado - 12.06.2012
143	Endoscopia Gastrenterológica	Luís Emanuel Alvelos Dias Gomes	luisdiasgomes@hotmail.com	enviado - 12.06.2012
144	Especialidades Médico-cirurgicas	Luís Emanuel Alvelos Dias Gomes	luisdiasgomes@hotmail.com	enviado - 12.06.2012
145	Cardiologia	Polidiagnóstico - Centro Polivalente de Medicina e Diagnóstico, SA	marinha@polidiagnostico.pt	enviado - 12.06.2012
146	Endoscopia Gastrenterológica	Polidiagnóstico - Centro Polivalente de Medicina e Diagnóstico, SA	marinha@polidiagnostico.pt	enviado - 12.06.2012
147	Medicina Física e de Reabilitação	Polidiagnóstico - Centro Polivalente de Medicina e Diagnóstico, SA	marinha@polidiagnostico.pt	enviado - 12.06.2012
148	Pneumologia e Imunoalergologia	CARPA - Clínica de Alergologia, Respiração e Pneumologia, Lda	mchloureiro@hotmail.com	enviado - 12.06.2012
149		MEDICONDE - CLÍNICA MED. FISICA, LDA.	mediconde_clinica@sapo.pt	enviado - 12.06.2012
150	Endoscopia Gastrenterológica	Confraria de Nossa Senhora da Nazaré	mesa.admin@cnsn.pt	enviado - 12.06.2012
151	Medicina Física e de Reabilitação	Santa Casa da Misericórdia de Vagos	misericordiadevagos@scmvagos.eu	enviado - 12.06.2012
152	Medicina Física e de Reabilitação	Santa Casa da Misericórdia de Porto de Mós	misericordiapm@mail.telepac.pt	Não entregue - 12.06.2012
153	Medicina Física e de Reabilitação	Misericórdia Nossa Senhora dos Milagres	misof@mail.telepac.pt	enviado - 12.06.2012
154	Radiologia	NDE - Núcleo Diagnóstico Ecográfico, Lda	nde.ppombal@sapo.pt	enviado - 12.06.2012
155	Dialise	Nefrovales, SA	Nefro.Dial@netc.pt	Não entregue - 12.06.2012
156		N. R. D. - NÚCLEO DE RADIODIAGNOSTICO, LDA.	nrd@nrd.pt	enviado - 12.06.2012
157	Anatomia Patológica	Citodiagnóstico - Análises Citológicas, Lda	odetereal@netcabo.pt	enviado - 12.06.2012
158		CITODIAGNÓSTICO - ANÁLISES CITOLÓGICAS, LDA.	odetereal@netcabo.pt	enviado - 12.06.2012
159		OSTEOMEDICAL - DOENÇAS ÓSSEAS, LDA.	osteomedical@gpm.pt	enviado - 12.06.2012

Relação de e-mail's enviados - CLINICAS e OUTRAS ORGANIZAÇÕES DE SAÚDE				
	Área Actividade	*Organização / Empresa*	*e-mail*	*Resultado Envio*
160	Medicina Física e de Reabilitação	Dulcídio Bastos, Lda	ovar@dulcidiobastos.com.pt	Não entregue - 12.06.2012
161	Endoscopia Gastrenterológica	Gastro-Diagnóstico do Liz, Lda	paulo_andrade@sapo.pt	enviado - 12.06.2012
162	Diálise	Nephrocare Portugal, SA	pedro.goncalves@fmc-ag.com fmc.lisboa@mail.telepac.pt -> ÑEntr	enviado - 12.06.2012
163		Capio Sanidad	pelvidinic@pelvidinic.mail.pt	enviado - 12.06.2012
164	Endoscopia Gastrenterológica	J. E. Pina Cabral - Clínica e Endoscopia Digestiva, Lda	pinacabral@pinacabral.com	enviado - 12.06.2012
165	Endoscopia Gastrenterológica	J. E. Pina Cabral - Clínica e Endoscopia Digestiva, Lda	pinacabral@pinacabral.com	enviado - 12.06.2012
166	Endoscopia Gastrenterológica	J. E. Pina Cabral - Clínica e Endoscopia Digestiva, Lda	pinacabral@pinacabral.com	enviado - 12.06.2012
167		LABETO - CENTRO ANALISES E BIOQUÍMICA., LDA.	poli@beatrizpodinho.pt	enviado - 12.06.2012
168		MEDISERVIÇOS COIMBRA, LDA	rbandeira@net.sapo.pt	enviado - 12.06.2012
169	Diálise	Nephrocare Portugal, SA	rui.cruto@fmc-ag.com fmc.lisboa@mail.telepac.pt	enviado - 12.06.2012
170	Radiologia	Centro Radiológico Dr. Vieira de Carvalho, Lda	rvieiracarvalho@sapo.pt	enviado - 12.06.2012
171	Medicina Física e de Reabilitação	Sociedade da Água de Luso, SA	sal@agualuso.pt	enviado - 12.06.2012
172	Cardiologia	SANFIL - Casa de Saúde de Santa Filomena, SA	sanfil@sanfil.pt	enviado - 12.06.2012
173		SANTOS ANDRADE, LDA.	santosandrade@iol.pt	enviado - 12.06.2012
174		SANTOS MONTEIRO, LDA.	santosmonteiro@iol.pt	enviado - 12.06.2012
175	Medicina Física e de Reabilitação	Santa Casa da Misericórdia de Castelo Branco	scmcb.informatica@netvisao.pt	Não entregue - 12.06.2012
176	Endoscopia Gastrenterológica	Santa Casa da Misericórdia da Covilhã	scmiscovilha@gmail.com	enviado - 12.06.2012
177	Radiologia	Santa Casa da Misericórdia de Montemor-o-Velho	scmmv@clix.pt	enviado - 12.06.2012
178	Medicina Física e de Reabilitação	Irmandade da Santa Casa da Misericórdia de Resende	scmr@scmr.pt	enviado - 12.06.2012
179	Diálise	EURODIAL - Centro de Nefrologia e Diálise de Leiria, SA	secretaria@eurodial.pt	Não entregue - 12.06.2012
180	Cardiologia	Santa Casa da Misericórdia de Sever do Vouga	serv.medicossomsv@sapo.pt	Não entregue - 12.06.2012
181		Casa de Repouso de Coimbra	sigic.crc@mail.telepac.pt	enviado - 12.06.2012
182		ASMECI - Associação de Socorros Mútuos dos Empregados do Comércio e Indústria	sigic@asmeci.org	enviado - 12.06.2012
183		CLINIGRANDE - Clínica da Marinha Grande	sigic@clinigrande.pt	enviado - 12.06.2012
184		SOERAD - Sociedade de Estudos Radiológicos	soerad@iol.pt	enviado - 12.06.2012
185		SÓNIA MARIA RUIVO PIMENTEL	somarupi@hotmail.com	enviado - 12.06.2012
186	Radiologia	SONOMEDICUS - Centro de Diagnóstico Médico, Lda	sonomedicus@sapo.pt	enviado - 12.06.2012
187		SURGIMED - Centro Médico Cirúrgico de Santarém	surgimed.quartos@net.novis.pt	Não entregue - 12.06.2012
188		IDEALMED, SA	uhc@idealmed.pt	enviado - 12.06.2012

Resumo de e-mail's Enviados	
188	Total enviados 12.06.2012
39	Não Entregues
149	Entregues

Relação de e-mail's enviados - Diferentes Sectores de Actividade				
Nº	**Área Actividade**	**Empresa**	**e-mail**	**Resultado Envio**
1	Mídia	Cofina Média - SGPS, SA	juarez@revistas.cofina.pt	enviado - 18.06.2012
2	TI / Consultoria	Accenture Portugal	pedro.lopes@accenture.com	enviado - 18.06.2012
3	TI / Plataforma	Aconex	dcorreia@aconex.com	enviado - 18.06.2012
4	TI / Serviços	Additve Tecnologia, Lda	apr@additive.pt	Não Entregue - 12.06.2012
5	TI / Backups	Altimate	jcharraz@altimate-group.com	Não Entregue - 12.06.2012
6	SW / Contact Center	Altitude SW	mario.pereira@altitude.com	enviado - 18.06.2012
7	HW / Distribuição	Asus portugal	helder_bastos@asus.com	enviado - 18.06.2012
8	TI / Revendor	Avelcellular	carlos_aguiar@avelcellular.pt	Não Entregue - 12.06.2012
9	TI / Comuniações	CaboVisão	ana.lopes@cabovisao.pt	enviado - 18.06.2012
10	TI / Consultoria	CapGemini	paulo.morgado@capgemini.com	enviado - 18.06.2012
11	HW / Redes	Cisco	nuno.carvalho@cisco.pt	Não Entregue - 12.06.2012
12	TI / Hosting e Redes	Claranet Portugal	jfolgado@pt.clara.net	enviado - 18.06.2012
13	SW / Desenvolvimento	Critical Helth, SA	jramos@critical-health.com	enviado - 18.06.2012
14	SW / Desenvolvimento	Critical Software, S.A.	info@criticalsoftware.com	enviado - 18.06.2012
15	TI / HW distribuição	DataBox, SA	v.fernandes@databox.pt	enviado - 18.06.2012
16	TI / Consultoria	Deloitte Consultores, SA	ncarvalho@deloitte.pt	enviado - 18.06.2012
17	HW / Storage	EMC2	sofia.lima@emc.com	Não Entregue - 12.06.2012
18	HW / Impressoras	Epson Ibérica	pedro_pepino@epson.pt	enviado - 18.06.2012
19	HW / Distribuição	Eurocabos, SA	pgarcia@eurocabos.pt	enviado - 18.06.2012
20	HW / Comunicações	Fujitsu,SA	f.marques@fujitsu.pt	enviado - 18.06.2012
21	TI / Consultoria	GFI Portugal	hugo.csousa@gfi.pt	enviado - 18.06.2012
22	TI / Distribuição	Informatica El Corte Inglés	daniel_yanes@iecisa.es	Não Entregue - 12.06.2012
23	SW / Serviços	Information Builders, SA	john_manning@ibi.com	Não Entregue - 12.06.2012
24	HW / Distribuição	Itautec Portugal, SA	mmajor@itautec.com	enviado - 18.06.2012
25	HW / Distribuição	JP Sá Couto	spdias@jpsacouto.pt	enviado - 18.06.2012
26	Energia	Galp Energia, SGPS, S.A.	galp@galpenergia.com	enviado - 18.06.2012
27	Energia	EDP Serviço Universal	edp.online@edp.pt	enviado - 18.06.2012
28	Diversos	SONAE	comunicacao@sonae.pt	enviado - 18.06.2012
29	Alimentar	Jeronimo Martins	rh@jeronimo-martins.pt	enviado - 18.06.2012
30	Transportes	TAP	tapcorporatefly@tap.pt	enviado - 18.06.2012
31			fale.connosco@tap.pt	enviado - 18.06.2012
32	Energia	EDP - ENERGIAS DE PORTUGAL S.A	ppec@edp.pt	enviado - 18.06.2012
33			eficienciaenergetica@edp.pt	enviado - 18.06.2012
34	Combustivel	Repsol	nsapage@repsol.com	enviado - 18.06.2012
35	Automóvel	Autoeuropa	isabel.carimbo@autoeuropa.pt	enviado - 18.06.2012
36			public-relations.office@autoeuropa.pt	enviado - 18.06.2012
37	Gestão Infraestruturas	Estradas de Portugal	gci@estradasdeportugal.pt	enviado - 18.06.2012
38	Alimentar	Unicre	geral@unicre.pt	Não Entregue - 12.06.2012
39	Alimentar	Auchan	infojumbo@auchan.pt	enviado - 18.06.2012
40	Energia	GALP - GÁS NATURAL, S.A.	galp@galpenergia.com	enviado - 18.06.2012
41	Telecomunicações	Telecom	geral@telecom.pt	enviado - 18.06.2012
42	Telecomunicações	TMN	apoio_1696@telecom.pt	Não Entregue - 12.06.2012
43	Telecomunicações	Optimus	1663@optimus.pt	enviado - 18.06.2012
44	Telecomunicações	Vodafone	crs.pt@vodafone.com	Não Entregue - 12.06.2012
45	Banca	BES	info@bes.pt	enviado - 18.06.2012
46	Banca	CGD	caixadirecta@cgd.pt	enviado - 18.06.2012
47	Bebidas	Superbock	superbock@unicer.pt	enviado - 18.06.2012
48	Bebidas	Coca Cola	webmaster@cocacola.pt	enviado - 18.06.2012
49	Diversos	Puma	info@puma.com	enviado - 18.06.2012
50	Alimentar	Delta Cafes	geral@delta-cafes.pt	enviado - 18.06.2012
51	Vestuário	Dielmar	geral@dielmar.pt	enviado - 18.06.2012

Relação de e-mail's enviados - Diferentes Sectores de Actividade				
Nº	**Área Actividade**	**Empresa**	**e-mail**	**Resultado Envio**
52	Alimentar/Diversos	Unilever	linha.ola@unilever.com	enviado - 18.06.2012
53	Electricidade	Efacec	am@efacec.com	enviado - 18.06.2012
54	/ Eletronica / Diversos		sgps@efacec.pt	enviado - 18.06.2012
55	Bebidas	Lipton (Uni Lever)	lipton.portugal@unilever.com	enviado - 18.06.2012
56	Mídias	SIC	atendimento@sic.pt	enviado - 18.06.2012
57	Combustiveis	Cepsa	relaciones.institucionales@cepsa.com	Não Entregue - 12.06.2012
58	Construção	Mota Engil	Antonio.capinha@mota-engil.pt	enviado - 18.06.2012
59	Alimentar	Mini Preço / Carrefour	geral@uptostart.com	enviado - 18.06.2012
60	Energia	EDP Comercial/Corporate	corporate@corporate.edp.pt	enviado - 18.06.2012
61	Hotelaria	Lagoas Park Centro congressos	centro.congressos@tdhotels.pt	enviado - 18.06.2012
62	Hotelaria	Hotel e Centro de Congressos	lagoas.hotel@tdhotels.pt	enviado - 18.06.2012
63	Construção	Teixeira Duarte	3n@teixeiraduarte.pt	enviado - 18.06.2012
64	Alimentar	Recheio	cliente@recheio.pt	enviado - 18.06.2012
65	Electrodomesticos	Worten	cliente@worten.pt	enviado - 18.06.2012
66	Cinema	ZON	comunicacao.corporativa@zon.pt	enviado - 18.06.2012
67			irene.m.luis@zon.pt	enviado - 18.06.2012
68	Alimentar	Lactogal	info@lactogal.pt	enviado - 18.06.2012
69	Equipamentos	GEDAZ	geral@gedaz.pt	enviado - 18.06.2012
70	Construção	ASC Engenharia Construção	asc@grupocampos.com	enviado - 18.06.2012
71	Publicidade	Caetsu	geral@e3o-caetsu.pt	enviado - 18.06.2012
72	Construção	João F Silva SA - Contrução Civil	geral@jfs-empreiteiros.com	Não Entregue - 12.06.2012
73	Alimentar	Portugal Fresh	info@portugalfresh.com	Não Entregue - 12.06.2012
74	Alimentar	Abrunhoeste – Conservação e Refrigeração de frutas, SA	geral@abrunhoeste.pt	enviado - 18.06.2012
75	Alimentar	Agromais – Entreposto Comercial e Agrícola, CRL	agromais@agromais.pt	enviado - 18.06.2012
76	Alimentar	Cacial, CRL	mail@cacial.com	enviado - 18.06.2012
77	Alimentar	Campotec, lda	campotec@campotec.pt	enviado - 18.06.2012
78	Alimentar	Cooperativa Agrícola de Mangualde, CRL	geral@coopagricmangualde.com	enviado - 18.06.2012
79	Alimentar	Cooperativa Agrícola do Távora, CRL	cooptavora@mail.telepac.pt	enviado - 18.06.2012
80	Alimentar	Cooperfrutas – crl	geral@cooperfrutas.pt	enviado - 18.06.2012
81	Alimentar	Coopval	coopval@coopval.com	Não Entregue - 12.06.2012
82	Alimentar	Emergosol	geral@emergosol.com	enviado - 18.06.2012
83	Alimentar	Eurobatata	eurobatata.pal@eurobatata.pt	enviado - 18.06.2012
84	Alimentar	FERREIRA DA SILVA, SA	ferreiradasilva@ferreiradasilva.pt	enviado - 18.06.2012
85	Alimentar	Hortapronta – hortas do oeste, SA	sede@hortapronta.com	enviado - 18.06.2012
86	Alimentar	Hortas de Santa Maria SA	geral@hortasdesantamaria.com	enviado - 18.06.2012
87	Alimentar	Primores do Oeste, SA	geral@primoresoeste.pt	Não Entregue - 12.06.2012
88	Alimentar	Torriba	geral@torriba.pt	enviado - 18.06.2012
89	Alimentar	Triportugal Frutas	triportugal@triportugal.pt	enviado - 18.06.2012
90	Alimentar	Vale da Rosa	geral@valedarosa.com	enviado - 18.06.2012
91	Alimentar	Triportugal	triportugal@triportugal.pt	enviado - 18.06.2012
92	Alimentar	SIVA, S.A.	ricardo.leite@silvas-sa.pt	enviado - 18.06.2012
93			comercial@silvas-sa.pt	enviado - 18.06.2012
94	Papel	Portucel	antonio.alves@portucelsoporcel.com	enviado - 18.06.2012
95	Electricidade	Barata e Marcelino	geral@barataemarcelino.pt	enviado - 18.06.2012
96	Construção	Soares da Costa	geral@soaresdacosta.pt	enviado - 18.06.2012
97	Construção	Zagope	zagope@zagope.pt	enviado - 18.06.2012
98	Instrumentação	CEGE	geral@cege.pt	enviado - 18.06.2012
99			costa.pereira@cege.pt	enviado - 18.06.2012

Relação de e-mail's enviados - Diferentes Sectores de Actividade				
Nº	**Área Actividade**	**Empresa**	**e-mail**	**Resultado Envio**
100	Produtos Veterinarios	SILOALVET	luis.sa@siloalvet.com	enviado - 18.06.2012
101	HW / Serviços	TI POST	isenap@gmail.com	enviado - 18.06.2012
102	Comunicação	CTT	informacao@ctt.pt	enviado - 18.06.2012
103	Electronica / Diversos	Bosch	geral@bosch.pt	enviado - 18.06.2012
104	Telecomunicações	PT Prime	apoio.ptprime@telecom.pt	enviado - 18.06.2012
105	Distrib. Farmacêtica	OCP Portugal	ocp.portugal@ocp.pt	enviado - 18.06.2012
106			geral@relacre.pt	enviado - 18.06.2012
107	Distrib. Farmacêutica	Alliance HealthCare	geral@alliance-healthcare.pt	Não Entregue - 12.06.2012
108	Seguros	Seguros Continente	geral@seguroscontinente.pt	enviado - 18.06.2012
109	Automóvel	Renault	geral@renault.pt	Não Entregue - 12.06.2012
110	Automóvel	Renault Entidade Gestora	indom@indom.com	enviado - 18.06.2012
111	Autoestradas	BRISA Auto-Estradas de Portugal, SA	info.bci@brisa.pt geral@brisa.pt	enviado - 18.06.2012
112	Serviços	Associação Portuguesa de Gestão de Projectos	info@apogep.pt	enviado - 18.06.2012
113	Administração Saúde	ACSS - Administração Central do Sistema de Saúde, IP	lsalavisa@acss.min-saude.pt	enviado - 18.06.2012
114	Formação	ATEC	joao.costa@atec.pt	enviado - 18.06.2012
115	TI / Consultoria	ATKS	info@atks.pt	enviado - 18.06.2012
116	Consultoria	AVENTIA PORTUGAL	geral.pt@aventia.com	enviado - 18.06.2012
117	Consultoria	BRIGHT PARTNERS	info@brightpartners.com	enviado - 18.06.2012
118	Banca	CA INFORMATICA (Grupo Crédito Agrícola)	ipess@creditoagricola.pt	enviado - 18.06.2012
119	construção	DDN - Gestão, Coordenação e Fiscalização de Obras Públicas e Privadas, Lda	geral@ddn.pt	enviado - 18.06.2012
120	Energia	EDP Distribuição - Energia, SA	garso.barao@edp.pt	enviado - 18.06.2012
121	HW/Equipamentos	FUJITSU, SA	informacoes@services.fujitsu.com	Não Entregue - 12.06.2012
122	TI / Consultoria	GTBC	info@gtbc.pt	enviado - 18.06.2012
123	Consultoria	INVESCON	invescon@invescon.pt	enviado - 18.06.2012
124	TI / Consultoria	LINK CONSULTING	info@link.pt	Não Entregue - 12.06.2012
125	TI / Consultoria	NOVABASE	info@novabase.pt	enviado - 18.06.2012
126	TI / Consultoria	SINFIC	formacao@sinfic.pt	enviado - 18.06.2012
127	Bebidas	Unicer	geral@unicer.pt teresa.figueiredo@unicer.pt	Não Entregue - 12.06.2012
128	Bebidas	Superbock	superbock@unicer.pt	enviado - 18.06.2012
129	Bebidas	Agua das Pedras	agua daspedras@unicer.pt	enviado - 18.06.2012
130	Laser	Quinta do Lago Golfe	geral@quintadolagogolf.com	Não Entregue - 12.06.2012
131	Metalomecânica	Projectos Metalomecanicos, lda	geral@maitec.pt	enviado - 18.06.2012
132	Cerâmica	UMBELINO MONTEIRO, S.A.	geral@umbelino.pt	enviado - 18.06.2012
133	Industria Vedantes	UCHIYAMA PORTUGAL-VEDANTES, LDA.	upv@umc-upv.com	enviado - 18.06.2012
134	Industria Cortiça	UNICOR 2 - PRODUTOS DE CORTIÇA, LDA	unicor.lda@netvisao.pt	enviado - 18.06.2012
135	Confecções	UNILOPES - INDUSTRIA DE CONFECÇÕES, LDA.	unilopes@unilopes.pt	enviado - 18.06.2012
136	Moldes	UNITOOLS - COMPANHIA EXPORTADORA DE MOLDES LDA	info@unitools.com	enviado - 18.06.2012
137	Metalomecânica	URFIC - INDÚSTRIA DE FERRAGENS, S.A.	geral@urfic.pt	enviado - 18.06.2012
138	Distrib. Farmacêutica	UDIFAR	geral@udifar.pt	enviado - 18.06.2012
139	Alimentar	Nestle	fale.connosco@pt.nestle.com	Não Entregue - 12.06.2012
140	Alimentar	Makro	cliente@makro.pt	enviado - 10.07.2012
141			contact.cliente@makro.pt	Não Entregue - 10.07.2012
142	Energia	Galp Energia	galp@galpenergia.com	enviado - 10.07.2012
143	Mineira	SOMINCOR - SOCIEDADE MINEIRA DE NEVES - CORVO S.A.	info@lundinmining.com	enviado - 10.07.2012
144	Retalho /Diversos	El Corte Ingles	servico_clientes@elcorteingles.pt	enviado - 10.07.2012

Relação de e-mail's enviados - Diferentes Sectores de Actividade				
Nº	***Área Actividade***	***Empresa***	***e-mail***	***Resultado Envio***
145	Transportes	NETJETS - TRANSPORTES AÉREOS,S.A.	netjetsinfo@netjets.com	enviado - 10.07.2012
146	Equipamento Electrico	DELPHI AUTOMOTIVE SYSTEMS - PORTUGAL, S.A	delphipt@mail.telepac.pt	Não Entregue - 10.07.2012
147	Automovel	BMW PORTUGAL, LDA.	info@bmw.pt	enviado - 10.07.2012
148			geral@bmw.pt	enviado - 10.07.2012
149	Alimentar	UNILEVER JERÓNIMO MARTINS, LDA.	geral@cnpd.pt	enviado - 10.07.2012
150	Electricidade / Eletronica / Diversos	EFACEC	sgps@efacec.pt	enviado - 10.07.2012
151			ase.eng@efacec.com	enviado - 10.07.2012
152			eng@efacec.com	enviado - 10.07.2012
153			geral.ao@efacec.com	enviado - 10.07.2012
154	Serviços	CIAB - Centro de Arbitragem de Consumo	geral@ciab.pt	enviado - 10.07.2012
155	Metalomecânica	SMM - Sociedade de Montagens Metalomecânicas, SA	smm.geral@smm.com.pt	enviado - 10.07.2012
156	Metalomecânica	Turbogas	info@turbogas.pt	enviado - 10.07.2012
157	Transportes	ANA - Aeroportos de Portugal, SA	pontadelgada.airport@ana.pt	enviado - 10.07.2012
158			nrsobral@ana.p	Não Entregue - 10.07.2012
159			info@ana.pt	Não Entregue - 10.07.2012
160	Automóveis	Toyota	toyota@toyotacaetano.pt	enviado - 10.07.2012
161			coimbra@toyotacaetano.pt	Não Entregue - 10.07.2012
162	Bebidas	Central de Cervejas	scc@centralcervejas.pt	enviado - 10.07.2012
163	Formação	CECOA	cecoa@cecoa.pt	enviado - 10.07.2012
164	Formação	EPAD	informacoes@epad.pt	Não Entregue - 10.07.2012
165	Formação	AEEP	aeep@aeep.pt	enviado - 10.07.2012
166	Formação	Certifer	geral@certifer.pt	enviado - 10.07.2012
167	Telecomunicações	SONAE COM	ricardo.goncalves@sonaecom.com	Não Entregue - 10.07.2012
168	comunicação Social	Expresso Emprego	expressoemprego@expressoemprego.pt	enviado - 10.07.2012
169	Telecomunicações	Vodafone Portugal	renato.pedro@vodafone.com	enviado - 10.07.2012
170	Estado	Ministerio da Educação	gepe@gepe.min-edu.pt	enviado - 10.07.2012
171	Distrb.Farmacéutica	Cooprofar	cooprofar@cooprofar.pt	enviado - 10.07.2012
172	Organização Publica	Ordem Farmaceuticos	cim@ordemfarmaceuticos.pt	enviado - 10.07.2012
173			direccao.nacional@ordemfarmaceuticos.pt	enviado - 10.07.2012
174	Energia	REN	info@ren.pt	enviado - 10.07.2012
175			secretaria.geral@ren.pt	enviado - 10.07.2012
176	Industria	Novelis	info@novelis.com	enviado - 10.07.2012
177	Gestão Infraestruturas	Ascendi	geral@ascendi.pt	enviado - 10.07.2012
178	construção	Somague	geral@hidurbe.somague.pt	enviado - 10.07.2012
179			somague@somague.pt	enviado - 10.07.2012
180	Cimenteira	Cimpor	geral@cimpor.pt	Não Entregue - 10.07.2012
181	Consultoria/Formação	Gocepi	geral@gocepi.pt	enviado - 10.07.2012
182	Consultoria	Numero Infinito	geral@numeroinfinito.com	enviado - 10.07.2012
183	TI / Consultoria	Biznet	biz@biznet.pt	enviado - 10.07.2012
184	Consultoria	Exchange	master@exchange.pt	enviado - 10.07.2012
185	TI / Consultoria	Etradecenter	info@etradecenter.com	Não Entregue - 10.07.2012
186		Fiducial	info@fiducial-portugal.com	enviado - 10.07.2012
187	SW / Informática	PHCSW	info@phc.pt	enviado - 10.07.2012
188	Consultoria	Biorumo	geral@biorumo.com	enviado - 10.07.2012
189	Arquitectura	Arquitectos	info@castro-natali.com	enviado - 10.07.2012
190	Organização Publica	IAPMEI	info@iapmei.pt	enviado - 10.07.2012
191	Gestão Financeira	Norgarante	mkt@norgarante.pt	enviado - 10.07.2012
192	construção	Secil	outao@secil.pt	enviado - 10.07.2012
193			geral@secil-britas.pt	enviado - 10.07.2012

Relação de e-mail's enviados - Diferentes Sectores de Actividade				
Nº	***Área Actividade***	***Empresa***	***e-mail***	***Resultado Envio***
194			secil@secil.pt	enviado - 10.07.2012
195	Comércio Retalho	fnac	geral@fnac.pt	Não Entregue - 10.07.2012
196			info@fnac.pt	enviado - 10.07.2012
197	Electricidade / Eletronica / Diversos	efacec	info@micropefacec.pt	Não Entregue - 10.07.2012
198			info.efapower@efacec.pt	enviado - 10.07.2012
199			info@efacec.pt	Não Entregue - 10.07.2012
200	Papel	Portucel soporcel	antonio.alves@portucelsoporcel.com	enviado - 10.07.2012
201	Alimentar	Sovena	info@sovena.pt	enviado - 10.07.2012
202	Construção / Industria	OPWAY	geral@opway.pt	enviado - 10.07.2012
203	Automóvel	Auto Sueco	info@auto-sueco.pt	enviado - 10.07.2012
204	Automóvel	OPEL	informacoes.opel.portugal@pt.gm.com	Não Entregue - 10.07.2012
205	Automóvel	Mercedez-Benz	info@mbp.mercedes-benz.com	Não Entregue - 10.07.2012
206	Automóvel	Aprilia	milfa@milfa.pt	enviado - 10.07.2012
207	Automóvel	AUDI	apoio.clientes@siva.pt	enviado - 10.07.2012
208	Automóvel	Mitsubishi	mmpgeral@mitsubishi.pt	enviado - 10.07.2012
209	Automóvel	Citroen	webmaster@citroen.pt	Não Entregue - 10.07.2012
210	Automóvel	Crysley	geral@chry-portugal.pt	enviado - 10.07.2012
211	Automóvel	SAAB	saab@cvl.pt	Não Entregue - 10.07.2012
212	Automóvel	Honda	honda.automovel@honda-eu.com	Não Entregue - 10.07.2012
213	Automóvel	SEAT	seat@seatportugal.pt	enviado - 10.07.2012
214	Automóvel	SUBARU	entrepostocomercial@entrepostovh.pt	enviado - 10.07.2012
215	Automóvel	Kawasaki	kawamotors@kawasaki.pt	enviado - 10.07.2012
216	Automóvel	TATA	lusilectra@lusilectra.pt	Não Entregue - 10.07.2012
217	Automóvel	KTM	scvouga@scvouga.pt	enviado - 10.07.2012
218	Automóvel	Toyota	comunicacao@salvadorcaetano.pt	enviado - 10.07.2012
219	Automóvel	Land Rover	lrpgeral@landrover.com	Não Entregue - 10.07.2012
220	Automóvel	Volvo	infor@auto-sueco.pt	Não Entregue - 10.07.2012
221	Automóvel	MAN	man-direccao@man.pt	Não Entregue - 10.07.2012
222	Organização Publica	SESARAM - Saúde	sec.geral@srs.pt	enviado - 10.07.2012
223			informatica@srs.pt	enviado - 10.07.2012
224	HW / Informática	CPCDI - informatica	cpcdi@cpcdi.pt	enviado - 10.07.2012
225	Viagens	Viagens Abreu	info@abreu.pt	Não Entregue - 10.07.2012
226	Confecções	CRISPIM	info@crispimabreu.pt	enviado - 10.07.2012
227	Viagens	HELMATUR	info@helmartur.pt	enviado - 10.07.2012
228	Enegenharia Ambiental	Enercon	info@enercon.de	enviado - 10.07.2012
229			geral@enercon.de	enviado - 10.07.2012
230	Construção	MSF - Engenharia SA	msf@msf.pt	Não Entregue - 10.07.2012
231	Construção	JMSF	geral@jmsf.pt	enviado - 10.07.2012
232	Tabaqueira	Tabaqueira	usl@unaolisboa-cgtp.pt	enviado - 10.07.2012
233	Franchising	Best Franchising	info@bestfranchising.pt	enviado - 10.07.2012
234	Automóvel	Citroen	citroen@autosertorio.pt	enviado - 10.07.2012
235	Construção	Edifer	geral@edifer.pt	enviado - 10.07.2012
236	Construção	Costa Carvalho	geral@costacarvalho.pt	enviado - 10.07.2012

Resumo de e-mail's Enviados	
236	total enviados (139 - 18.06.2012 e 97 -> 10.07.2012)
43	Não entregues
193	Entregues

4. Estatística – *emails* enviados (entregues vs respostas)

Estatística - *emails* enviados (entregues vs respostas)

Questionário - Estatistica sobre emails enviados Hospitais, Centros Hospitalares, Clinicas e ARS			
Enviados	**491**	100%	
Não entregues	119	24%	
Entregues	372	76%	100%
Não Lidas	149		40%
Lidas	203		55%
Respostas	***20***		**5%**

Questionário - Estatistica sobre emails enviados Outros Sectores de Actividade			
Enviados	**236**	100%	
Não entregues		0%	
Entregues	236	100%	100%
Não Lidas	43		18%
Lidas	187		79%
Respostas	***6***		**3%**

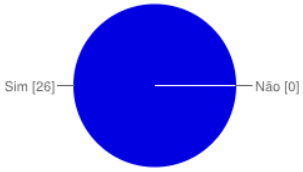
Questionário - Estatistica sobre emails enviados TOTAIS (organizações de Saúde e Outras)			
Enviados	**727**	100%	
Não entregues	119	16%	
Entregues	608	84%	100%
Não Lidas	192		32%
Lidas	390		64%
Respostas	***26***		**4%**

5. Resumo do Questionário

Resumo - Questionário sobre a Implementação de Sistemas de Gestão da Segurança da Informação (SGSI)

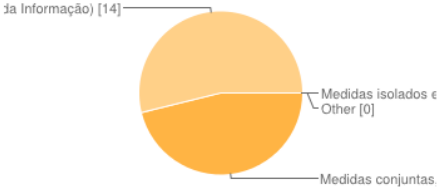
Total de *emails*: Enviados-> **727** (Área saúde: 491, Outras áreas: 236); Entregues-> **608** (Não entregues: 119); Lidas sem resposta-> **390** (Não lidas: 192); **RESPOSTAS-> 26** (**4%** dos entregues)

1. A Segurança de Informação têm grande relevância para a sua organização ?



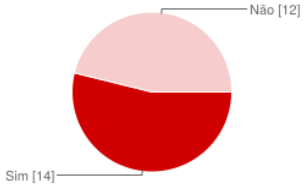
Sim	26	100%
Não	0	0%

2. Acha que a forma mais adequada de o fazer é através de um processo, que resultante de:



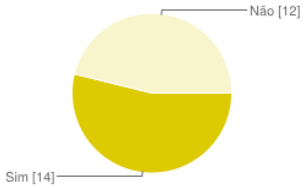
Medidas isolados e informais	0	0%
Medidas conjuntas, integradas e monitorizadas	12	46%
Implementação de um SGSI (Sistema de Gestão de Segurança da Informação)	14	54%
Other	0	0%

3. Conhece a norma ISO/IEC 27001?



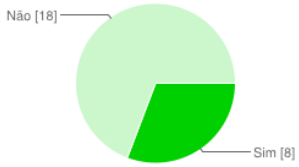
Sim	14	54%
Não	12	46%

4. Conhece a norma ISO/IEC 27002?



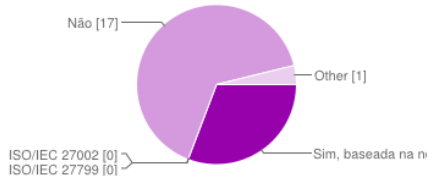
Sim	14	54%
Não	12	46%

5. Conhece a norma ISO/IEC 27799?



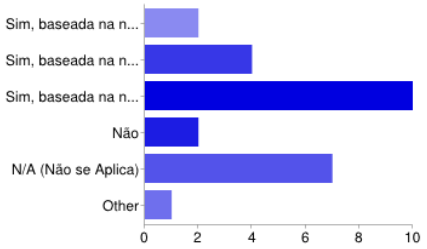
Sim	8	31%
Não	18	69%

6. Têm implementado algum SGSI ?



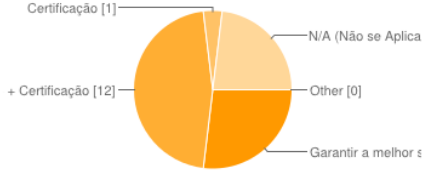
Sim, baseada na norma ISO/IEC 27001	8	31%
Sim, baseada na norma ISO/IEC 27002	0	0%
Sim, baseada na norma ISO/IEC 27799	0	0%
Não	17	65%
Other	1	4%

7. Gostaria de implementar um SGSI ?



Sim, baseada na norma ISO/IEC 27001	2	8%
Sim, baseada na norma ISO/IEC 27002	4	15%
Sim, baseada na norma ISO/IEC 27799	10	38%
Não	2	8%
N/A (Não se Aplica)	7	27%
Other	1	4%

8. Com que obejctivo gostaria de implementar um SGSI ?

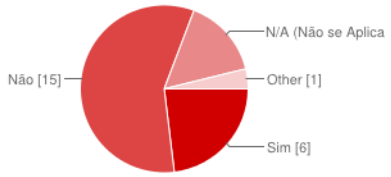


Garantir a melhor solução para segurança da informação	7	27%
Garantir a melhor solução para segurança da informação + Certificação	12	46%
Certificação	1	4%
N/A (Não se Aplica)	6	23%
Other	0	0%

Resumo - Questionário sobre a Implementação de Sistemas de Gestão da Segurança da Informação (SGSI)

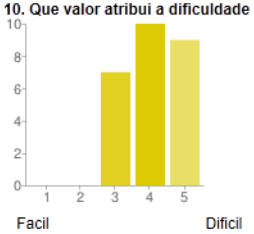
Total de *emails*: Enviados-> **727** (Área saúde: 491, Outras áreas: 236); Entregues-> **608** (Não entregues: 119); Lidas sem resposta-> **390** (Não lidas: 192); **RESPOSTAS-> 26** (**4%** dos entregues)

9. Esta satisfeito com a solução que têm implementada ?



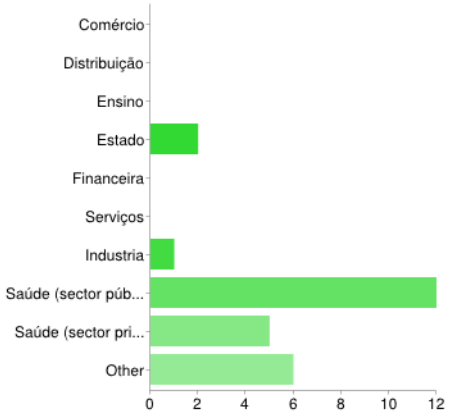
Sim	6	23%
Não	15	58%
N/A (Não se Aplica)	4	15%
Other	1	4%

10. Que valor atribui a dificuldade de implementação de um SGSI ?



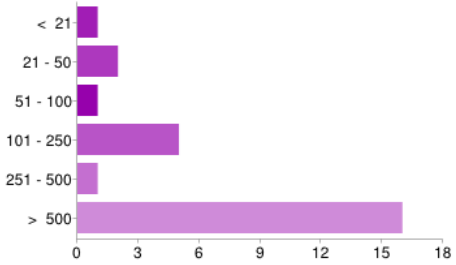
1 -	Facil	0	0%
2		0	0%
3		7	27%
4		10	38%
5 -	Dificil	9	35%

11. Qual é a área de actividade da empresa ?



Comércio	0	0%
Distribuição	0	0%
Ensino	0	0%
Estado	2	8%
Financeira	0	0%
Serviços	0	0%
Industria	1	4%
Saúde (sector público)	12	46%
Saúde (sector privado)	5	19%
Other	6	23%

12. Quantos trabalhadores tem a empresa ?



< 21	1	4%
21 - 50	2	8%
51 - 100	1	4%
101 - 250	5	19%
251 - 500	1	4%
> 500	16	62%

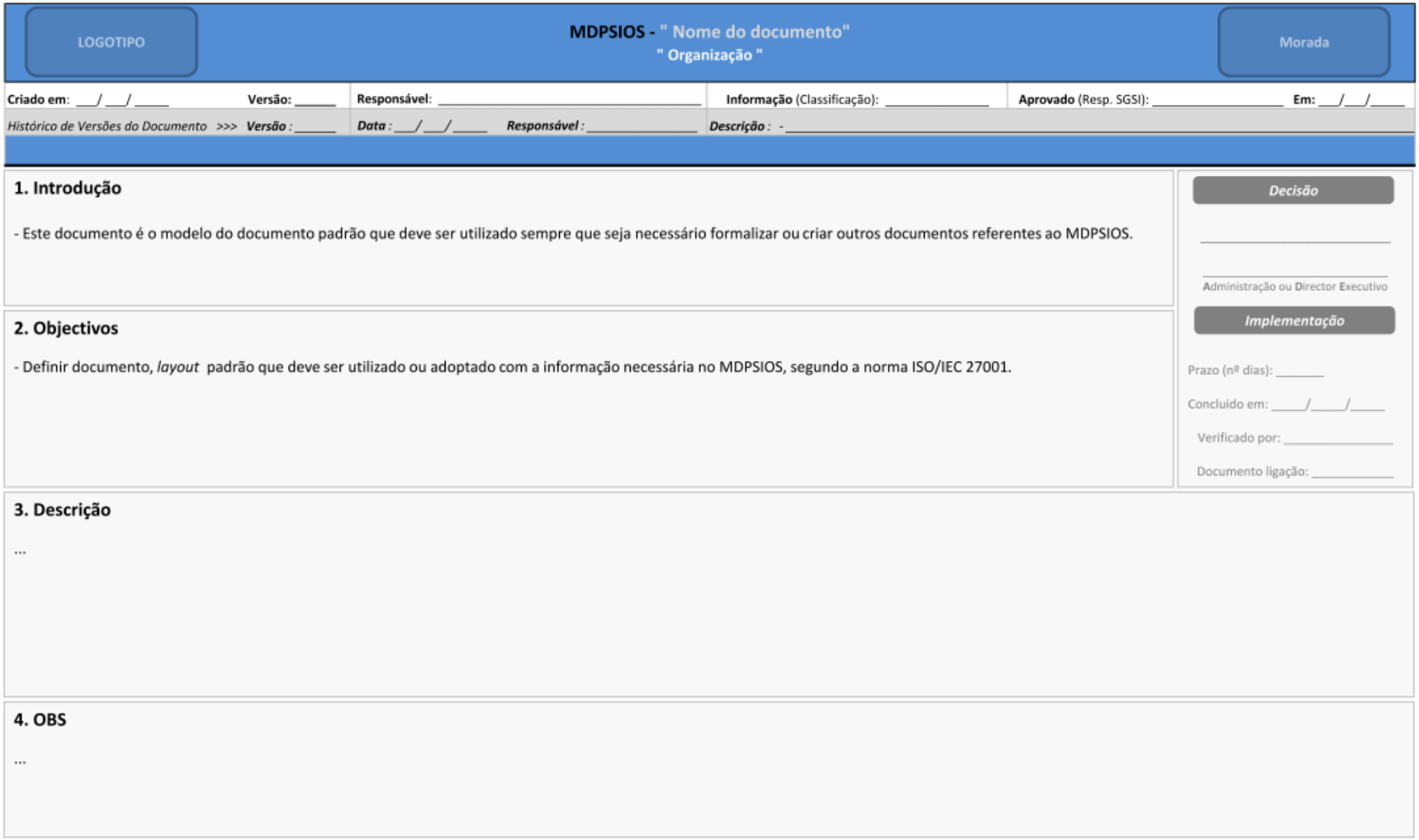
Comentário / OBS:

Não conheço as normas, mas gostaria de implementar. Não estou satisfeito com a solução que tenho, mas que posso melhorar posso | Sim, gostaria de implementar um SGSI, em regime de out-sourcing | Gostaria de analisar as normas para decidir implementar | Exmo Sr, Terei muito gosto em receber o grupo que está a desenvolver este trabalho para uma sessão de troca de ideais e informação sobre este Tema. | Encontra-se em fase de análise a implementação de um SGSI | Não estou satisfeito com a solução que tenho, mas podemos melhorar | A solução que tenho pode sempre ser melhorada

Número de respostas diárias

Anexo F - MPDSIOS

1. Documento Padrão



LOGOTIPO

MDPSIOS - " Nome do documento"
" Organização "

Morada

Criado em: ___/___/_____ **Versão:** _____ | **Responsável**: _____ | **Informação** (Classificação): _____ | **Aprovado** (Resp. SGSI): _____ **Em:** ___/___/_____

Histórico de Versões do Documento >>> ***Versão :*** _____ ***Data :*** ___/___/_____ ***Responsável :*** _____ ***Descrição :*** - _____

1. Introdução

- Este documento é o modelo do documento padrão que deve ser utilizado sempre que seja necessário formalizar ou criar outros documentos referentes ao MDPSIOS.

2. Objectivos

- Definir documento, *layout* padrão que deve ser utilizado ou adoptado com a informação necessária no MDPSIOS, segundo a norma ISO/IEC 27001.

Decisão

_____

_____
Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

3. Descrição

...

4. OBS

...

2. Documento Inventário de Ativos

LOGOTIPO

MDPSIOS - Inventário de Ativos
Organização de Saúde XPTO

Morada

Criado em: 10 / 10 / 2012 **V** **Responsável:** Francisco Carvalho **Informação** (Classificação): Interna **Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 12 / 10 / 2012

Histórico de Versões do Documento >>> ***Versão:*** *V.01* ***Data:*** *10 / 10 / 2012* ***Responsável:*** *Francisco Carvalho* ***Descrição:*** *- Aprovação do Documento*

Iteração nº _____

1. Introdução

2. Objectivos

Decisão

APROVADO

Luís Anibal
~~Administração ou~~ Director Executivo

Implementação

Prazo (nº dias): Imediata

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

Nº Activo	Nome	Localização	Tipo	Data Instalação	Responsável	Área Negócio	Controlo (Actual/Novo)	Vulnerabilidade	Ameaça	Nivel Dificiência	Nivel Exposição	Nivel Severidade (Consequência)

4. OBS

3. Catálogo de Ameaças mais comuns "Tipo e Origem"

LOGOTIPO

MDPSIOS - Ameaças Comuns (Tipo e Origem) / Motivação (Origem e Possiveis Consequências)

" Organização "

Fonte: ISO/IEC 27005:2008

Morada

Tipo	Ameaças Comuns	Origem/Causa
Comprometer Funções	**Abuso de Direitos**	Acidental, Intencional
Dano Físico	**Acidente Grave**	Acidental, Intencional, Natural
Dano Físico	**Água**	Acidental, Intencional, Natural
Comprometer Informação	**Alteração de *Hardware***	Intencional
Comprometer Informação	**Alteração de *Software***	Acidental, Intencional
Acções Não autorizadas	**Comprometimento de Dados**	Intencional
Acções Não autorizadas	**Cópia ilegal de *Software***	Intencional
Comprometer Informação	**Dados de Fontes Não Confiáveis**	Acidental, Intencional
Falhas Técnicas	**Defeito do Equipamento**	Acidental
Falhas Técnicas	**Defeito do *Software***	Acidental
Dano Físico	**Destruição Equipamento e/ou Suporte Magnetico**	Acidental, Intencional, Natural
Comprometer Informação	**Determinação da localização**	Intencional
Comprometer Informação	**Divulgação Indevida**	Acidental, Intencional
Comprometer Funções	**Erro Durante a Utilização**	Acidental
Comprometer Informação	**Escuta Não Autorizada**	Intencional
Comprometer Informação	**Espionagem à Distância**	Intencional
Paragem Serviços Essenciais	**Falha do Ar-condicionado ou Sistema Fornecimento de Água**	Acidental, Intencional
Falhas Técnicas	**Falha do Equipamento**	Acidental
Paragem Serviços Essenciais	**Falha do Equipamento de Telecomunicações**	Acidental, Intencional
Causas Naturais	**Fenômeno Climático**	Natural
Causas Naturais	**Fenômeno Meterológico**	Natural
Causas Naturais	**Fenômeno Sismico**	Natural
Causas Naturais	**Fenômeno Vulcânico**	Natural
Dano Físico	**Fogo**	Acidental, Intencional, Natural
Comprometer Funções	**Forjar Direitos**	Intencional
Comprometer Informação	**Furto de Equipamentos**	Intencional
Comprometer Informação	**Furto de Suporte Magnetico e/ou Documentos**	Intencional
Comprometer Funções	**Indisponibilidade Recursos Humanos**	Acidental, Intencional, Natural
Comprometer Informação	**Interceptação de Sinais e ou Interferência Comprometedora**	Intencional
Paragem Serviços Essenciais	**Interrupção do Fornecimento de Energia**	Acidental, Intencional, Natural
Causas Naturais	**Inundação**	Natural
Causas Naturais	**Poeira, Corrosão, Congelamento**	Acidental, Intencional, Natural
Dano Físico	**Poluição**	Acidental, Intencional, Natural

Origem das Ameaças	Motivação	Possiveis Consequências
Hacker ou Cracker	Desafio Ego Rebeldia *Status* Dinheiro	. Hacker . Engenharia Social . Invasão de Sistemas, Infiltrações e Entradas Não Autorizadas . Acesso Não autorizado ao Sistema
Criminoso Digital	Destruição de Informações Divulgação Ilegal de Informações Ganho Monetário Alteração de dados Não Autorizados	. Crime Digital (ex.: perseguição no mundo digital) . Acto Fraudolento (ex.: reutilização indevida de credenciais e dados transmitidos, fazer-se passar por outra pessoa, interceptação) . Suborno por Informação . Spoofing (fazer-se passar por outro) . Invasão de Sistemas
Terrorista	Chantagem Destruição Exploração Vingança Ganho Político	. Bomba/Terrorismo . Guerra de Informação . Ataque a Sistemas (ex.: ataque distribuido de negação de serviços) . Invasão de Sistema . Alteração do Sistema
Espionagem Industrial (serviços de inteligência, empresas, governos estrangeiros, outros grupos de interesse ligadosao governo)	Vantagem Competitiva Espionagem Econômica	. Garantir Vantagem de um Posicionamento Defensivo . Garantir Vantagem Politica . Exploração Econômica . Furto de Informação .Violação da privacidade de Pessoas . Engenharia Social . Invasão de Sistema . Acesso Não Autorizado ao Sistema (acesso a informação restrita, de propriedade esclusiva, e/ou relativa à Tecnologia)
	Curiosidade Ego Obtenção de Informações Úteis para Serviços de Inteligência	. Agressão a Funcionário . Chantagem

LOGOTIPO

MDPSIOS - Ameaças Comuns (Tipo e Origem) / Motivação (Origem e Possiveis Consequências)

" Organização "

Fonte: ISO/IEC 27005:2008

Morada

Tipo	Ameaças Comuns	Origem/Causa
Acções Não autorizadas	**Processamento Ilegal de Dados**	Intencional
Disturbios por Radiação	**Pulsos Electromagnéticos**	Acidental, Intencional, Natural
Disturbios por Radiação	**Radiação Electromagnética**	Acidental, Intencional, Natural
Disturbios por Radiação	**Radiação Térmica**	Acidental, Intencional, Natural
Comprometer Informação	**Recuperação de Suporte Magnetico Reciclada ou Deitada Fora**	Intencional
Comprometer Funções	**Repúdio de Acções**	Intencional
Falhas Técnicas	**Saturação do Sistema de Informação**	Acidental, Intencional
Acções Não autorizadas	**Uso Cópias *Software* falsificado ou Ilegal**	Acidental, Intencional
Acções Não autorizadas	**Uso Não Autorizado de Equipamento**	Intencional
Falhas Técnicas	**Violação Condições Uso SI que Possibilitam a sua Manutenção**	Acidental, Intencional

Origem das Ameaças	Motivação	Possiveis Consequências
Pessoal Interno (funcionários mal treinados, insatisfeitos, mal intencionados, negligntes, desonestos ou dispensados)	Ganho Monetário Vingança Erros e Omissões Não Intencionais (ex.: erro na entrada de dados, erro de programação)	. Vasculhar Informação de Proriedade esclusiva . Uso Impróprio de Recurso Computacional . Fraude e Furto . Suborno por Informação . Entrada de dados Falsificados ou Corrompidos . Interceptação . Código Malicioso (ex.: virus, bomba lógica, cavalo de troia, outros) . Venda de Informações Pessoais . Defeitos {*bugs*} no Sistema . Invasão de Sistemas . Sabotagem de Sistemas . Acesso Não Autorizado ao Sistema

4. Catálogo de Vulnerabilidades mais Comuns “Tipos e Ex. Ameaças”

LOGOTIPO

MDPSIOS - Vulnerabilidades mais Comuns (Tipos e Exemplos de Ameaças)

" Organização "

Fonte: ISO/IEC 27005:2008

Morada

Tipos	Vulnerabilidades Comuns	Exemplo de Ameaças
Organização	Acordo de Nível de Serviço (SLA - da sigla do termo em inglês) inexistente ou insuficiente	Violação de condições de utilização do SI que possibilitem a sua manutenção
Hardware	Armazenamento Não Protegido	Furto de suporte magnetico ou documentos
Rede	Arquitetura Insegura de rede	Espionagem à distância
Software	Atribuição Errada de Direitos de Acesso	Abuso de direitos
Organização	Atribuição Inadequada das Responsabilidades Pela Segurança da Informação	Repúdio de ações
Organização	Ausência das Responsabilidade Ligadas à segurança da Informação nas Descrições de Cargos e Funções	Erro durante a utilização
Recursos Humanos	Ausência de Recursos Humanos	Indisponibilidade Recursos Humanos
Organização	Ausência de Registos nos Arquivos de Auditoria (*logs*) de Administratores e Operadores	Erro durante a utilização
Rede	Conexões de Redes Públicas Desprotegidas	Uso não autorizado de equipamento
Software	Configuração de Parametros Incorreto	Erro durante a utilização
Software	Datas Incorretas	Erro durante a utilização
Software	Destruição ou Reutelização de Suporte Magnetico de Armazenamento sem Procedimento Apropriado de remoção de Dados	Abuso de direitos
Software	Documentação Inexistente	Erro durante a utilização
Rede	Download e Uso Não Controlado de *Software*	Alteração de *software*
Rede	Especificações Confusas ou Incompletas para os Programadores	Defeito de *software*
Software	Falhas Conhecidas no Software	Abuso de direitos
Software	Falta de *"Logout"* quando não ninguem na estção de trabalho	Abuso de direitos
Recursos Humanos	Falta de Conscientização em segurança	Erro durante a utilização
Hardware	Falta de Cuidado Durante a Destruição	Furto de suporte magnetico ou documentos
Hardware	Falta de Rotina de Substituição Periódica	Destruição Equipamento ou suporte Magnetico
Local ou Instalações	fornecimento de Energia Instável	Interrupção de fornecimento de energia
Rede	Gestão de Password/Senhas mal efetuada	Forjar Direitos
Rede	Gestão de Rede Inadequada (quanto à flexibilidade de roteamento)	Saturação do Sistema de Informação
Organização	Inexistência de Análises Críticas Periódicas Por Parte da Direção	Uso não autorizado de equipamento
Organização	Inexistência de Auditorias Periódicas (supervisão)	Abuso de direitos
Organização	Inexistência de Autrização Para as Instalações de Processamento de Informações	Furto de suporte magnetico ou documentos
Hardware	Inexistencia de Controle Eficiente de Mudança de Configuração	Erro durante a utilização
Rede	Inexistência de Controlo Eficaz de Mudança	Defeito de *software*
Organização	Inexistência de Controlo sobre Ativos Fora das Dependências	Furto de equipamentos
Rede	Inexistência de Cópias de Segurança (backup)	Alteração de *software*
Rede	Inexistência de Evidências que Comprovem o Envio ou Recebimento de Mensagens	Repúdio de ações

LOGOTIPO

MDPSIOS - Vulnerabilidades mais Comuns (Tipos e Exemplos de Ameaças)

" Organização "

Fonte: ISO/IEC 27005:2008

Morada

Tipos	Vulnerabilidades Comuns	Exemplo de Ameaças
Recursos Humanos	Inexistência de Mecanismos de Monitorização	Processamento ilegal de dados
Rede	Inexistência de Mecanismos de Protecção Física no Edificio, Portas e Janelas	Furto de suporte magnetico ou documentos
Local ou Instalações	Inexistência de Mecanismos de Protecção Física no Edificio, Portas e Janelas	Furto de equipamentos
Organização	Inexistência de Mecanismos Estabelicidos Para a Monitorização de Violação de Segurança	Furto de suporte magnetico ou documentos
Organização	Inexistência de Plano de Continuidade	Falha de equipamento
Organização	Inexistência de Politica de Utilização de Correspondência Electrônica (*e-mail*)	Erro durante a utilização
Organização	Inexistência de Politica Formal Sobre Utilização de Computadores Portateis ou Dispositivos Móveis	Furto de equipamentos
Recursos Humanos	Inexistência de Politicas de Utilização Correta de Telecomunicação e Troca Mensagens	Uso não autorizado de equipamento
Organização	Inexistência de Procedimento de Controle de Mudanças	Violação de condições de utilização do SI que possibilitem a sua manutenção
Organização	Inexistência de Procedimento Formal Para Controle da Documentação do SGSI	Comprometimento de dados
Organização	Inexistência de Procedimento Formal Para Registo e Remoção de Utilizadores	Abuso de direitos
Organização	Inexistência de Procedimento Formal Para Supervisão dos Registos do SGSI	Comprometimento de dados
Organização	Inexistência de Procedimento Para Garantir a Conformidade Com os Direitos de Propriedade Intelectual	Uso de cópias de software falsificadas ou ilegais
Organização	Inexistência de Procedimentos de Monitorização das Instalações de Processamento de Informações	Abuso de direitos
Organização	Inexistência de Procedimentos Para a Manipulação de Informações Classificadas	Erro durante a utilização
Organização	Inexistência de Procedimentos Para Identificação e Análise/Avaliação de Riscos	Abuso de direitos
Organização	Inexistência de Procedimentos Para Instalção de *Software* em Sitemas Operacionais	Erro durante a utilização
Organização	Inexistência de Procedimentos Para o Relato de Fragilidades Ligadas à Segurança	Uso não autorizado de equipamento
Organização	Inexistência de Processo disciplinar em Caso de Incidentes Relacionados com Segurança da Informação	Furto de equipamentos
Organização	Inexistência de Processo Formal de Autorização das Disponiveis Publicamente	Dados de fontes não confiáveis
Organização	Inexistência de Processo Formal Para Analise Crítica dos Direitos de Acesso (supervisão)	Abuso de direitos
Rede	Inexistência de Relatórios de Gestão	Uso não autorizado de equipamento
Organização	Inexistência de Relatos de Falha nos Arquivos (logs) de Auditoria das Actividades de Administradores e Operadores	Abuso de direitos
Software	Inexistencia de Um trilho de Auditoria	Abuso de direitos
Rede	Inexistencia Mecanismos de Autenticação e Identificação (ex.: atenticação utilizadores)	Forjar Direitos
Software	Interface de Utilizador Complicado	Erro durante a utilização
Rede	Junções da Cablagem Mal Feitas	Falha de equipamento de telecomunicações

LOGOTIPO

MDPSIOS - Vulnerabilidades mais Comuns (Tipos e Exemplos de Ameaças)

" Organização "

Fonte: ISO/IEC 27005:2008

Morada

Tipos	Vulnerabilidades Comuns	Exemplo de Ameaças
Rede	**Linhas de comunicação Desprotegidas**	Escuta não autorizada
Local ou Instalações	**Localização em área suscetivel a Inundações**	Inudação
Hardware	**Manutenção Insuficiente / Instalação Defeituosa do Suporte Magnetico de Armazenamento**	Violação de condições de utilização do SI que possibilitem a sua manutenção
Rede	**Não Identificação e Não Autenticação do Emissor e do Receptor**	Forjar Direitos
Organização	**Política de Mesas e Telas Limpas (clear desk and clear screen) Inexistente ou Insuficiente**	Furto de suporte magnetico ou documentos
Rede	**Ponto Único de Falha**	Falha de equipamento de telecomunicações
Recursos Humanos	**Procedimentos de Recrutamento Inadequados**	Destruição Equipamento ou suporte Magnetico
Software	**Procedimentos de teste de Software insuficientes ou Inexistentes**	Abuso de direitos
Organização	**Provisões (relativas à Segurança) Insuficientes ou Inexistentes, em Contratos com Clientes e/ou Terceiros**	Abuso de direitos
Organização	**Provisões (relativas à Segurança) Insuficientes ou Inexistentes, em Contratos com Clientes e/ou Terceiros**	Processamento ilegal de dados
Hardware	**Realização de Cópias Não Controlada**	Furto de suporte magnetico ou documentos
Organização	**Resposta Inadequada do Serviço de Manutenção**	Violação de condições de utilização do SI que possibilitem a sua manutenção
Hardware	**Sensibilidade à humidade, poeira, sujidade**	Poeira, corrosão, congelamento
Hardware	**Sensibilidade À Radiação Eletromagnética**	Radiação eletromagnetica
Hardware	**Sensibilidade a Variações de Temperatura**	Fenômeno meteorológico
Hardware	**Sensibilidade a Variações de Voltagem**	Interrupção de fornecimento de energia
Rede	**Serviços Desnecessários Continuam Activados**	Processamento ilegal de dados
Software	***Software* Muito Destruido**	Comprometimento de dados
Rede	***Software* Novo ou Imaturo**	Defeito de *software*
Recursos Humanos	**Trabalho Não Supervisionado do Pessoal de Limpeza ou de Terceiros**	Furto de suporte magnetico ou documentos
Rede	**Tráfego Sensivel Desprotegido**	Escuta não autorizada
Rede	**Transferência de Password / Senhas em Claro**	Espionagem à distância
Recursos Humanos	**Treino Insuficiente em Segurança**	Erro durante a utilização
Local ou Instalações	**Uso Inadequado ou Sem Cuidados Necessários de Mecanismos de Controle do Acesso Fisico as Instalações**	Destruição Equipamento ou suporte Magnetico
Recursos Humanos	**Uso Incorreto de *Software* e *Hardware***	Erro durante a utilização
Software	**Utilização de Programas com Um conjunto Errado de Dados (referentes a outros periodos)**	Comprometimento de dados

5. Níveis de Risco

Nível de Risco (NR) = NP x NS A matriz do nível de risco indica a prioridade de intervenção, a qual é expressa em cinco níveis. (Fonte: "Avaliação de Riscos" de Cristina P Amador)		- Não é de esperar que a situação perigosa se materialize, ainda que possa ser concebida.	- A materialização da situação perigosa pode ocorrer.	- A materialização da situação perigosa é possivel de ocorrer pelo menos uma vez com danos.	-A materialização da situação perigosa pode ocorrer várias vezes durante o período de trabalho.	- Normalmente a materialização da situação perigosa ocorre com frequência.
Danos na Informação e/ou materiais	**NS / NP**	**1 a 3**	**4 a 6**	**10 a 18**	**24 a 30**	**40 a 70**
- Pequenas perdas de informação, sem qualquer impacto. - Pequenas perdas materiais	**10**	V 10 30	V 40 60	V 80 IV 180	IV 240 300	III 400 700
- Pequenas perdas de informação, com ligeiro impacto. - Reparação sem necessidade de paragem do processo ou actividade.	**25**	V 25 75	IV 100 150	IV 200 III 450	III 600 750	III 1000 II 2400
- Perda de informação que pode ser recuperavel. - Para efetuar a reparação, requer a paragem do processo ou actividade.	**60**	V 60 IV 180	IV 240 III 460	III 480 1080	II 1440 1800	II 2400 I 4200
- Perda informação que podem ser irrecuperavel ou irreparaveis. - Destruição parcial do sistema (reparação complexa e onerosa).	**90**	IV 90 270	III 360 540	III 720 II 1620	II 2160 2700	I 3600 6300
- Perda de informação total e/ou pernamente. - Destruição total do sistema (difícil renovação ou reparação)	**155**	IV 155 III 465	III 620 930	II 1240 2790	I 3720 4650	I 6200 10850

6. Níveis de Controlo

Nivel de Risco (NR)		*Nível de Controlo (NC)*	*Significado*
[3600; 10850]	Muito Alto	I = 1	Situação Critica. Intervenção Imediata. Eventual paragem imediata. Isolar o perigo até serem adotadas medidas de controlo permanentes.
[1240; 3100]	Alto	II = 2	Situação a Corrigir. Adotar medidas de controlo enquanto a situação. Perigosa não for eliminada ou reduzida.
[360; 1080]	Médio	III = 3	Situação a melhorar. Deverão ser elaborados planos ou programas documentados de intervenção.
[90; 300]	Baixo	IV = 4	Melhorar se possível justificando a intervenção
[10; 80]	Muito Baixo	V = 5	Intervir apenas se uma analise mais pormenorizada o justificar.

7. Documento de Analise / Avaliação / Monitorização do Risco

LOGOTIPO

MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Documento AAM nº _____ | Iteração nº _____

Avaliação / Classificação

ID Activo: _____ Dimensão: _____

Norma: _____ Dominio(nº):_____ Secção (nº): _____

Risco não residual (%): _____ Risco Residual (%): _____

Questões ou Riscos identificados:

(As Questões ou Riscos identificados a colocar nesta caixa servem para detectar problemas de segurança da informação e determinar como implementar com sucesso o SGSI). Servirá também para orientação da Administração , Director Executivo ou Responsavel SGSI, na avaliação e decisão sobre as medidas a adoptar)

Decisão

_____

Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: ____/____/____

Verificado por: _____

Documento ligação: _____

Considerações do responsável do SGSI:

(Nesta caixa devem ser colocadas as questões relevantes em termos de negócio que o responsável do SGSI deve ter como preocupação em relação a questão / risco acima colocado)

Fontes e/ou localização da Informação e/ou equipamentos:

(Nesta caixa deve ser colocada a fonte e/ou localização da informação e/ou equipamentos, que estejam dentro ou fora da organização para ajudar o responsável do SGSI na determinação da resposta ou medida relativamente a questão / risco acima colocado)

Critérios de Avaliação e Desempenho:

(Nesta caixa devem ser identificados os critérios que podem ser utilizados pelo responsavel do SGSI para determinar a eficácia da organização e/ou abordar os problemas de segurança em relação a questão / risco acima colocado)

Medidas a Implementar: (ver Documento de Apoio ao Tratamento do Risco)

(Nesta caixa deve-se descrever os passos que a organização deve seguir para fazer face as considerações e situações de segurança acima descritas)

MDPSIOS [Pag. 1 de 2]

LOGOTIPO

MDPSIOS - Documento de Analise / Avaliação / Monitorização do Risco

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Documento AAM nº _____ | Iteração nº _____

Analise Financeira (previsão de perda "Custo" vs Custo Investimento vs resultado a previsto) :

Decisão do CIO: _____ *Ass:* _____ *Data:* ___/___/____

(Nesta caixa deve-se descrever a previsão de perda "quanto custa organização a concretização do risco" versos o custo do investimento para metigar o risco versos a previsão do resultado que se obtem mediante o investimento a fazer)

8. Documento de Apoio ao Tratamento do Risco

LOGOTIPO	**MDPSIOS - Documento de Apoio ao Tratamento do Risco** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

ID Ativo: _____ Nome Ativo: _____ Documento AAM nº _____ | Iteração nº _____

Atitude Perante o Risco

1. Deve-se definir qual a atitude correcta a assumir, tendo em conta o valor do risco associado a cada recurso.
2. As atitudes possiveis e definidas para este Modelo Documental são:

Atitude a assumir	Descrição	Observações
Aceitar/Reter o Risco	Considerar os índices de 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 aceitaveis para a organização.	
Anular/Evitar 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.	
...	...	

Tipo de medidas

1. Pode ser definido um catalogo de médidas que ser utilizada como referência (Catalogo de Medidas). *Não definido, será um ponto de melhoramento a considerar neste Modelo Documental.*
2. No entanto um tipo de classificação das medidas, que normalmente não aparece nos catálogos, mas que pode ser útil para a estratégia de segurança da organização e que vamos considerar para este Modelo Documental e a seguinte:

Medidas	Descrição	Observações
Correcção	Medidas que tem como objectivo reduziro efeito da ocorrencia de um incidente.	
Dissuação	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 correctivas.	
Diversão	Medidas que permitem 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.	
...	...	

(Adicionar futuros itens ou informação relevante que pode servir de apoio a decisão e melhoramento do SGSI)

---

9. Avaliação de Risco / Definição de Controlos - Global

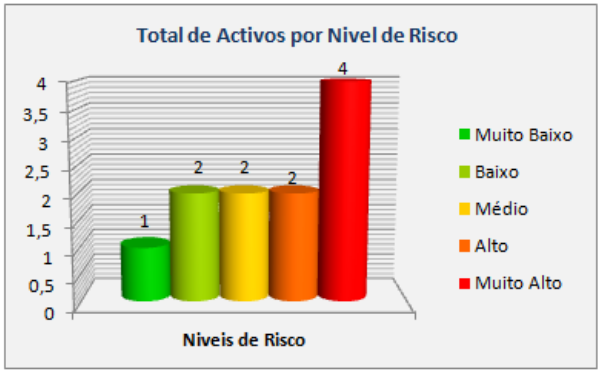
LOGOTIPO

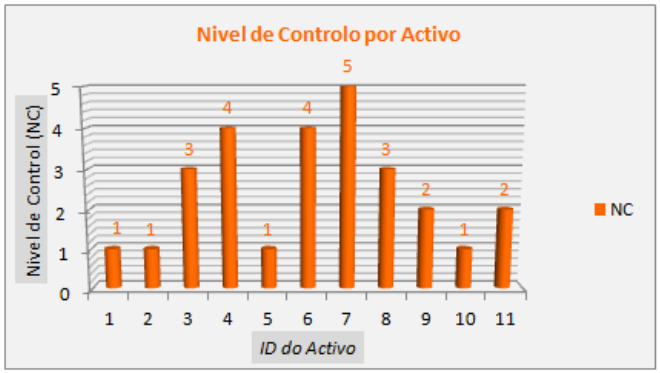
MDPSIOS - Identificação de Activos / Avaliação de Risco / Definição de Objectivos_Controlos

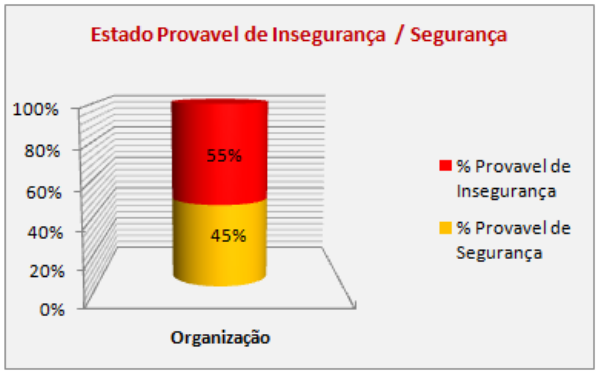
" Organização "

Morada

Identificação de Activos e Necessidade de Segurança						Avaliação do Risco (...)										Objectivos e Gestão Documental				
ID	Activo	Dimensão	Domínio (ISO 27002 | ISO 27799)	Ameaça (...)	Vulnerabilidade (...)	Nível Deficiência	(ND)	Nível Exposição	(NE)	Nível Probabilidade	(NP)	Nível de Severidade	(NS)	NÍVEL de RISCO	(NR)	Nível Controlo (NC)	Atitude Assumida (...)	Tipo de Medidas (...)	ISO 27002 - Objectivo / Medidas / Controlo (...)	ISO 27799 - Objectivo / Medidas / Controlo (...)	Documento Apoio Iteração Nº (...)
1	Software ERP	1. Confidencialidade	11. | 7.8 - Controlo de Acesso.	Alteração de Software	Atribuição Errada de Direitos de Acesso	4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	4. Grave	90	Muito Alto	45000	1	Reduzir o Risco	Correcção	11.5.3 - Sistema de Gestão de Passwords	7.8.5.1 - Restrição de acesso a informação	
2	Software ERP	3. Disponibilidade	14. | 7.11 - Gestão da Continuidade do Negócio.	Falha do Equipamento	Inexistência de Plano de Continuidade	4. Muito Deficiente	10	3. Ocasional	3	Alta	30	5. Catastrófico	155	Muito Alto	46500	1	Amular/Evitar o Risco	Detecção	14.1 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	7.11 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	
3	Software ERP	2. Integridade	8. | 7.5 - Segurança Relacionada Com os Pessoas.	Erro Durante a Utilização	Inexistência de Procedimentos Para a Manipulação de Informações Classificadas	3. Dificente	6	1. Esporádica	1	Baixa	6	3. Moderado	60	Médio	360	3	Amular/Evitar o Risco	Prevenção	8.2.2 - Consencialização para segurança de informação, educação e formação	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
4	A1	5. Autenticidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Software	Falhas Conhecidas no Software	2. Melhorável	2	2. Pouco Frequente	2	Baixa	4	2. Leve	25	Baixo	100	4	Transferir o Risco	Dissuação	8.1.1 - Papéis e Responsabilidades	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
5	A3	3. Disponibilidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Hardware	Uso Incorreto de Software e Hardware	3. Dificente	6	4. Frequente	4	Alta	24	5. Catastrófico	155	Muito Alto	3720	1	Aceitar/Reter o Risco	Correcção	10.2.3 - Gestão de mudanças nos serviços de terceiros	7.7.2 Gestão de Prestação de Serviços por Terceiros	
6	A5					4. Muito Deficiente	10	1. Esporádica	1	Média	10	2. Leve	25	Baixo	250	4					
7	A6					1. Aceitável	1	3. Ocasional	3	Muito Baixa	3	2. Leve	25	Muito Baixo	75	5					
8	A8					4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	1. Insignificante	10	Médio	500	3					
9	A10					4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	2. Leve	25	Alto	1250	2					
10	A12					5. Deficiência Total	14	5. Continuada	5	Muito Alta	70	4. Grave	90	Muito Alto	6300	1					
11	A14					3. Dificente	6	3. Ocasional	3	Média	18	5. Catastrófico	155	Alto	2790	2					







10. Avaliação de Risco – Identificação Ativos e Necessidade Segurança

LOGOTIPO

Identificação de Activos e Necessidade de Segurança

ID	Activo	Dimensão	Dominio (ISO 27002 | ISO 27799)	Ameaça (...)	Vulnerabiliade (...)
1	Software ERP	1. Confidencialidade	11. | 7.8 - Controlo de Acesso.	Alteração de Software	Atribuição Errada de Direitos de Acesso
2	Software ERP	3. Disponibilidade	14. | 7.11 - Gestão da Continuidade do Negócio.	Falha do Equipamento	Inexistência de Plano de Continuidade
3	Software ERP	2. Integridade	8. | 7.5 - Segurança Relacionada Com as Pessoas.	Erro Durante a Utilização	Inexistência de Procedimentos Para a Manipulação de Informações Classificadas
4	A1	5. Autenticidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Software	Falhas Conhecidas no Software
5	A3	3. Disponibilidade	10. | 7.7 - Gestão das Operações e Comunicações.	Alteração de Hardware	Uso Incorreto de Software e Hardware
6	A5				
7	A6				
8	A8				
9	A10				
10	A12				
11	A14				

11. Avaliação de Risco – Estimativa de Riscos

MDPSIOS - Identificação de Activos / Avaliação de Risco / Definição de Controlos

" Organização "

Avaliação do Risco (...)

Nivel Deficiência	(ND)	Nivel Exposição	(NE)	Nivel Probabilidade	(NP)	Nivel de Severidade	(NS)	NIVEL de RISCO	(NR)	Nivel Controlo (NC)
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	4. Grave	90	Muito Alto	4500	1
4. Muito Deficiente	10	3. Ocasional	3	Alta	30	5. Catastrófico	155	Muito Alto	4650	1
3. Dificente	6	1. Esporádica	1	Baixa	6	3. Moderado	60	Médio	360	3
2. Melhorável	2	2. Pouco Frequente	2	Baixa	4	2. Leve	25	Baixo	100	4
3. Dificente	6	4. Frequente	4	Alta	24	5. Catastrófico	155	Muito Alto	3720	1
4. Muito Deficiente	10	1. Esporádica	1	Média	10	2. Leve	25	Baixo	250	4
1. Aceitável	1	3. Ocasional	3	Muito Baixa	3	2. Leve	25	Muito Baixo	75	5
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	1. Insignificante	10	Médio	500	3
4. Muito Deficiente	10	5. Continuada	5	Muito Alta	50	2. Leve	25	Alto	1250	2
5. Deficiência Total	14	5. Continuada	5	Muito Alta	70	4. Grave	90	Muito Alto	6300	1
3. Dificente	6	3. Ocasional	3	Média	18	5. Catastrófico	155	Alto	2790	2

12. Avaliação de Risco – Medidas, Objectivos e Controlos

Morada

Objectivos e Gestão Documental

Atitude Assumida (...)	Tipo de Medidas (...)	ISO 27002 - Objectivo / Medidas / Controlo (...)	ISO 27799 - Objectivo / Medidas / Controlo (...)	Documento Apoio Iteração Nº (...)
Reduzir o Risco	Correcção	11.5.3 - Sistema de Gestão de Passwords	7.8.5.1 - Restrição de acesso a informação	
Anular/Evitar o Risco	Detecção	14.1 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	7.11 Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio	
Anular/Evitar o Risco	Prevenção	8.2.2 - Consencialização para segurança de informação, educação e formação	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
Transferir o Risco	Dissuação	8.1.1 - Papéis e Responsabilidades	7.5.2.2 - Consencialização para segurança de informação, educação e formação	
Aceitar/Reter o Risco	Correcção	10.2.3 - Gestão de mudanças nos serviços de terceiros	7.7.2 Gestão de Prestação de Serviços por Terceiros	

13. Estatística Controlos Implementados

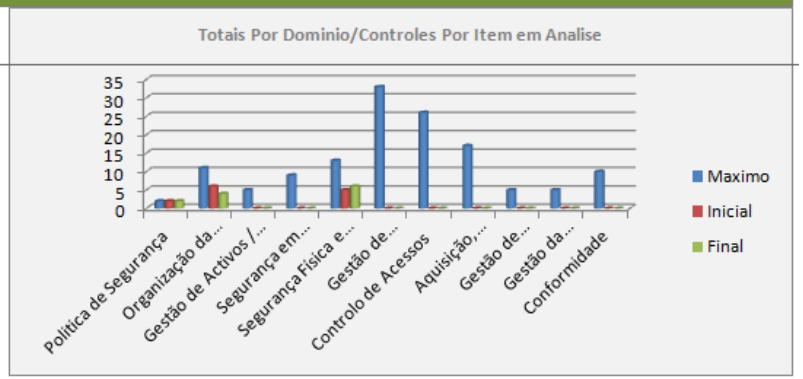
LOGOTIPO

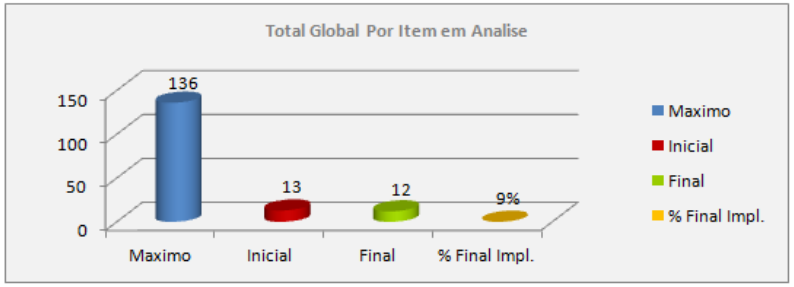
MDPSIOS - Estatistica Controlos Implementados (ISO 27799)

" Organização "

Morada

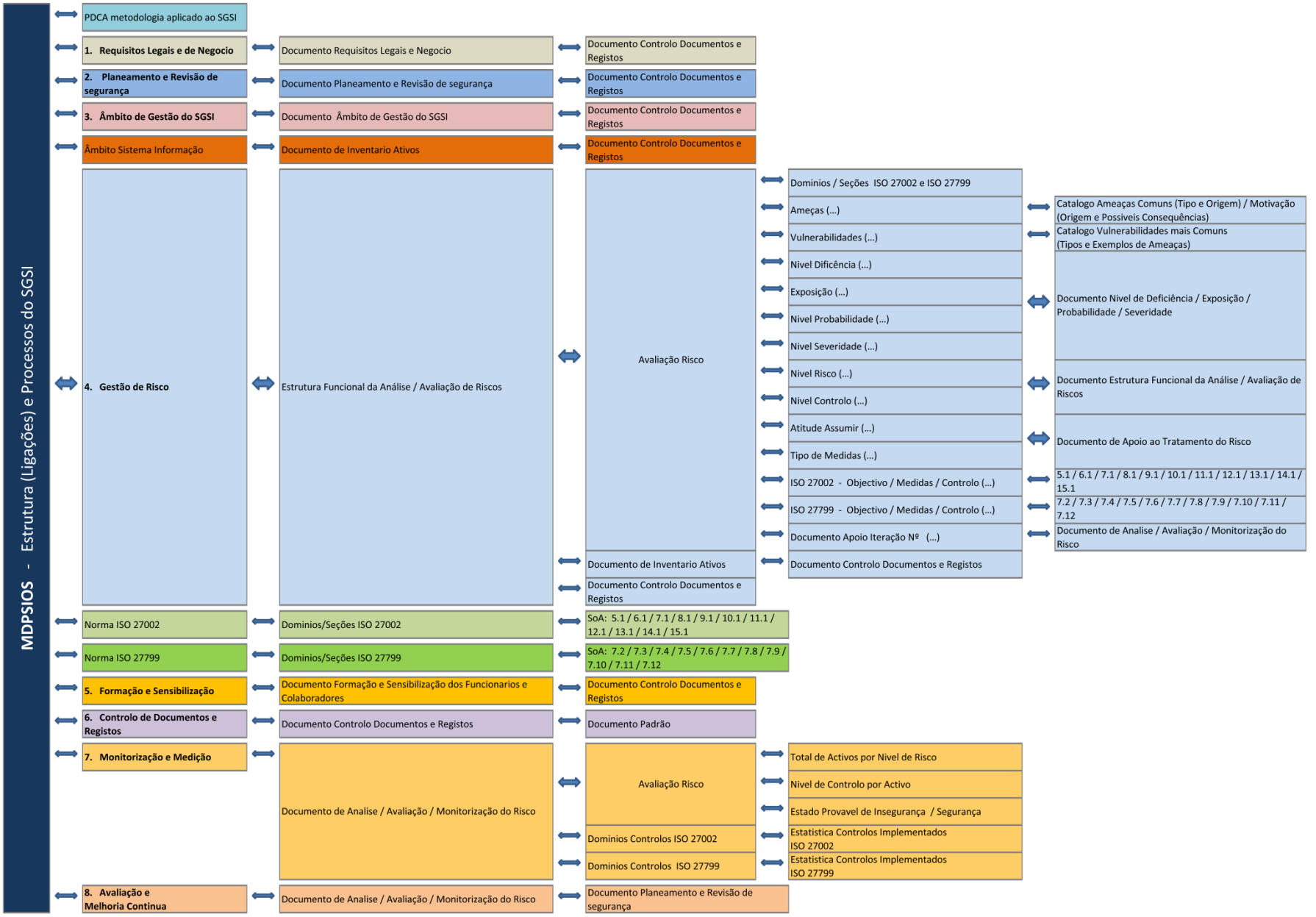
Dominio ***(Controlos)*** ->	***Maximo***	***Inicial***	***Final***	***% Final Impl.***
7.2 Politica de Segurança	2	2	2	100%
7.3 Organização da Segurança da Informação	11	6	4	36%
7.4 Gestão de Activos / Recursos	5	0	0	0%
7.5 Segurança em Recursos Humanos	9	0	0	0%
7.6 Segurança Física e Ambiental	13	5	6	46%
7.7 Gestão de Comunicações e Operações	33	0	0	0%
7.8 Controlo de Acessos	26	0	0	0%
7.9 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	17	0	0	0%
7.10 Gestão de Incidentes de Segurança da Informação	5	0	0	0%
7.11 Gestão da Continuidade do Negócio	5	0	0	0%
7.12 Conformidade	10	0	0	0%
Total	***136***	***13***	***12***	***9%***





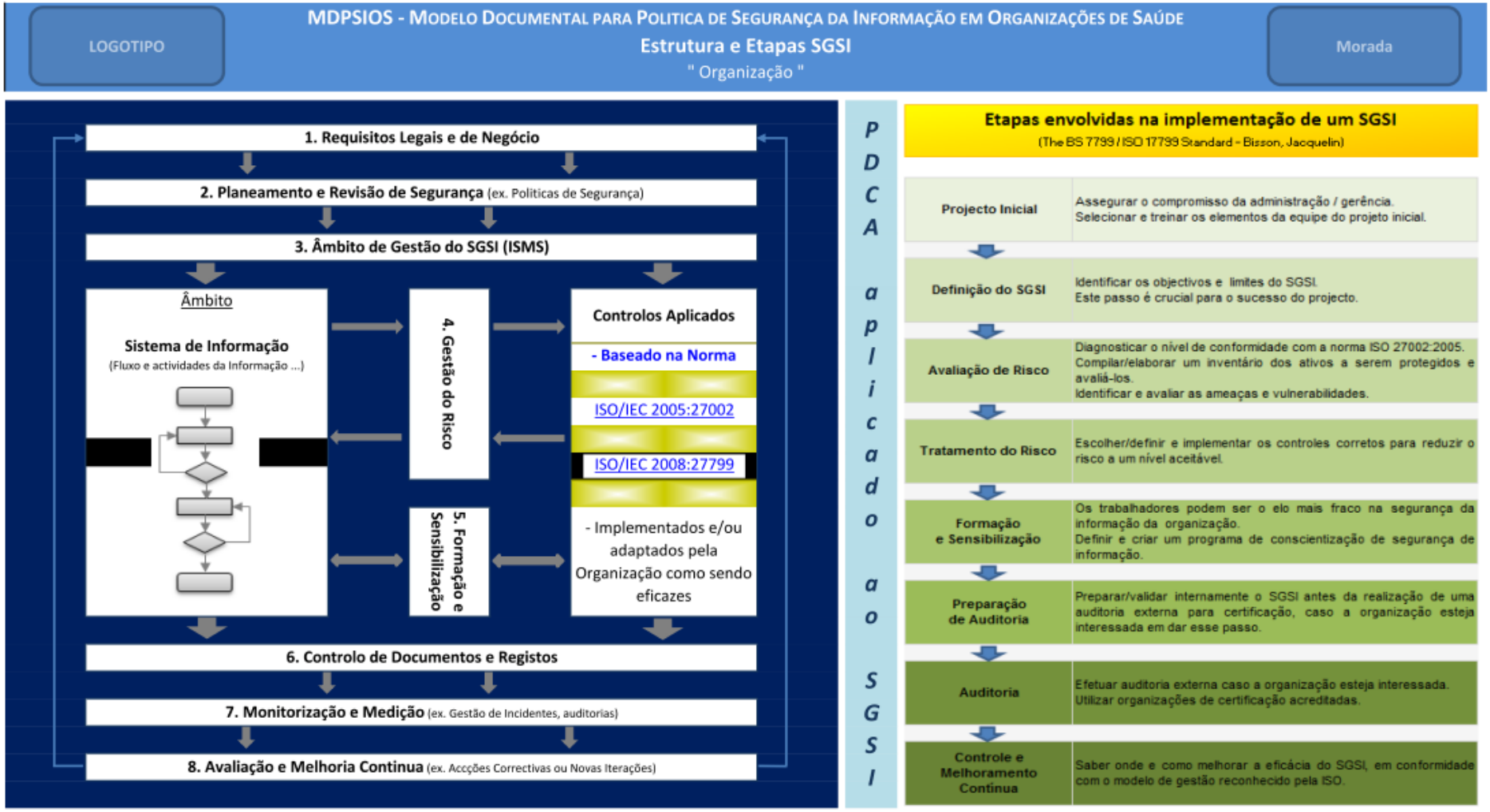
14. Estrutura Funcional da Aplicação

(disponível na página seguinte)

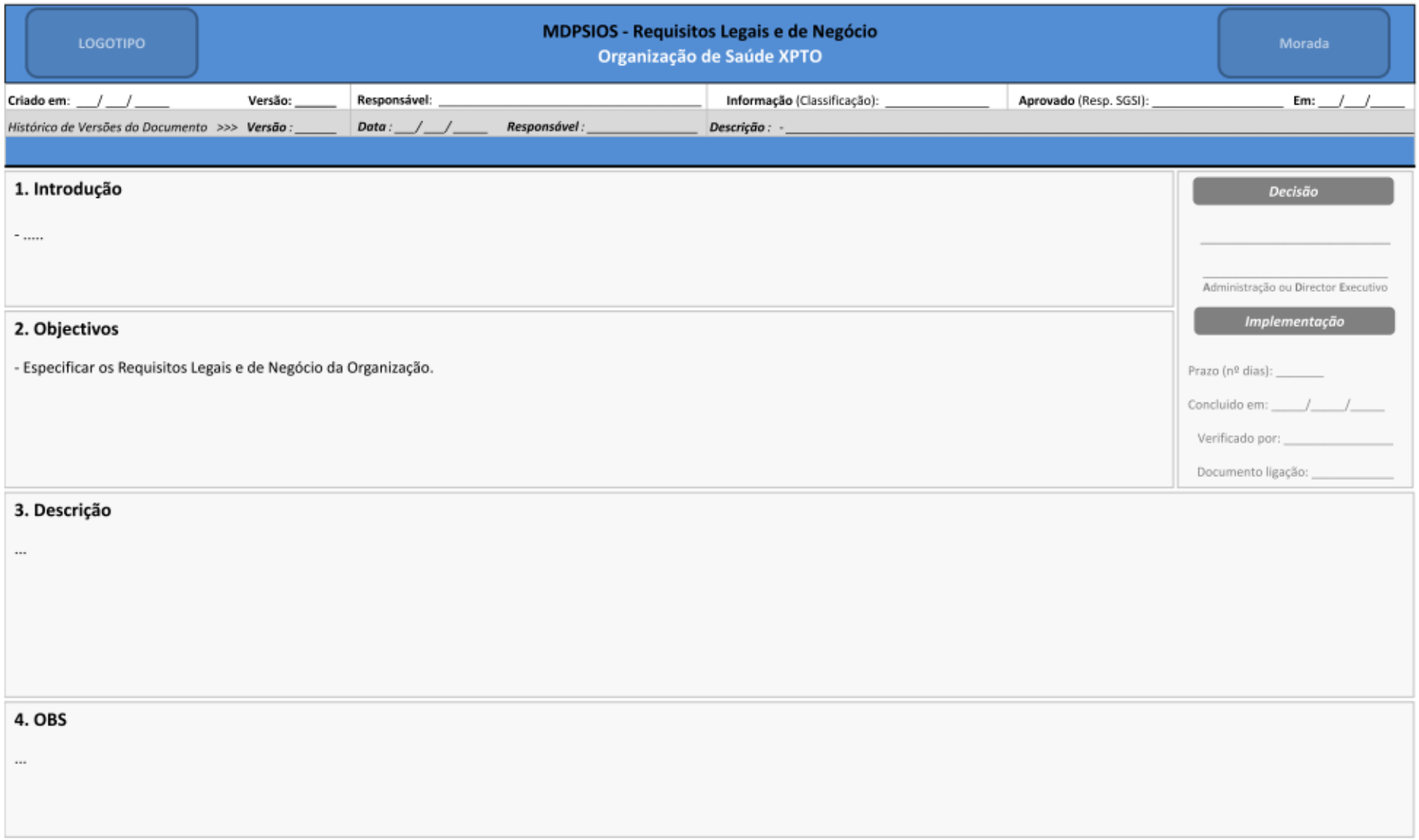


MDPSIOS [Pag. 1 de 1]

15. Estrutura e Etapas SGSI



16. Documento Requisitos Legais e de Negócio



LOGOTIPO

MDPSIOS - Requisitos Legais e de Negócio
Organização de Saúde XPTO

Morada

Criado em: ___/___/_____ **Versão:** _____ | **Responsável:** _____ | **Informação** (Classificação): _____ | **Aprovado** (Resp. SGSI): _____ **Em:** ___/___/_____

Histórico de Versões do Documento >>> ***Versão :*** _____ ***Data :*** ___/___/_____ ***Responsável :*** _____ ***Descrição :*** - _____

1. Introdução

- .....

2. Objectivos

- Especificar os Requisitos Legais e de Negócio da Organização.

Decisão

_____

_____
Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

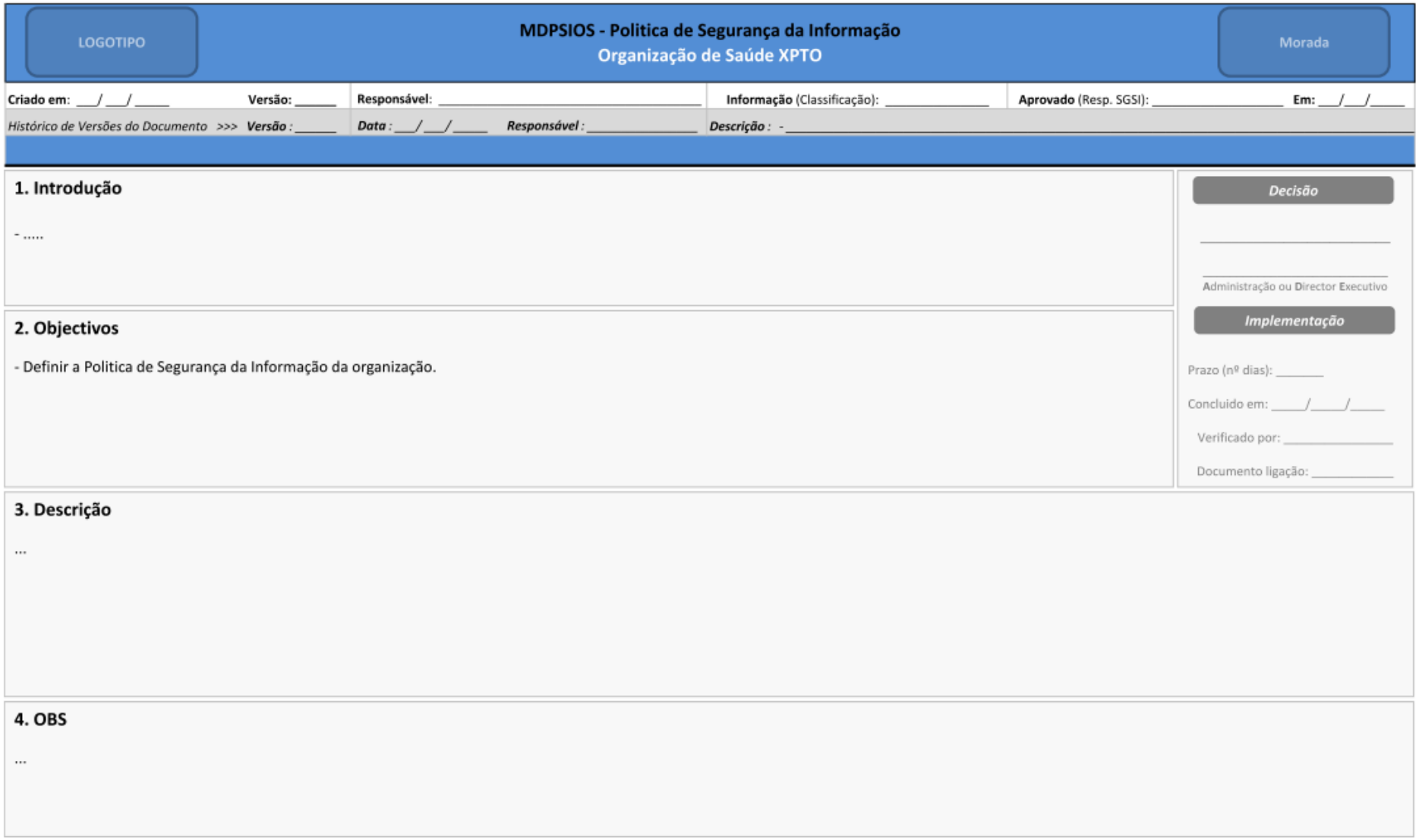
3. Descrição

...

4. OBS

...

17. Documento Politica da Segurança da Informação



LOGOTIPO

MDPSIOS - Politica de Segurança da Informação
Organização de Saúde XPTO

Morada

Criado em: ___/___/_____ **Versão:** _____ **Responsável:** _____ **Informação** (Classificação): _____ **Aprovado** (Resp. SGSI): _____ **Em:** ___/___/____

Histórico de Versões do Documento >>> ***Versão :*** _____ ***Data :*** ___/___/_____ ***Responsável :*** _____ ***Descrição :*** - _____

1. Introdução

- .....

2. Objectivos

- Definir a Politica de Segurança da Informação da organização.

Decisão

_____

_____
Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

3. Descrição

...

4. OBS

...

18. Documento Objectivos do SGSI

LOGOTIPO	**MDPSIOS - Objectivos do SGSI** **Organização de Saúde XPTO**	Morada

Criado em: ___/___/_____ **Versão:** _____	**Responsável:** _____	**Informação** (Classificação): _____	**Aprovado** (Resp. SGSI): _____ **Em:** ___/___/_____
Histórico de Versões do Documento >>> ***Versão :*** _____	***Data :*** ___/___/_____ ***Responsável :*** _____	***Descrição :*** - _____	

1. Introdução

- .....

2. Objectivos

- Definir os objectivos do SGSI na organização.

Decisão

_____

_____
Administração ou Director Executivo

Implementação

Prazo (nº dias): _____

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

3. Descrição

...

4. OBS

...

19. Formação e Sensibilização dos Funcionários e Colaboradores

LOGOTIPO	**MDPSIOS - Formação e Sensibilização dos Funcionarios e Colaboradores** **Organização de Saúde XPTO**	Morada

Criado em: 30 / 10 / 2012 **Versão: V.01**	**Responsável:** Francisco Carvalho	**Informação** (Classificação): Interna	**Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 30 / 10 / 2012
*Histórico de Versões do Documento >>> **Versão:** V.01*	***Data:** 30 / 10 / 2012 **Responsável:** Francisco Carvalho*	***Descrição:** - Aprovação do Documento*	

1. Introdução

- A formação e sensibilização dos funcionarios e colaboradores é um factor muito importante para o sucesso de qualquer SGSI.

2. Objectivos

- Definir formas e meios a utilizar para dar formação e promover a sensibilização dos funcionarios e colaboradores da organização.

Decisão

APROVADO

Luís Anibal
~~Administração ou~~ Director Executivo

Implementação

Prazo (nº dias): Imediata

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

3. Descrição

- Todos os funcionarios e colaboradores devem ser devidamente escalrecidos e formados sobre a importância da segurança da informação , independentemente da sua função ou cargo na organização.
- Devem-se encontrar as melhores soluções e formas de fazer chegar ou divulgar as informações sobre segurança a todos, se possivel recorrendo a apresentações, intranet, etc.
- As politicas de segurança adotadas, devem ser de conhecimento geram, assim a abertura paranovas sugestões e ideias que possam surgir por parte de qualquer funcionario.
- Deve-se sempre que necessário realizar novas acções de formação e ou sensibilização para todos ou por areas caso tal justifique.

4. OBS

...

20. Controlo de Documentos e Registos

LOGOTIPO	**MDPSIOS - Controlo de Documentos e Registos** **Organização de Saúde XPTO**	Morada

Criado em: 12 / 10 / 2012 **Versão: V.01**	**Responsável:** Francisco Carvalho	**Informação** (Classificação): Interna	**Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 12 / 10 / 2012
*Histórico de Versões do Documento >>> **Versão:** V.01*	***Data:** 12 / 10 / 2012 **Responsável:** Francisco Carvalho*	***Descrição:** - Aprovação do Documento*	

1. Introdução

O controlo de documentos e registos é um obrigatoriedade na implemetação de qualquer SGSI, para formaliza este ponto, foram elaborados durante a fase de planificação do projecto um conjunto de documentos que ajudam a implementar e manter este sistema.
O Conselho de Segurança da Informação decidiu sobre a criação de documentos obrigatorios por exigência da norma da ISO/IEC 27001, e outros por decisão e necessidade da organização.

Decisão

APROVADO

Luís Anibal
~~Administração ou~~ Director Executivo

Implementação

Prazo (nº dias): Imediata

Concluido em: _____/_____/_____

Verificado por: _____

Documento ligação: _____

2. Objectivos

Assegurar a criação e gestão de documentos e registos obrigatorios e necessários para implemetação e manutenção do SGSI.

3. Descrição

Fase de Planificação Ciclo PDCA	*Documentos a Criar*	*Status*
Criar Concelho de Segurança	*Concelho de Segurança da Informação*	Concluido
Definir Objectivos SGSI	*Objectivos SGSI*	Em Analise
Identificar e Inventariar Ativos	*Gestão de Ativos*	Em Analise
Definir responsabilidades		
Criar/Definir Politica de Segurança	*Gestão de Politicas Segurança*	Por Definir
	Segurança da Informação Regulamento Interno	Concluido
	Segurança da Informação Termo de Responsabilidade	Concluido
	Norma para Classificação da Informação	Por Definir
	Norma para Utilização dos Recursos de Informação/Datacenter	Por Definir
	(Outros a definir pela Organização se Necessário)	---
Analise e Avaliação do Risco	*Gestão de Risco*	Concluido
Definição dos Controlos a Aplicar		
Plano de Tratamento do Risco		
Definir Documento de Aplicabilidade	*Documento de Objectivos / Aplicabilidade*	Concluido

- Deve-se considerar as seguintes ações de gestão e controlo documental:

1. Os documentos devem ser aprovados antes da sua emissão ou publicação.

2. Os documentos devem ser anlisados de forma critica para sua atualização ou reprovação quando necessário.

3. Deve-se validar se as versões de documentos pertinentes estão disponiveis nos locais habituais e disponiveis a quem as deve consultar.

4. Sempre que existam alterações deve-se assegurar que estas estão devidamente identificadas.

5. Validar se os documentos continuam legiveis e faiclmente identificações.

6. Validar se a transferencia, arquivo e destruição de documentos segue os procedimentos definidos de acordo com sua classificação e controlo.

7. Assegurar a devida identificação e classificação de documentos de origem externa.

8. Prevenir e assegurar a não utilização de documentos obsoletos.

LOGOTIPO	MDPSIOS - Controlo de Documentos e Registos Organização de Saúde XPTO			Morada
Criado em: 12 / 10 / 2012 **Versão: V.01**	**Responsável:** Francisco Carvalho	**Informação** (Classificação): Interna	**Aprovado** (Resp. SGSI): Francisco Carvalho **Em:** 12 / 10 / 2012	
*Histórico de Versões do Documento >>> **Versão:** V.01*	***Data:** 12 / 10 / 2012 **Responsável:** Francisco Carvalho*	***Descrição:** - Aprovação do Documento*		

4. OBS

Anexo G – MPDSIOS – Domínios/Cláusulas norma ISO/IEC 27002

LOGOTIPO	MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27002) " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)		DOCUMENTO DE OBJECTIVOS (secções)
5. *(ISO 27002)* **Política de Segurança**	Descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.	ISO/IEC 27001:2005 ISO/IEC 27002:2005	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:		5.1 | 5.2
6. *(ISO 27002)* **Segurança Organizacional**	Descreve a estrutura de uma gestão para a segurança de informação, assim como o estabelecimento de responsabilidades, incluindo terceiros e fornecedores de serviços.	ISO/IEC 27001:2005 ISO/IEC 27002:2005	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:		6.1 | 6.2
7. *(ISO 27002)* **Classificação e Controlo de Activos de Informação**	Trabalha a classificação, o registro e o controlo dos activos da organização.	ISO/IEC 27001:2005 ISO/IEC 27002:2005	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:		7.1 | 7.2
8. *(ISO 27002)* **Segurança Relacionada Com as Pessoas**	Foca o risco decorrente de actos intencionais ou acidentais feitos por pessoas. Pode também abordar aspectos como a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e formação em assuntos relacionados com a segurança.	ISO/IEC 27001:2005 ISO/IEC 27002:2005	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:		8.1 | 8.2 | 8.3
9. *(ISO 27002)* **Segurança Física e Ambiental**	Descreve a necessidade de se definirem áreas de circulação restrita e a necessidade de proteger os equipamentos e a infra-estrutura de tecnologia de informação.	ISO/IEC 27001:2005 ISO/IEC 27002:2005	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade:		9.1 | 9.2

LOGOTIPO

MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27002)

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)		DOCUMENTO DE OBJECTIVOS (secções)
			Não Repúdio		
			Credibilidade:		
10. *(ISO 27002)* **Gestão das Operações e Comunicações**	Descreve as principais áreas que devem ser objecto de especial atenção da segurança. Entre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gestão de redes, controlo e prevenção de vírus, controlo de mudanças, execução e armazenamento de backups, controlo de documentação, segurança de correio electrónico, etc.	ISO/IEC 27001:2005	Confidencialidade:		10.1 | 10.2 | 10.3 | 10.4 10.5 | 10.6 | 10.7 | 10.8 10.9 | 10.10
			Integridade:		
		ISO/IEC 27002:2005	Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		
11. *(ISO 27002)* **Controlo de Acesso**	Regula o controlo de acessos aos sistemas, definição de competências, o sistema de monitorização de acesso e uso, a utilização de senhas,etc.	ISO/IEC 27001:2005	Confidencialidade:		11.1 | 11.2 | 11.3 | 11.4 11.5 | 11.6 | 11.7
			Integridade:		
		ISO/IEC 27002:2005	Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		
12. *(ISO 27002)* **Desenvolvimento e Manutenção de Sistemas**	Descreve os requisitos de segurança dos sistemas, controlos de criptografia, controlo de arquivos e segurança do desenvolvimento e suporte de sistemas.	ISO/IEC 27001:2005	Confidencialidade:		12.1 | 12.2 | 12.3 | 12.4 12.5 | 12.6
			Integridade:		
		ISO/IEC 27002:2005	Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		
13. *(ISO 27002)* **Gestão de Incidentes de Segurança**	Descreve a notificação de fragilidades e eventos de segurança da informação, bem como a gestão de incidentes de segurança da informação e melhorias.	ISO/IEC 27001:2005	Confidencialidade:		13.1 | 13.2
			Integridade:		
		ISO/IEC 27002:2005	Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		
		ISO/IEC 27001:2005	Confidencialidade:		

LOGOTIPO

MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27002)

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)		DOCUMENTO DE OBJECTIVOS (secções)
14. *(ISO 27002)* **Gestão da Continuidade do Negócio**	Descreve a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e actualizado.	ISO/IEC 27002:2005	Integridade:		14.1
			Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		
15. *(ISO 27002)* **Conformidade**	Descreve a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a protecção da informação de clientes/utentes.	ISO/IEC 27001:2005	Confidencialidade:		15.1 | 15.2 | 15.3
			Integridade:		
		ISO/IEC 27002:2005	Disponibilidade:		
			Responsabilidade/ Autoria:		
			Autenticidade:		
			Não Repúdio		
			Credibilidade:		

1. 5_Política de Segurança

LOGOTIPO	MDPSIOS - Documento de Objectivos de Controlo / Aplicabilidade " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **5.1 - Politica de Segurança**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
5.1	***Política de Segurança da Informação***	***Para proporcionar o apoio necessário a direcção e Administração relativamente a segurança da informação, em conformidade com os requisitos do negócio, as leis e regulamentos relevantes.***								
5.1.1	Documento da Política de Segurança da Informação	O documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado a todos os funcionários e colaboradores externas relevantes.	IMP			27001				Referência: SI-Regulamento Interno
5.1.2	Revisão da Política de Segurança da Informação	A política de segurança da informação deve ser revista em intervalos planificados, ou se ocorrerem mudanças significativas para garantir a sua continua eficiência, eficácia e adequação.	IEC			27002				Referência: Gestão de Politicas
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

2. 6_Organização da Segurança da Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Dominio: **6.1 - Organização da Segurança da Informação**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
6.1	***Organização Interna***	***Para gerir a segurança da informação dentro da organização.***								
6.1.1	Compromisso de Gestão (da organização) com a segurança da informação	A Administração deve apoiar activamente a segurança dentro da organização através de uma direcção clara, compromisso demonstrado, atribuição explícita e reconhecimento das responsabilidades de segurança da informação.	IMP			27001				Referência: Carta da Administração
6.1.2	Coordenação de segurança da informação	Actividades de segurança da informação devem ser coordenados por representantes de diferentes partes da organização, com papéis relevantes e funções de trabalho.	IMP			27001				Referência: Concelho de Segurança da Informação
6.1.3	Atribuição de Responsabilidades de segurança da informação	Todas as responsabilidades de segurança da informação devem ser claramente definidas.	IEC	Atribuição prevista no próximo ciclo PDCA						
6.1.4	Processo de autorização para instalações de Processamento de Informações	Um processo de autorização da gestão para novas instalações de processamento de informação devem ser definidas e implementadas.	N/A	Não faz parte do objectivo						
6.1.5	Contractos de confidencialidade	Requisitos para os acordos de confidencialidade ou de não-divulgação, que reflitam as necessidades da organização para a protecção das informações, devem ser identificados e revistos periodicamente.	N/A	Atribuição prevista no próximo ciclo PDCA						
6.1.6	Contacto com as autoridades	Contactos apropriados com autoridades relevantes devem ser mantidos.	N/A	Não faz parte do objectivo						
6.1.7	Contacto com grupos de interesse especiais	Contactos apropriados com grupos de interesses especiais ou outros forúns especialistas de segurança, e associações profissionais, devem ser mantidos.	N/A	Não faz parte do objectivo						
6.1.8	Revisão independente de segurança da informação	A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objectivos dos controlos, políticas, processos e procedimentos de segurança da informação) deve ser revista de forma independente em intervalos planeados, ou quando ocorrerem alterações significativas na implementação de segurança.	IMP			27001				Esta etapa ainda não contemplada pelo SGSI
6.2	***Terceiros***	***Para manter a segurança da informação da organização e das instalações de processamento de informação que são acedidos, processados, comunicados com, ou geridos por terceiros.***								
6.2.1	Identificação de riscos relacionados com terceiros	Os riscos da informação da organização e das instalações de processamento informação, decorrentes de processos de negócios envolvendo terceiros, deverão ser identificados e implementados controles apropriados antes de ser concedido acesso.	IMP				■			Referência: Documento de Analise/Avaliação da Entidade/Terceiro
6.2.2	Abordar a segurança ao lidar com clientes	Todos os requisitos de segurança identificados devem ser considerados antes de ser dado acesso aos clientes, às informações da organização ou activos.	IMP				■			Referência: Documento de Analise/Avaliação do Cliente

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **6.1 - Organização da Segurança da Informação**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
6.2.3	Abordar a segurança em contractos com terceiros	Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gestão de informação da organização ou de instalações de processamento de informação, ou a adição de produtos ou serviços às instalações de processamento de informação, deve cobrir todos os requisitos de segurança relevantes.	IMP		■					Referência: Si-Termo Responsabilidade
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

3. 7_Classificação e Controlo de Ativos de Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

*Histórico do Documento >>> **Versão:** _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____*

Dominio: **7.1 - Gestão de Activos / Recursos**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
7.1	***Responsabilidade por activos/recursos***	***Para alcançar e manter a proteção adequada dos ativos e recursos da organização.***								
7.1.1	Inventário de activos/recursos (património)	Todos os activos devem ser claramente identificados e deve ser elaborado e mantido um inventário de todos os activos importantes.								
7.1.2	Propriedade de activos/recursos	Todas as informações e activos associados às instalações de processamento de informação serão "detidas" por uma parte designada da organização.								
7.1.3	Uso aceitável de activos/recursos	Regras para o uso aceitável de informação e activos associados a instalações de processamento de informações devem ser identificadas, documentadas, e implementadas.								
7.2	***Classificação de informação***	***Para garantir que a informação recebe um nível adequado de protecção.***								
7.2.1	Directrizes de classificação	A informação deve ser classificada em função do seu valor, requisitos legais, sensibilidade e criticidade para a organização.								
7.2.2	Rotulagem e Tratamento de informação	Um conjunto apropriado de procedimentos para rotulagem e manipulação de informação devem ser desenvolvidos e implementados em conformidade com o esquema de classificação adoptado pela organização.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

4. 8_Segurança em Recursos Humanos

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **8.1 - Segurança em Recursos Humanos**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
8.1	***Antes da atribuição de Emprego***	***Para garantir que os funcionários, contratados e terceiros entendem as suas responsabilidades, e são adequadas para as funções para que são considerados, e para reduzir o risco de roubo, fraude ou uso indevido das instalações.***								
8.1.1	Funções e Responsabilidades	Funções de segurança e responsabilidades dos funcionários, contratados e terceiros devem ser definidas e documentadas de acordo com a política de segurança da informação da organização.								
8.1.2	Triagem	Verificações de controlo de antecedentes de todos os candidatos a emprego, contratados e terceiros devem ser realizadas em conformidade com as disposições legais, regulamentares e éticos, e proporcionais ao requisitos de negócio, à classificação da informação a ser acedida, e dos riscos percebidos.								
8.1.3	Termos e condições de emprego	Como parte da sua obrigação contratual, funcionários, contratados e terceiros devem concordar e assinar os termos e condições do seu contrato de trabalho, os quais deverão indicar as suas responsabilidades e as da organização, para a segurança da informação.								
8.2	***Durante Emprego***	***Para garantir que todos os funcionários, contratados e terceiros estão conscientes das ameaças e preocupações de segurança da informação, das suas responsabilidades e obrigações, e estão equipados para dar apoio à política de segurança organizacional no decurso do seu trabalho normal, e para reduzir o risco de erro humano.***								
8.2.1	Responsabilidade de Gestão	A Administração deve exigir dos funcionários, contratados e terceiros para aplicar a segurança em conformidade com as políticas estabelecidas e procedimentos da organização.								
8.2.2	Consencialização para segurança de informação, educação e formação	Todos os funcionários da organização e, eventualmente, contratados e terceiros, devem receber formação adequada e actualizações regulares das políticas e procedimentos organizacionais, como relevantes para a sua função.								
8.2.3	Processo disciplinar	Deve haver um processo disciplinar formal para empregados que tenham cometido uma violação de segurança.								
8.3	***Término ou mudança de emprego***	***Para garantir que os funcionários, contratados e terceiros saiam de uma organização ou mudam de emprego de uma forma ordenada.***								
8.3.1	Responsabilidade de término (rescisão)	Responsabilidades para realizar cessação de emprego ou alteração de posto de trabalho devem ser claramente definidas e atribuídas.								
8.3.2	Retorno de activos/recursos	Todos os funcionários, contratados e terceiros devem devolver todos os activos da organização em sua posse, ao término do seu emprego, contrato de trabalho, ou acordo.								

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **8.1 - Segurança em Recursos Humanos**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
8.3.3	Retirada de direitos de acesso	Os direitos de acesso de todos os funcionários, contratados e terceiros à informação e às instalações de processamento de informação, devem ser removidos ao término de seu emprego, contrato de trabalho, ou acordo, ou ajustado em caso de mudança.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR:** Exigência da Norma de Referência, **RN/MP:** Requisitos de Negócio / Melhores Práticas adoptadas, **RAR:** Resultados da Avaliação de Risco, **ACP:** Até Certo Ponto

5. 9_Segurança Física e Ambiental

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

*Histórico do Documento >>> **Versão:** _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____*

Dominio: **9.1 - Segurança Física e Ambiental**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
9.1	***Áreas Seguras***	***Para prevenir acesso físico não autorizado, danos e interferências com o recinto e informação da organização.***								
9.1.1	Perímetro físico de segurança	Perímetros de segurança (barreiras tais como paredes, portões de entrada com controlo de cartão ou balcões de recepção) devem ser utilizados para proteger as áreas que contenham informação e instalações de processamento de informação.	IMP	Controlos existentes		27001				
9.1.2	Controlos físicos de entrada	As áreas de segurança devem ser protegidas por controlos de entrada apropriados para garantir que somente pessoas autorizadas têm acesso.	IMP	Controlos existentes		27001	■	■		Implementar controlo de acesso por cartão magnetico em todos os centros de dados, e estabelecer registo de controlo de visitantes.
9.1.3	Segurança em escritórios, salas e instalações	Segurança física para escritórios, salas e instalações devem ser concebida e aplicada.	IMP	Controlos existentes				■		
9.1.4	Protecção contra ameaças externas e ambientais	Protecção física contra danos causados por incêndio, inundação, terramoto, explosão, distúrbios civis, e outras formas de catástrofes naturais ou provocadas pelo homem, devem ser concebidos e aplicados.	IMP	Controlos existentes						
9.1.5	Trabalhar em áreas seguras	Protecção física e orientações para trabalho em áreas seguras deve ser concebida e aplicada.	IMP	Controlos existentes			■			Politica criada
9.1.6	Acesso público, entregas e áreas de carga	Pontos de acesso, tais como áreas de entrega e zonas de carga, e outros pontos onde as pessoas não autorizadas podem entrar nas instalações devem ser controlados e, se possível, isoladas de instalações de processamento de informação, para evitar acesso não autorizado.	IMP	Controlos existentes						
9.2	***Segurança de equipamentos***	***Para evitar perdas, danos, furto ou comprometimento de activos, e interrupção das actividades da organização.***								
9.2.1	Localização e protecção de equipamento	Os equipamentos devem ser alojados ou protegidos para reduzir os riscos de ameaças e perigos ambientais, e oportunidades de acesso não autorizado.	IMP	Controlos existentes		27001		■		
9.2.2	Utilitários de apoio	Os equipamentos devem ser protegidos contra falhas de energia e outras interrupções causadas por falhas nos serviços de apoio.	IMP	Controlos existentes				■		
9.2.3	Segurança de cablagem	Cablagem de alimentações e de telecomunicações que transmitam dados ou de apoio a serviços de informação devem ser protegidos contra intercepção ou danos.	IMP	Controlos existentes		27001				
9.2.4	Manutenção de Equipamentos	Os equipamentos devem ser correctamente mantidos para assegurar sua continua disponibilidade e integridade.	IMP	Controlos existentes		27001	■	■		Mecanismo MP formalizado
9.2.5	Segurança de equipamentos fora das instações (da organização)	Segurança deve ser aplicada em equipamentos situados fora das instalações, tendo em conta os diferentes riscos de trabalhar fora das instalações da organização.	IMP	Controlos existentes						
9.2.6	Abate seguro ou reutilização de equipamentos	Todos os itens de equipamento que contenham media de armazenamento devem ser verificados para garantir todos os dados sensíveis e software licenciado foram apagados ou removidos de forma segura antes da eliminação.	N/A	Não faz parte do objectivo						
9.2.7	Remoção de Propriedade	Equipamento, informação ou software não devem ser levados das instalações sem autorização prévia.	IMP	Controlo existente.						Usar controlo de acessos.
...										
...										

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **9.1 - Segurança Física e Ambiental**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP**: Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

6. 10_Gestão de Comunicação e Operações

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

*Histórico do Documento >>> **Versão:** _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____*

Dominio: **10.1 - Gestão de Comunicações e Operações**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
10.1	***Procedimentos operacionais e responsabilidades***	Para garantir a operação segura e correcta das instalações de processamento de informação.								
10.1.1	Procedimentos operacionais documentados	Procedimentos operacionais devem ser documentados, mantidos, e disponibilizados para todos os utilizadores que deles precisam.								
10.1.2	Gestão de Mudança	Alterações às instalações e sistemas de processamento da informação devem ser controladas.								
10.1.3	Segregação de funções	Funções e áreas de responsabilidade devem ser segregadas para reduzir oportunidades de modificação não autorizada ou acidental, ou uso indevido dos bens da organização.								
10.1.4	Separação de instalações de Desenvolvimento e Operações	Instalações de desenvolvimento, teste e produção devem ser separadas para reduzir os riscos de acesso não autorizado ou alterações no sistema operacional.								
10.2	***Gestão de Prestação de Serviços por Terceiros***	Para implementar e manter o nível adequado de segurança da informação, e prestação de serviços em consonância com o acordo de prestação de serviços por terceiros.								
10.2.1	Prestação de Serviços	Deve ser garantido que os controlos de segurança, definições de serviços e níveis de prestação incluídos no acordo de prestação de serviços por terceiros são implementados, operados e mantidos pelos terceiros.								
10.2.2	Acompanhamento e revisão de serviços de terceiros	Os serviços, relatórios e registos fornecidos pelos terceiros deverão ser regularmente monitorizados e analisados, e devem ser realizadas auditorias regularmente.								
10.2.3	Gestão de mudanças nos serviços de terceiros	Alterações à prestação de serviços, incluindo manutenção e melhoramento de políticas, procedimentos e controlos de segurança da informação existentes, devem ser geridos, tendo em conta a criticidade dos sistemas e processos de negócio envolvidos, e reavaliação dos riscos.								
10.3	***Planeamento de Sistema e Aceitação***	Para minimizar o risco de falhas nos sistemas.								
10.3.1	Gestão de capacidade	A utilização de recursos deve ser monitorizada, sincronizada, e as projecções de requisitos de capacidade futura devem ser feitas para garantir o necessário desempenho do sistema.								
10.3.2	Aceitação do sistema	Critérios de aceitação para novos sistemas de informação, upgrades e novas versões devem ser estabelecidos, e testes apropriados do sistema(s) devem ser realizados durante o desenvolvimento e antes da aceitação.								
10.4	***Proteção contra código malicioso e móvel***	Para proteger a integridade do software e informação.								
10.4.1	Controlo contra código malicioso	Controlos de detecção, prevenção, recuperação para proteger contra código malicioso, e procedimentos adequados de conscienlização do utilizador devem ser implementados.								
10.4.2	Controlo contra código móvel	Quando o uso de código móvel é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança claramente definida, e código móvel não autorizado deve ser impedido de ser executado.								
10.5	***Backup***	Para manter a integridade e disponibilidade da informação e das instalações de processamento da informação.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **10.1 - Gestão de Comunicações e Operações**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
10.5.1	Backup de informação	Cópias de segurança da informação e de software devem ser retiradas e testadas regularmente de acordo com a política de backup acordada.								
10.6	***Gestão da Segurança de Rede***	Para garantir a protecção da informação em rede, e a protecção da infra-estrutura de apoio.								
10.6.1	Controlos de rede	Redes devem ser adequadamente geridas e controladas, a fim de serem protegidas contra ameaças, e para manter a segurança para os sistemas e aplicações que usam a rede, incluindo a informação em trânsito.								
10.6.2	Segurança dos serviços de rede	Os recursos de segurança, níveis de serviço e requisitos de gestão de todos os serviços de rede devem ser identificados e incluídos em qualquer contracto de serviços de rede, quer esses serviços sejam prestados internamente ou por terceiros.								
10.7	***Manuseamento de Media***	Para evitar a divulgação, modificação, remoção ou destruição de bens não autorizada, e interrupção de actividades empresariais.								
10.7.1	Gestão de media amovível	Devem existir procedimentos em execução para a gestão de media removível.								
10.7.2	Eliminação de media	Media deve ser eliminada de maneira segura e cuidadosa quando deixar de ser necessária, através de procedimentos formais.								
10.7.3	Procedimentos de manuseamento de informação	Procedimentos para o manuseamento e armazenamento de informação devem ser estabelecidos para proteger essa informação contra divulgação não autorizada ou uso indevido.								
10.7.4	Segurança da documentação do sistema	Documentação do sistema deve ser protegida contra acesso não autorizado.								
10.8	***Troca de Informação***	Para manter a segurança da informação e software trocados dentro de uma organização e com qualquer entidade externa.								
10.8.1	Políticas e procedimentos de troca de informação	Políticas, procedimentos e controlos de trocas formais devem estar disponíveis para proteger a troca de informação através da utilização de todos os tipos de meios de comunicação.								
10.8.2	Acordos de troca	Devem ser estabelecidos acordos de troca de informação e software entre a organização e entidades externas.								
10.8.3	Media física em trânsito	Media contendo informação deve ser protegida contra acesso não autorizado, uso indevido ou corrupção durante o transporte para além dos limites físicos da organização.								
10.8.4	Mensagens electrónicas	Informação envolvida em mensagens eletrónicas deve ser adequadamente protegida.								
10.8.5	Sistemas de Informação Empresariais	Políticas e procedimentos devem ser desenvolvidos e implementados para proteger a informação associada à interligação dos sistemas de informação do negócio.								
10.9	***Serviços de Comércio Eletrónico***	Para garantir a segurança dos serviços de comércio electrónico, e a sua utilização segura.								
10.9.1	Comércio Electrónico	Informação envolvida em comércio electrónico em redes públicas deve ser protegida contra actividades fraudulentas, disputas contractuais, e divulgação não autorizada e modificações.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **10.1 - Gestão de Comunicações e Operações**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
10.9.2	Transacções On-Line	Informação envolvida em transações on-line deve ser protegida para prevenir transmissão incompleta, erro de rota, alteração não autorizada da mensagem, divulgação não autorizada, duplicação não autorizada da mensagem ou repetição.								
10.9.3	Informação disponível ao público	A integridade da informação disponibilizada ao público num sistema de acesso livre deve ser protegida para impedir a modificação não autorizada.								
10.1	***Monitorização***	Para detectar actividades não autorizadas de processamento de informação.								
10.10.1	Registo de auditoria	Relatórios de auditoria que registem actividades do utilizador, excepções e eventos de segurança da informação devem ser produzidos e mantidos por um período acordado, para auxiliar em futuras investigações e monitorização de controlo de acesso.								
10.10.2	Monitorização do uso do sistema	Procedimentos de monitorização da utilização de instalações de processamento de informação deve ser estabelecida, e os resultados de monitorização das actividades devem ser revistos regularmente.								
10.10.3	Protecção de informação de registo	Instalações de registo e informações de acesso devem ser protegidas contra adulteração e acesso não autorizado.								
10.10.4	Registo de administrador e operador	Actividades do administrador do sistema e do operador do sistema devem ser registadas.								
10.10.5	Registo de falhas	Falhas devem ser registadas, analisadas e tomadas as medidas adequadas.								
10.10.6	Sincronização dos relógios	Os relógios de todos os sistemas de processamento de informação relevantes dentro de uma organização ou domínio de segurança devem ser sincronizados com uma fonte precisa de tempo definida.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

7. 11_Controlo de Acessos

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

*Histórico do Documento >>> **Versão:** _____ Data: ___/___/___ Responsável: _____ Descrição da Atualização: _____*

Dominio: **11.1 - Controlo de Acessos** (ao sistema informático)

ISO 27002:20058 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
11.1	***Requisitos de Negócio para Controlo de Acesso***	***Para controlar o acesso à informação.***								
11.1.1	Política de controlo de acesso	Uma política de controlo de acesso deve ser estabelecida, documentada e analisada, tendo por base os requisitos de acesso do negócio e da segurança.								
11.2	***Gestão de Acesso de Utilizadores***	***Para assegurar acesso de utilizador autorizado e prevenir acesso não autorizado a sistemas de informação.***								
11.2.1	Registo de Utilizadores	Deve existir um procedimento formal de registo e cancelamento de utilizador para garantir e revogar acessos a todos os sistemas de informação e serviços.								
11.2.2	Avaliação de Privilégios	A concessão e o uso de privilégios deve ser restrita e controlada.								
11.2.3	Gestão de passwords de utilizadores	A concessão de passwords deve ser controlada através de um processo formal de gestão.								
11.2.4	Revisão de direitos de acesso de utilizadores	A gestão deve rever os direitos de acesso dos utilizadores em intervalos regulares de tempo, através de um processo formal								
11.3	***Responsabilidade dos Utilizadores***	***Para prevenir o acesso não autorizado dos utilizadores, e evitar o comprometimento ou roubo de informação e das instalações de processamento de informação.***								
11.3.1	Uso de password	Os utilizadores devem ser orientados a seguir boas práticas de segurança na selecção e uso de passwords.								
11.3.2	Equipamento de utilizador disponível sem monitorização	Os utilizadores devem assegurar que os equipamentos não monitorizados tenham protecção adequada.								
11.3.3	Política de Secretária livre e Ecran livre	Deve ser adoptada uma política de secretária limpa de papéis e de medias de armazenamento removíveis, e uma política de ecran limpo, para as instalações de processamento de informação.								
11.4	***Controlo de acesso à rede***	***Para prevenir acesso não autorizado aos serviços de rede.***								
11.4.1	Política de uso de serviços de rede	Os utilizadores devem receber acesso apenas aos serviços a que tenham sido especificamente autorizados a usar.								
11.4.2	Autenticação de utilizador para ligações externas	Métodos apropriados de autenticação devem ser usados para controlar o acesso de utilizadores remotos.								
11.4.3	Identificação de equipamentos na rede	Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.								
11.4.4	Diagnóstico remoto e proteção de configuração de porta	Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.								
11.4.5	Segregação em redes	Grupos de serviços de informação, utilizadores e sistemas de informação devem ser segregados em redes.								
11.4.6	Controlo de ligações na rede	Para redes partilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de utilizadores se ligarem à rede deve ser restringida, de acordo com a política de controlo de acesso e os requisitos das aplicações do negócio (ver 11.1).								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Dominio: **11.1 - Controlo de Acessos** (ao sistema informático)

ISO 27002:20058 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
11.4.7	Controlo de routing na rede	Deve ser implementado controlo de roteamento na rede para assegurar que as ligações de computador e fluxos de informação não violem a política de controlo de acesso das aplicações do negócio.								
11.5	***Controlo de acesso ao Sistema Operativo***	***Para prevenir acesso não autorizado aos sistemas operativos.***								
11.5.1	Procedimentos de Log-on seguro	O acesso aos sistemas operativos deve ser controlado por um procedimento seguro de entrada no sistema (log-on).								
11.5.2	Identificação e autenticação de utilizador	Todos os utilizadores devem ter um identificador único (ID de utilizador) para o seu uso pessoal e exclusivo, e deve ser escolhida uma técnica adequada de autenticação para validar a identidade alegada por um utilizador.								
11.5.3	Sistema de Gestão de Passwords	Sistemas para gestão de passwords devem ser interactivos e devem assegurar senhas de qualidade.								
11.5.4	Uso de utilidades do sistema	O uso de programas utilitários que possam ser capazes de sobrepor os controlos dos sistemas e aplicações deve ser restrito e estritamente controlado.								
11.5.5	Time-out de sessão	Sessões inactivas devem ser terminadas após um período definido de inactividade.								
11.5.6	Limitação do tempo de ligação	Restrições nos tempos de ligação devem ser utilizadas para proporcionar segurança adicional para aplicações de alto risco.								
11.6	***Controlo de acesso a Aplicações***	***Para prevenir acesso não autorizado a informação contida nos sistemas de aplicações.***								
11.6.1	Restrição de acesso a informação	O acesso a informação e funções dos sistemas de aplicações por utilizadores e pessoal do suporte deve ser restringido de acordo com a política de controlo de acesso definida.								
11.6.2	Isolamento de sistemas sensíveis	Sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).								
11.7	***Computação móvel e trabalho remoto***	***Para garantir a segurança da informação quando se utiliza computação móvel e recursos de trabalho remoto.***								
11.7.1	Computação móvel e comunicação	Uma política formal deve ser estabelecida, e medidas de segurança apropriadas devem ser adotadas para a protecção contra os riscos do uso de recursos de computação e comunicação móveis.								
11.7.2	Trabalho remoto	Uma política, planos operacionais e procedimentos devem ser desenvolvidos e implementados para actividades de trabalho remoto.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para seleção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

8. 12_Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ___/___/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ___/___/___ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **12.1 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
12.1	***Requisitos de Segurança de Sistemas de Informação***	***Para garantir que segurança é parte integrante dos sistemas de informação.***								
12.1.1	Análise e especificações de requisitos de segurança	Devem ser especificados os requisitos para controlo de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.								
12.2	***Processamento correcto em Aplicações***	***Para prevenir a ocorrência de erros, perdas, modificação não autorizada ou uso indevido de informação em aplicações.***								
12.2.1	Validação de dados de entrada	Os dados de entrada de aplicações devem ser validados para garantir que são correctos e apropriados.								
12.2.2	Controlo de processamento interno	Devem ser incorporadas nas aplicações verificações de validação para detectar qualquer corrupção de informação, por erros de processamento ou por actos deliberados.								
12.2.3	Integridade da mensagem	Requisitos para garantir a autenticidade e proteger a integridade da mensagem em aplicações devem ser identificados, e os controlos apropriados devem ser identificados e implementados.								
12.2.4	Validação de dados de saída	Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas é correcto e apropriado às circunstâncias.								
12.3	***Controlos de criptografia***	***Para proteger a confidencialidade, autenticidade ou integridade da informação por meios criptográficos.***								
12.3.1	Política sobre o uso de controlos criptográficos	Deve ser desenvolvida e implementada uma política sobre o uso de controlos criptográficos para protecção da informação.								
12.3.2	Gestão de chaves	Um processo de gestão de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.								
12.4	***Segurança dos arquivos de sistema***	***Para garantir a segurança de ficheiros de sistema.***								
12.4.1	Controlo de software Operacional	Devem existir procedimentos para controlar a instalação de software em sistemas operacionais.								
12.4.2	Protecção de dados de teste do sistema	Os dados de teste devem ser seleccionados com cuidado, e protegidos e controlados.								
12.4.3	Controlo de acessos ao código-fonte dos programas	O acesso ao código-fonte dos programas deve ser restrito.								
12.5	***Segurança nos processos de Desenvolvimento e Suporte***	***Para manter a segurança do software de sistemas de aplicações e informação.***								
12.5.1	Mudança do controlo de processos	A implementação de mudanças deve ser controlada utilizando procedimentos formais de controlo de mudanças.								
12.5.2	Revisão técnica de aplicações após mudanças no Sistema Operativo	Aplicações críticas do negócio devem ser analisadas e testadas quando os sistemas operativos são mudados, para garantir que não há qualquer impacto adverso na operação ou segurança da organização.								
12.5.3	Restrições para alterações em pacotes de software	Modificações a pacotes de software não devem ser incentivadas, devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **12.1 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
12.5.4	Fugas de informação	Devem ser prevenidas oportunidades para fugas de informações.								
12.5.5	Desenvolvimento de software por terceiros	A organização deve supervisionar e monitorizar o desenvolvimento de software por terceiros.								
12.6	***Gestão de Vulnerabilidades Técnicas***	***Para reduzir os riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.***								
12.6.1	Controlo de vulnerabilidades técnicas	Deve ser obtida informação em tempo útil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a essas vulnerabilidades, e devem ser tomadas as medidas apropriadas para lidar com os riscos associados.								
	...									
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para seleção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

9. 13_Gestão de Incidentes de Segurança da Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **13.1 - Gestão de Incidentes de Segurança da Informação**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
13.1	***Notificação de Eventos e Fraquezas de Segurança da Informação***	***Para asssegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados de maneira a permitir a tomada de acção correctiva em tempo útil.***								
13.1.1	Notificação de eventos de segurança da Informação	Eventos de segurança da informação devem ser comunicados o mais cedo possível, através canais de gestão apropriados.								
13.1.2	Notificação de fraquezas de segurança	Todos os funcionários, contratados e terceiros, que utilizem sistemas de informação e serviços, serão obrigados a anotar e reportar quaisquer falhas de segurança, observadas ou suspeitas , nos sistemas ou serviços.								
13.2	***Gestão de Incidentes de Segurança da Informação e Melhorias***	***Para garantir que uma abordagem consistente e efectiva seja aplicada à gestão de incidentes de segurança da informação.***								
13.2.1	Responsabilidades e procedimentos	Devem ser estabelecidas responsabilidades e procedimentos de gestão, para garantir uma resposta rápida, eficaz e ordenada sobre incidentes de segurança da informação.								
13.2.2	Aprendizagem por incidentes de segurança da Informação	Deverá haver mecanismos para permitir que o tipo, quantidade, e custo dos incidentes de segurança da informação possam ser quantificados e monitorizados.								
13.2.3	Recolha de provas	No seguimento de uma acção contra uma pessoa ou organização após um incidente de segurança da informação que involva acção legal (quer civil ou criminal), as provas devem ser recolhidas, mantidas e apresentadas em conformidade com as regras para provas, definidas na jurisdição relevante.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR:** Exigência da Norma de Referência, **RN/MP:** Requisitos de Negócio / Melhores Práticas adoptadas, **RAR:** Resultados da Avaliação de Risco, **ACP:** Até Certo Ponto

10.14_Gestão Continuidade do Negócio

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **14.1 - Gestão da Continuidade do Negócio**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
14.1	***Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio***	***Para contrariar interrupções a actividades do negócio e para proteger os processos críticos do negócio contra efeitos de falhas graves de sistemas de informação ou desastres, e assegurar o seu recomeço em tempo útil.***								
14.1.1	Incluir a Segurança da Informação no processo de gestão da continuidade do Negócio	Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.								
14.1.2	Continuidade do Negócio e Avaliação de Risco	Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto com a probabilidade e impacto de tais interrupções e as suas conseqüências para a segurança da informação.								
14.1.3	Desenvolvimento e implementação de planos de continuidade incluindo segurança da informação	Devem ser desenvolvidos e implementados planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.								
14.1.4	Quadro de planeamento de continuidade de Negócio	Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação, e para identificar prioridades para testes e manutenção.								
14.1.5	Testar, manter e re-avaliar os planos de continuidade do Negócio	Os planos de continuidade do negócio devem ser testados e actualizados regularmente, de forma a assegurar sua permanente actualização e efectividade.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR:** Exigência da Norma de Referência, **RN/MP:** Requisitos de Negócio / Melhores Práticas adoptadas, **RAR:** Resultados da Avaliação de Risco, **ACP:** Até Certo Ponto

11.15_Conformidade

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ___/___/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ___/___/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ___/___/___ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **15.1 - Conformidade**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
15.1	***Conformidade com Requisitos Legais***	***Para evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de qualsquer requisitos de segurança da informação.***								
15.1.1	Identificação de legislação aplicável	Todos os requisitos estatutários, regulamentares e contractuais relevantes e a abordagem da organização para atender a estes requisitos devem ser explicitamente definidos, documentados e mantidos actualizados para cada sistema de informação e para a organização.								
15.1.2	Direitos de Propriedade Intelectual (DPI)	Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contractuais no uso de material, em relação ao qual pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.								
15.1.3	Protecção de registos organizacionais	Registos importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.								
15.1.4	Protecção de Dados e privacidade de informações pessoais	A privacidade e protecção de dados devem ser asseguradas conforme o exigido nas legislações relevantes, regulamentações, e, se aplicável, nas cláusulas contratuais.								
15.1.5	Prevenção do mau uso das instalações de processamento de informação	Os utilizadores devem ser dissuadidos de usar as instalações de processamento de informação para propósitos não autorizados.								
15.1.6	Regulamentação de controlos criptográficos	Controlos de criptografia devem ser usados em conformidade com todas as leis, acordos e regulamentações relevantes.								
15.2	***Conformidade com Políticas e Normas de Segurança, e conformidade Técnica***	***Para garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança.***								
15.2.1	Conformidade com a política de segurança	Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados correctamente para garantir a conformidade com as normas e políticas de segurança.								
15.2.2	Verificação de conformidade técnica	Os sistemas de informação devem ser periodicamente verificados relativamente à sua conformidade com as normas de implementação de segurança.								
15.3	***Considerações de Auditoria do Sistema de Informação***	***Para maximizar a eficácia de, e minimizar a interferência para/de, o processo de auditoria dos sistemas de informação.***								
15.3.1	Controlos de Auditoria do Sistema de Informação	Os requisitos e actividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planeados e acordados para minimizar os riscos de interrupção dos processos do negócio.								
15.3.2	Protecção das ferramentas de auditoria de sistemas de informação	O acesso às ferramentas de auditoria do sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.								
...										
...										

Legenda

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **15.1 - Conformidade**

ISO 27002:2005 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR:** Exigência da Norma de Referência, **RN/MP:** Requisitos de Negócio / Melhores Práticas adoptadas, **RAR:** Resultados da Avaliação de Risco, **ACP:** Até Certo Ponto

Anexo H – MPDSIOS – Domínios/Cláusulas norma ISO/IEC 27799

LOGOTIPO

MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27799)

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)	DOCUMENTO DE OBJECTIVOS (secções)
7.2 *(ISO 27799)* **Politica de Segurança**	Descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.	ISO/IEC 27001:2005 / ISO/IEC 27799:2008	Confidencialidade: / Integridade: / Disponibilidade: / Responsabilidade/ Autoria: / Autenticidade: / Não Repúdio / Credibilidade:	7.2.1 | 7.2.2
7.3 *(ISO 27799)* **Segurança Organizacional**	Descreve a estrutura de uma gestão para a segurança de informação, assim como o estabelecimento de responsabilidades, incluindo terceiros e fornecedores de serviços.	ISO/IEC 27001:2005 / ISO/IEC 27799:2008	Confidencialidade: / Integridade: / Disponibilidade: / Responsabilidade/ Autoria: / Autenticidade: / Não Repúdio / Credibilidade:	7.3.1 | 7.3.2 | 7.3.3
7.4 *(ISO 27799)* **Classificação e Controlo de Activos de Informação**	Trabalha a classificação, o registro e o controlo dos activos da organização.	ISO/IEC 27001:2005 / ISO/IEC 27799:2008	Confidencialidade: / Integridade: / Disponibilidade: / Responsabilidade/ Autoria: / Autenticidade: / Não Repúdio / Credibilidade:	7.4.1 | 7.4.2
7.5 *(ISO 27799)* **Segurança Relacionada Com as Pessoas**	Foca o risco decorrente de actos intencionais ou acidentais feitos por pessoas. Pode também abordar aspectos como a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e formação em assuntos relacionados com a segurança.	ISO/IEC 27001:2005 / ISO/IEC 27799:2008	Confidencialidade: / Integridade: / Disponibilidade: / Responsabilidade/ Autoria: / Autenticidade: / Não Repúdio / Credibilidade:	7.5.1 | 7.5.2 | 7.5.3
7.6 *(ISO 27799)* **Segurança Física e Ambiental**	Descreve a necessidade de se definirem áreas de circulação restrita e a necessidade de proteger os equipamentos e a infra-estrutura de tecnologia de informação.	ISO/IEC 27001:2005 / ISO/IEC 27799:2008	Confidencialidade: / Integridade: / Disponibilidade: / Responsabilidade/ Autoria: / Autenticidade: / Não Repúdio / Credibilidade:	7.6.1 | 7.6.2

MDPSIOS [Pag. 1 de 3]

LOGOTIPO

MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27799)

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)	DOCUMENTO DE OBJECTIVOS (secções)
7.7 *(ISO 27799)* **Gestão das Operações e Comunicações**	Descreve as principais áreas que devem ser objecto de especial atenção da segurança. Entre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gestão de redes, controlo e prevenção de vírus, controlo de mudanças, execução e armazenamento de backups, controlo de documentação, segurança de correio electrónico, etc.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:	7.7.1 | 7.7.2 | 7.7.3 | 7.7.4 7.7.5 | 7.7.6 | 7.7.7 |7.7.8 7.7.9 | 7.7.10
7.8 *(ISO 27799)* **Controlo de Acesso**	Regula o controlo de acessos aos sistemas, definição de competências, o sistema de monitorização de acesso e uso, a utilização de senhas,etc.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:	7.8.1 | 7.8.2 | 7.8.3 | 7.8.4 7.8.5 | 7.8.6
7.9 *(ISO 27799)* **Desenvolvimento e Manutenção de Sistemas**	Descreve os requisitos de segurança dos sistemas, controlos de criptografia, controlo de arquivos e segurança do desenvolvimento e suporte de sistemas.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:	7.9.1 | 7.9.2 | 7.9.3 | 7.9.4 7.9.5
7.10 *(ISO 27799)* **Gestão de Incidentes de Segurança**	Descreve a notificação de fragilidades e eventos de segurança da informação, bem como a gestão de incidentes de segurança da informação e melhorias.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:	7.10.1 | 7.10.2
7.11 *(ISO 27799)* **Gestão da Continuidade do Negócio**	Descreve a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e actualizado.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:	7.11.1 (adoptado na intrega o objectivo "14." da ISO 27002)

LOGOTIPO	MDPSIOS - Dominios / Modelo / Dimensões / Objectivos (ISO 27799) " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ Descrição da Atualização: _____

DOMINIOS DA POLITICA DE SEGURANÇA	FINALIDADE / OBJECTIVO	NORMA A IMPLEMENTAR	DIMENSÕES A APLICAR (Sim/Não)		DOCUMENTO DE OBJECTIVOS (secções)
7.12 *(ISO 27002)* **Conformidade**	Descreve a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a protecção da informação de clientes/utentes.	ISO/IEC 27001:2005 ISO/IEC 27799:2008	Confidencialidade: Integridade: Disponibilidade: Responsabilidade/ Autoria: Autenticidade: Não Repúdio Credibilidade:		7.12.1 | 7.12.2 | 7.12.3 7.12.4

1. 7.2_Política de Segurança

LOGOTIPO

MDPSIOS - Documento de Objectivos de Controlo / Aplicabilidade (ISO 27799)
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.2 - Politica de Segurança**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.2	***Política de Segurança da Informação***	***Para proporcionar o apoio necessário a direcção e Administração relativamente a segurança da informação, em conformidade com os requisitos do negócio, as leis e regulamentos relevantes.***								
		Documento da Política de Segurança da Informação. Toda a organização que processa informação de saúde, incluindo informações pessoais de saúde, deve ter escrito um documento da política de segurança da informação aprovado pela direção, publicado e comunicado a todos os funcionários e colaboradores externos relevantes. *A aplicação deste controle de segurança é obrigatório em saúde.*	IMP			27001				Referência: SI-Regulamento Interno
		Revisão da Política de Segurança da Informação. A política de segurança da informação de uma organização de saúde deve ser revista em intervalos planificados (pelo menos anualmente), ou se ocorrer um incidente de segurança grave ou mudanças significativas para garantir a sua continua eficiência, eficácia e adequação.	IEC			27799				Referência: Gestão de Politicas
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

2. 7.3_Organização da Segurança da Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade (ISO 27799)
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> **Versão:** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Domínio: **7.3 - Organização da Segurança da Informação**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.3.1	***Organização da Segurança da Informação***	***A gestão de uma organização de saúde é responsável pela segurança de informações pessoais de saúde e da proteção de outros dados processados pela organização relacionados com à saúde. Isto é especialmente digno de nota para as organizações que dependem de serviços geridos ou fornecidos por terceiros. Coordenação eficaz é também é uma exigência essencial para a manutenção da segurança da informação. Esta situações exigem um segurança da infra-estrutura de gestão da informação explícita e robusta.***								
7.3.2	***Organização Interna***	***Para gerir a segurança da informação dentro da organização.***								
7.3.2.1	Compromisso de Gestão (da organização) com a segurança da informação. Coordenação de segurança da informação. Atribuição de Responsabilidades de segurança da informação.	A Administração da organização que processo infromações pessoais de saúde, deve apoiar activamente a segurança dentro da organização através de uma direcção clara. Actividades de segurança da informação devem ser coordenados por representantes de diferentes partes da organização, com papéis relevantes em funções de trabalho. Deve ter no mínimo uma pessoa dentro da organização responsável pela segurança de informação. A declaração de objectivos deve definir formalmente o limite de atividade de conformidade em termos de pessoas, processos, lugares, plataformas e aplicações.	IMP			27001				Referência: Carta da Administração
7.3.2.2	Processo de autorização para instalações de Processamento de Informações.	Um processo de autorização da gestão para novas instalações de processamento de informação devem ser definidas e implementadas.	N/A	Não faz parte do objectivo						
7.3.2.3	Contractos de confidencialidade.	Requisitos para os acordos de confidencialidade ou de não-divulgação, que reflitam as necessidades da organização para a protecção das informações, devem ser identificados e revistos periodicamente. Além da orientação dada pela ISO / IEC 27002, as organizações de saúde devem ter um contrato de confidencialidade que especifica a natureza confidencial do informação. O acordo deve ser aplicável a todas as pessoas que acedam as informações de saúde.	N/A	Atribuição prevista no próximo ciclo PDCA						
7.3.2.4	Contacto com as autoridades e grupos de interesse especiais. Revisão independente de segurança da informação.	Contactos apropriados com autoridades relevantes devem ser mantidos. Contactos apropriados com grupos de interesses especiais ou outros forúns especialistas de segurança, e associações profissionais, devem ser mantidos. A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objectivos dos controlos, políticas, processos e procedimentos de segurança da informação) deve ser revista de forma independente em intervalos planeados, ou quando ocorrerem alterações significativas na implementação de segurança.	N/A	Não faz parte do objectivo						

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** (ISO 27799) " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.3 - Organização da Segurança da Informação**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações)
					RL	ENR	RN/MP	RAR	ACP	Documento AAM
Secção	**Objectivo**	**Controlo / Descrição**								
7.3.3	***Terceiros***	***Para manter a segurança da informação da organização e das instalações de processamento de informação que são acedidos, processados, comunicados com, ou geridos por terceiros.***								
7.3.3.1	Identificação de riscos relacionados com terceiros.	Os riscos da informação e das instalações de processamento informação da organização de saúde, decorrentes de processos de negócios envolvendo terceiros, deverão ser identificados e implementados controles apropriados antes de ser concedido acesso, assim como para a identificação de riscos e das tecnologias utilizadas.	IMP				■			Referência: Documento de Analise/Avaliação da Entidade/Terceiro
7.3.3.2	Abordar a segurança ao lidar com clientes.	Todos os requisitos de segurança identificados devem ser considerados antes de ser dado acesso aos clientes, às informações da organização ou activos.	IMP				■			Referência: Documento de Analise/Avaliação do Cliente
7.3.3.3	Abordar a segurança em contractos com terceiros.	As organizações de saúde que utilizam os serviços de terceiros, para processamento de inofrmção pessoal de saúde, deve ter contratos formais que especificam: a) A natureza confidencial e valor da informação pessoal de saúde; b) As medidas de segurança a serem implementadas e / ou cumpridas; c) Limitações ao acesso a estes serviços por terceiros; d) Os níveis de serviço a serem alcançados nos serviços prestados; e) O formato e a frequência dos relatórios para o Concelho segurança da informação da organização de saúde; f) A forma de representação do terceiro em reuniões adequadas da organização saúde e ou grupos de trabalha desta; g) As modalidades de auditoria de conformidade de terceiros; h) As penalizações exigidas no caso de qualquer falha referente aos pontos acima.	IMP		■					Referência: Si-Termo Responsabilidade
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

3. 7.4_Classificação e Controlo de Ativos de Informação

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.4 - Gestão de Activos / Recursos**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.4.1	***Responsabilidade por activos/recursos de saúde.***	***Para alcançar e manter a proteção adequada dos ativos e recursos da organização.***								
		Inventário de activos/recursos (património) Todos os activos devem ser claramente identificados e deve ser elaborado e mantido um inventário de todos os activos importantes (patrimonio).								
		Propriedade de activos/recursos Todas as informações e activos associados às instalações de processamento de informação serão "detidas" por uma parte designada da organização.								
		Uso aceitável de activos/recursos Regras para o uso aceitável de informação e activos associados a instalações de processamento de informações devem ser identificadas, documentadas,e implementadas.								
7.4.2	***Classificação da informação de saúde***	***Para garantir que a informação recebe um nivel adequado de protecção.***								
7.4.2.1	Directrizes de classificação.	A informação deve ser classificada em função do seu valor, requisitos legais, sensibilidade e criticidade para a organização.								
7.4.2.2	Rotulagem e Tratamento de informação.	Um conjunto apropriado de procedimentos para rotulagem e manipulação de informação devem ser desenvolvidos e implementados em conformidade com o esquema de classificação adoptado pela organização de saúde. Devem também informar os utilizadores do confidencialidade das informações pessoais de saúde acessível a partir do sistema.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

4. 7.5_Segurança em Recursos Humanos

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.5 - Segurança em Recursos Humanos**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.5.1	***Antes da atribuição de Emprego***	***Para garantir que os funcionários, contratados e terceiros entendem as suas responsabilidades, e são adequados para as funções para que são considerados, e para reduzir o risco de roubo, fraude ou uso indevido das instalações.***								
7.5.1.1	Funções e Responsabilidades	Funções de segurança e responsabilidades dos funcionários, contratados e terceiros devem ser definidas e documentadas de acordo com a política de segurança da informação da organização de saúde. Especial atenção deve ser dada as funções e responsabilidades de funcionários temporários ou de curto prazo, tais como, voluntarios, estudantes, estagiários, etc.								
7.5.1.2	Triagem	Verificações de controlo de antecedentes de todos os candidatos a emprego, contratados e terceiros devem ser realizadas em conformidade com as disposições legais, regulamentares e éticos, e proporcionais ao requisitos de negócio, à classificação da informação a ser acedida, e dos riscos percebidos.								
7.5.1.3	Termos e condições de emprego	Como parte da sua obrigação contratual, funcionários, contratados e terceiros devem concordar e assinar os termos e condições do seu contrato de trabalho, os quais deverão indicar as suas responsabilidades e as da organização de saúde, para a segurança da informação. Em relação ao corpo clínico, os termos e condições de emprego devem especificar os direitos de acesso aos registros de assuntos de cuidados de saúde e sistemas de informação associados no caso de reclamações de terceiros.								
7.5.2	***Durante o Emprego***	***Para garantir que todos os funcionários, contratados e terceiros estão conscientes das ameaças e preocupações de segurança da informação, das suas responsabilidades e obrigações, e estão equipados para dar apoio à política de segurança organizacional no decurso do seu trabalho normal, e para reduzir o risco de erro humano.***								
7.5.2.1	Responsabilidade de Gestão	A Administração deve exigir dos funcionários, contratados e terceiros para aplicar a segurança em conformidade com as políticas estabelecidas e procedimentos da organização de saúde. É importante salvaguardar as preocupações dos utentes que não desejam que a sua informação pessoal de saúde seja acedida por trabalhadores de saúde, que são vizinhos, colegas ou parentes.								
7.5.2.2	Consencialização para segurança de informação, educação e formação	Todos os funcionários da organização e, eventualmente, contratados e terceiros, devem receber formação adequada e actualizações regulares das políticas e procedimentos organizacionais, como relevantes para a sua função. Em saúde é importante e relevantes, que terceiros contratados como pesquisadores, estudantes e voluntários que processam informação pessoal de saúde sejam integrados neste objectivo.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.5 - Segurança em Recursos Humanos**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.5.2.3	Processo disciplinar	Deve haver um processo disciplinar formal para empregados que tenham cometido uma violação de segurança. Além de cumprir com as leis aplicáveis, tais processos devem cumprir com os acordos alcançados entre os profissionais de saúde e o corpo de profissionais de saúde corpos.								
7.5.3	***Término ou mudança de emprego***	***Para garantir que os funcionários, contratados e terceiros saiam de uma organização ou mudam de emprego de uma forma ordenada.***								
7.5.3.1	Responsabilidade de término (rescisão) e Retorno de activos/recursos	Responsabilidades para realizar cessação de emprego ou alteração de posto de trabalho devem ser claramente definidas e atribuídas. Todos os funcionários, contratados e terceiros devem devolver todos os activos da organização em sua posse, ao término do seu emprego, contrato de trabalho, ou acordo.								
7.5.3.2	Retirada de direitos de acesso	Os direitos de acesso de todos os funcionários, contratados e terceiros à informação e às instalações de processamento de informação de saúde ou não, devem ser removidos no término de seu emprego, contrato de trabalho, ou acordo, ou ajustado em caso de mudança.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR:** Exigência da Norma de Referência, **RN/MP:** Requisitos de Negócio / Melhores Práticas adoptadas, **RAR:** Resultados da Avaliação de Risco, **ACP:** Até Certo Ponto

5. 7.6_Segurança Física e Ambiental

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Dominio: **7.6 - Segurança Física e Ambiental**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.6.1	***Áreas Seguras***	***Para prevenir acesso físico não autorizado, danos e interferências com o recinto e informação da organização.***								
7.6.1.1	Perímetro físico de segurança.	Perímetros de segurança (barreiras tais como paredes, portões de entrada com controlo de cartão ou balcões de recepção) devem ser utilizados para proteger as áreas que contenham informação e instalações de processamento de informação.	IMP	Controlos existentes		27001				
7.6.1.2	Controlos físicos de entrada; Segurança em escritórios, salas e instalações. Protecção contra ameaças externas e ambientais. Trabalhar em áreas seguras.	As áreas de segurança devem ser protegidas por controlos de entrada apropriados para garantir que somente pessoas autorizadas têm acesso. Segurança física para escritórios, salas e instalações devem ser concebida e aplicada. Protecção física contra danos causados por incêndio, inundação, terramoto, explosão, distúrbios civis, e outras formas de catástrofes naturais ou provocadas pelo homem, devem ser concebidos e aplicados. Protecção física e orientações para trabalho em áreas seguras deve ser concebida e aplicada.	IMP	Controlos existentes		27001	■	■		Implementar controlo de acesso por cartão magnetico em todos os centros de dados, e estabelecer registo de controlo de visitantes.
7.6.1.3	Acesso público, entregas e áreas de carga	Pontos de acesso, tais como áreas de entrega e zonas de carga, e outros pontos onde as pessoas não autorizadas podem entrar nas instalações devem ser controlados e, se possível, isoladas de instalações de processamento de informação, para evitar acesso não autorizado. Para garantir que a privacidade dos utentes dos cuidados de saúde seja mantida, muitas vezes requer que os anúncios sejam publicados em elevadores, atrás de portas, entrevistas que podem ser realizados, ou em outras áreas. Esses avisos servem como um lembrete para evitar discussão de casos de pacientes em áreas públicas.	IMP	Controlos existentes						
7.6.2	***Segurança de equipamentos***	***Para evitar perdas, danos, furto ou comprometimento de activos, e interrupção das actividades da organização.***								
7.6.2.1	Localização e protecção de equipamento	Os equipamentos devem ser alojados ou protegidos para reduzir os riscos de ameaças e perigos ambientais, e oportunidades de acesso não autorizado. Os dispositivos médicos de registro ou relatório de dados exigem considerações especiais de segurança em relação ao ambiente em que operam e às emissões eletromagnéticas que ocorrem durante a sua operação. Organizações de saúde, especialmente hospitais, devem garantir que as orientações de montagem e proteção para oa equipamentos TI tenham a exposição minimizaddas a tais emissões ou ambientes.	IMP	Controlos existentes		27001		■		

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.6 - Segurança Física e Ambiental**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.6.2.2	Utilitários de apoio. Segurança de cablagem. Manutenção de Equipamentos.	Os equipamentos devem ser protegidos contra falhas de energia e outras interrupções causadas por falhas nos serviços de apoio. Cablagem de alimentações e de telecomunicações que transmitam dados ou de apoio a serviços de informação devem ser protegidos contra intercepção ou danos. As organizações de saúde devem dar grande relevo a blindagem da rede TIC e outros cabos em áreas com altas emissões de dispositivos médicos. Os equipamentos devem ser correctamente mantidos para assegurar sua continua disponibilidade e integridade.	IMP	Controlos existentes				■		
7.6.2.3	Segurança de equipamentos fora das instações (da organização)	Segurança deve ser aplicada em equipamentos situados fora das instalações, tendo em conta os diferentes riscos de trabalhar fora das instalações da organização. As organizações de saúde devem assegurar que uso de quaisquer dispositivos médicos que efetua registro dados ou relatório médicos, fora de suas instalações, foi devidamente autorizado para oefeito. Isto deve incluir equipamentos utilizados pelos trabalhadores remotos, mesmo quando tal uso é perpétua (isto é, dentro da organização, em ambulância, por terapeutas, etc).	IMP	Controlos existentes						
7.6.2.4	Abate seguro ou reutilização de equipamentos	Todos os itens de equipamento que contenham mídia de armazenamento de informação devem ser verificados para garantir que todos os dados sensíveis e software licenciado foram apagados ou removidos de forma segura antes da eliminação. As organizações de saúde devem substituir de forma segura, ou então destruir todas as mídias que tenham software aplicativo de saúde ou informações pessoais de saúde, quando deixam de ser nececessários.	N/A	Não faz parte do objectivo						
7.6.2.5	Remoção de Propriedade	Equipamento, informação ou software não devem ser levados das instalações sem autorização prévia.	IMP	Controlo existente.						Usar controlo de acessos.
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

6. 7.7_Gestão de Comunicações e Operações

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.7.1	***Procedimentos operacionais e responsabilidades***	Para garantir a operação segura e correcta das instalações de processamento de informação.								
7.7.1.1	Procedimentos operacionais documentados	Procedimentos operacionais devem ser documentados, mantidos, e disponibilizados para todos os utilizadores que deles precisam.								
7.7.1.2	Gestão de Mudança	Alterações às instalações e sistemas de processamento da informação devem ser controladas. As organizações de saúde devem, por meio de um processo formal e estruturado de controle de mudanças. Por exemplo na mudança de instalações de processamento de informações e sistemas que processam informações pessoais de saúde, deve garantir um controle adequado da continuidade da assistência ao paciente por parte das aplicações do host e sistemas.								
7.7.1.3	Segregação de funções	Funções e áreas de responsabilidade devem ser segregadas para reduzir oportunidades de modificação não autorizada ou acidental, ou uso indevido dos bens da organização. As organizações de saúde devem assegurar que os sistemas de TI utilizados contêm funcionalidades na aplicação que impõem a aprovação de processos clínicos por detentores de papéis diferentes, onde este é necessário.								
7.7.1.4	Separação de instalações de Desenvolvimento e Operações	Instalações de desenvolvimento, teste e produção devem ser separadas para reduzir os riscos de acesso não autorizado ou alterações no sistema produtivo. As organizações de saúde devem separar (física ou virtualmente) desenvolvimento e ambientes de testes do sistema de informação. As regras para migração de software de desenvolvimento para o ambiente produção devem ser definidas e documentados pela organização que hospeda o aplicativo afetado(s).								
7.7.2	***Gestão de Prestação de Serviços por Terceiros***	Para implementar e manter o nível adequado de segurança da informação, e prestação de serviços em consonância com o acordo de prestação de serviços por terceiros.								
		Prestação de Serviços. Deve ser garantido que os controlos de segurança, definições de serviços e níveis de prestação incluídos no acordo de prestação de serviços por terceiros são implementados, operados e mantidos pelos terceiros.								
		Acompanhamento e revisão de serviços de terceiros. Os serviços, relatórios e registos fornecidos pelos terceiros deverão ser regularmente monitorizados e analisados, e devem ser realizadas auditorias regularmente.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
		Gestão de mudanças nos serviços de terceiros. Alterações à prestação de serviços, incluindo manutenção e melhoramento de políticas, procedimentos e controlos de segurança da informação existentes, devem ser geridos, tendo em conta a criticidade dos sistemas e processos de negócio envolvidos, e reavaliação dos riscos.								
7.7.3	***Planeamento de Sistema e Aceitação***	Para minimizar o risco de falhas nos sistemas.								
7.7.3.1	Gestão de capacidade	A utilização de recursos deve ser monitorizada, sincronizada, e as projecções de requisitos de capacidade futura devem ser feitas para garantir o necessário desempenho do sistema.								
7.7.3.2	Aceitação do sistema	Critérios de aceitação para novos sistemas de informação, upgrades e novas versões devem ser estabelecidos, e testes apropriados do sistema(s) devem ser realizados durante o desenvolvimento e antes da aceitação.								
7.7.4	***Proteção contra código malicioso e móvel***	Para proteger a integridade do software e da informação.								
7.7.4.1	Controlo contra código malicioso	Controlos de detecção, prevenção, recuperação para proteger contra código malicioso, e procedimentos adequadamente de conscienlização do utilizador devem ser implementados.								
7.7.4.2	Controlo contra código móvel	Quando o uso de código móvel é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança claramente definida, e código móvel não autorizado deve ser impedido de ser executado.								
		Para manter a integridade e disponibilidade da informação e das instalações de processamento da informação.								
7.7.5	***Backup de informação de Saúde***	**Backup de informação** Cópias de segurança da informação e de software devem ser retiradas e testadas regularmente de acordo com a política de backup acordada. - As organizações de saúde devem fazer backup de todas as informações pessoais de saúde e armazená-la em ambiente fisicamente seguro para garantir a sua disponibilidade futura. - Para proteger a sua confidencialidade, as informações pessoais de saúde devem ser apoiadas num formato encriptado.								
7.7.6	***Gestão da Segurança de Rede***	Para garantir a protecção da informação em rede, e a protecção da infra-estrutura de apoio.								
7.7.6.1	Controlos de rede	Redes devem ser adequadamente geridas e controladas, a fim de serem protegidas contra ameaças, e para manter a segurança para os sistemas e aplicações que usam a rede, incluindo a informação em trânsito.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> **Versão:** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.7.6.2	Segurança dos serviços de rede	As organizações de saúde devem considerar cuidadosamente o impacto que a perda de disponibilidade de serviço de rede terá sobre a prática clínica. Ver também 7.11. Os recursos de segurança, níveis de serviço e requisitos de gestão de todos os serviços de rede devem ser identificados e incluídos em qualquer contracto de serviços de rede, quer esses serviços sejam prestados internamente ou por terceiros.								
7.7.7	***Manuseamento de Mídia (Suportes)***	Para evitar a divulgação, modificação, remoção ou destruição de bens não autorizada, e interrupção de atividades empresariais.								
7.7.7.1	Gestão de mídia amovível/removíveis	Devem existir procedimentos em execução para a gestão de media removível. As organizações de saúde devem assegurar que todas as informações pessoais de saúde armazenadas em mídia removível, são/estão: a) encriptadas durante a comunicação ou b) protegidas contra qualquer tentativa de roubo.								
7.7.7.2	Eliminação de mídia	Todas as informações pessoais de saúde devem ser devidamente distruidas ou então a mídia destruída quando quando deixam de ser necessárias. NO caso se proceder a destruição da mídia, esta deve ser feita devede maneira segura e cuidadosa, através de procedimentos formais.								
7.7.7.3	Procedimentos de manuseamento ou manipulação de informação	Procedimentos para o manuseamento e armazenamento de informação devem ser estabelecidos para proteger essa informação contra divulgação não autorizada ou uso indevido. A mídia que conêm informações pessoais de saúde devem ser fisicamente protegidos ou então devem os seus dados encriptotados. O status e a localização dos mídias encriptados com informações pessoais de saúde devem ser monitoradas.								
7.7.7.4	Segurança da documentação do sistema	A documentação do sistema deve ser protegida contra acesso não autorizado.								
7.7.8	***Troca de Informação***	Para manter a segurança da informação e software trocados dentro de uma organização e com qualquer entidade externa.								
7.7.8.1	Políticas e procedimentos e acordos de troca de informações de saúde	Políticas, procedimentos e controlos de trocas formais devem estar disponíveis para proteger a troca de informação através da utilização de todos os tipos de meios de comunicação. As organizações de saúde devem assegurar que a segurança de trocas de informações seja um tema ou ponto da política de desenvolvimento e auditoria de conformidade (ver 7.12). A segurança da troca de informações pode ser facilitada pelo uso de acordos de troca de informações que especificam o conjunto mínimo de controles a serem implementados.								
7.7.8.2	Mídia (meios física) em trânsito	A mídia que contêm informação deve ser protegida contra acesso não autorizado, uso indevido ou corrupção durante o transporte para além dos limites físicos da organização.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.7.8.3	Mensagens electrónicas	Informação envolvida em mensagens eletrónicas deve ser adequadamente protegida. Ss organizações que transmitem informações pessoais de saúde por mensagens eletrônicas deve tomar medidas para garantir a sua confidencialidade e integridade. O E-mail entre os profissionais de saúde que contém informações pessoais de saúde devem ser encriptotados durante a comunicação. Uma abordagem a este envolve o uso de certificados digitais.Existe uma lista de normas relacionadas com o uso de certificados digitais em ambientes de saúde. Ver secção 7.12.2.2 para uma analise prévia para a comunicação fora da organização.								
7.7.8.4	Sistemas de Informação de saúde	Políticas e procedimentos devem ser desenvolvidas e implementados para proteger a informação associada à interligação dos sistemas de informação do negócio.								
7.7.9	***Serviços de Comércio Eletrónico de Saúde***	Para garantir a segurança dos serviços de comércio electrónico, e a sua utilização segura.								
7.7.9.1	Comércio Electrónico e Transacções On-Line	Informação envolvida em comércio electrónico em redes públicas deve ser protegida contra actividades fraudulentas, disputas contractuais, e divulgação não autorizada e modificações. É importante observar os cuidados que devem ser tomados para determinar se os dados envolvidos em comércio eletrônico e transações on-line contêm informações pessoais de saúde. Se o fizerem, essa informação deve ser protegida adequadamente. Informação envolvida em transações on-line deve ser protegida para prevenir transmissão incompleta, erro de rota, alteração não autorizada da mensagem, divulgação não autorizada, duplicação não autorizada da mensagem ou repetição.								
7.7.9.2	Informação de saúde disponíveis ao público	A integridade da informação disponibilizada ao público num sistema de acesso livre deve ser protegida para impedir a modificação não autorizada. As informações de saúde disponíveis ao público (como distinto de informações pessoais de saúde) deve ser arquivado. A integridade dessas informações deve ser protegida para impedir a modificação não autorizada. A fonte (autoria) de informações de saúde disponíveis ao público deve ser declarada ea sua integridade deve ser protegida.								
7.7.10	***Monitorização***	Para detectar actividades não autorizadas de processamento de informação.								
7.7.10.1	Registo de auditoria	Relatórios de auditoria que registem actividades do utilizador, excepções e eventos de segurança da informação devem ser produzidos e mantidos por um período acordado, para auxiliar em futuras investigações e monitorização de controlo de acesso. O registo de auditoria eficaz pode ajudar a descobrir mau uso do sistema de informação de saúde ou de informações pessoais de saúde.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.7.10.2	Log da Auditoria	Procedimentos de monitorização da utilização do sistema de processamento de informação deve ser estabelecida, e os resultados de monitorização das actividades devem ser revistos regularmente. Os sistemas de informação de processamento de informações pessoais de saúde devem criar um registro de auditoria seguro sempre que um utilizador acede, cria, efetua atualizações em arquivos de informações pessoais de saúde através do sistema. O log de auditoria deve identificar o usuário, identificar a pessoa em causa (ou seja, o assunto do cuidado), identificar a função desempenhada pelo usuário (criação do registro, acesso, atualização, etc), e a hora e a data em que o função foi executada.								
7.7.10.3	Monitorização do uso do sistema	Num sistema de informação de saúde o log de auditoria deve estar operacional/disponivel a qualquer momento para ser utilizado em caso de necessidade. Os sistemas de informação em saúde, que tenham informações pessoais de saúde devem permitir a análise de logs e trilhas de auditoria que: a) permitem a identificação de todos os utilizadores do sistema que têm acesso ou modificade um dado assunto num registro de tratamento(s) ao longo de um determinado período de tempo; b) permitir a identificação de todos os assuntos de cuidados cujos registros foram acedidos ou modificados por um utilizador do sistema durante um determinado período de tempo.								
7.7.10.4	Protecção de informação de Log (Auditoria)	Instalações de registo informações de acesso (log) devem ser protegidas contra adulteração e acesso não autorizado. O registro de auditoria deve estar seguro e à prova de falsificação. O acesso a ferramentas de auditoria de sistemas e trilhas de auditoria devem ser salvaguardados para evitar o uso indevido ou quebras de compromisso.								
7.7.10.5	Registo de administrador e operador	Actividades do administrador do sistema e do operador do sistema devem ser registadas.								
7.7.10.6	Registo de falhas	Falhas devem ser registadas, analisadas e tomadas as decisões ou medidas adequadas.								
7.7.10.7	Sincronização dos relógios	Os relógios de todos os sistemas de processamento de informação relevantes dentro de uma organização ou domínio de segurança devem ser sincronizados com uma fonte precisa de tempo definida. Sistemas de informação de apoio a actividades de saúde e cuidados em que o tempo é crítico deve fornecer serviços de sincronização de tempo para apoiar o rastreamento e reconstituição de cronogramas de atividades, quando necessário.								
...										
...										

LOGOTIPO	MDPSIOS - Documento de Objectivos / Aplicabilidade " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> **Versão:** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.7 - Gestão de Comunicações e Operações**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

7. 7.8_Controlo de Acessos

LOGOTIPO	**MDPSIOS - Documento de Objectivos / Aplicabilidade** " Organização "	Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.8 - Controlo de Acessos** (ao sistema informático)

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.8.1	***Requisitos de Negócio para Controlo de Acesso***	***Para controlar o acesso à informação.***								
7.8.1.1	Requisitos para controle de acesso em saúde	As organizações de saúde com informações pessoais de saúde devem controlar o acesso a essas informações. Em geral, os utilizadores dos sistemas de informação de saúde só devem aceder as informações pessoais de saúde: a) quando existe um relacionamento de saúde entre o utilizador e a utente em causa (pessoa cuja informação pessoal de saúde está aser acedida); b) quando o utilizador está a realizar uma atividade em nome da pessoa em causa; c) quando existe uma necessidade de dados específicos para apoiar esta actividade.								
7.8.1.2	Política de controlo de acesso	Uma política de controlo de acesso deve ser estabelecida, documentada e analisada, tendo por base os requisitos de acesso do negócio e da segurança. As organizações de saúde com informações pessoais de saúde devem ter uma política de controle de acesso que rege o acesso a esse informação (dados). A política da organização sobre o controle de acesso deve ser estabelecida com base em papéis pré-definidos com autoridades associados que são coerentes, mas limitando a, as necessidades desse papel. A política de controle de acesso, como um componente do quadro da política de segurança da informação descrito no ponto 7.2.1, deve reflectir aspectos profissionais, éticos, legais.								
7.8.2	***Gestão de Acesso de Utilizadores***	***Para assegurar acesso de utilizador autorizado e prevenir acesso não autorizado a sistemas de informação.***								
7.8.2.1	Registo de Utilizadores	Deve existir um procedimento formal de registo e cancelamento de utilizador para garantir e revogar acessos a todos os sistemas de informação e serviços. O acesso a sistemas de informação de saúde com informações pessoais de saúde devem estar sujeitos a um processo formal de registo de utilizador. Este processo deve garantir que o nível de autenticação necessária da identidade do utilizador seja consistente com o nível (s) de acesso que está disponível para o mesmo. Os detalhes de registo do utilizaor deve ser revisto periodicamente para assegurar que estão completos, precisos e que o acesso continua a ser necessária.								
7.8.2.2	Gestão / Avaliação de Privilégios	A concessão e o uso de privilégios deve ser restrita e controlada. Nas organizações de saúde as estratégias de controle de acesso são várias, estas devem garantir significativamente a confidencialidade e integridade das informações pessoais de saúde. Entre outras devem garantir que durante o registo os privilégios de acesso dos utilizadores é restringido apenas as necessárias para cumprir um ou mais papéis bem definidos.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.8 - Controlo de Acessos** (ao sistema informático)

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.8.2.3	Gestão de passwords de utilizadores	A concessão de passwords deve ser controlada através de um processo formal de gestão. Nas organizações de saúde a pressão das alterações temporais das passwords pode fazer uma utilização eficaz das mesmas em termos de segurança, mas difícil de utilizar. Muitas organizações de saúde têm considerado a adoção de tecnologias de utenticação alternativas para resolver este problema.								
7.8.2.4	Revisão de direitos de acesso de utilizadores	A gestão deve rever os direitos de acesso dos utilizadores em intervalos regulares de tempo, através de um processo formal. Nas organizações de saúde, deve-se ter uma atenção especialaos utilizadores que podem prestar cuidados de emergência, eles podem ter acesso a informações pessoais de saúde em situações de emergência, onde o utente aos cuidados de emergência pode ser incapaz para comunicar o seu consentimento ao acesso a informação.								
		Para prevenir o acesso não autorizado dos utilizadores, e evitar o comprometimento ou roubo de informação e das instalações de processamento de informação. As organizações de saúde devem, ao determinar responsabilidades do utilizador respeitar os direitos e responsabilidades éticas dos profissionais de saúde, tal como acordado na lei e como aceite pelos membros dos órgãos profissionais de saúde .								
7.8.3	***Responsabilidade dos Utilizadores***	**Uso de password** Os utilizadores devem ser orientados a seguir boas práticas de segurança na selecção e uso de passwords.								
		Equipamento de utilizador disponivel sem monitorização Os utilizadores devem assegurar que os equipamentos não monitorizados tenham protecção adequada.								
		Política de Secretária livre e Ecran livre Deve ser adoptada uma política de secretária limpa de papéis e de medias de armazenamento removíveis, e uma política de ecran limpo, para as instalações de processamento de informação.								
		Para prevenir acesso não autorizado aos serviços de rede.								
		Política de uso de serviços de rede Os utilizadores devem receber acesso apenas aos serviços a que tenham sido especificamente autorizados a usar.								
		Autenticação de utilizador para ligações externas Métodos apropriados de autenticação devem ser usados para controlar o acesso de utilizadores remotos.								
		Identificação de equipamentos na rede Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.8 - Controlo de Acessos** (ao sistema informático)

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.8.4	***Controlo de acesso à rede eControlo de acesso ao Sistema Operativo***	**Diagnóstico remoto e proteção de configuração de porta** Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.								
		Segregação em redes Grupos de serviços de informação, utilizadores e sistemas de informação devem ser segregados em redes.								
		Controlo de ligações na rede Para redes partilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de utilizadores se ligarem à rede deve ser restringida, de acordo com a política de controlo de acesso e os requisitos das aplicações do negócio (ver 7.8.1).								
		Controlo de routing na rede Deve ser implementado controlo de roteamento na rede para assegurar que as ligações de computador e fluxos de informação não violem a política de controlo de acesso das aplicações do negócio.								
		Para prevenir acesso não autorizado aos sistemas operativos.								
		Procedimentos de Log-on seguro O acesso aos sistemas operativos deve ser controlado por um procedimento seguro de entrada no sistema (log-on).								
		Identificação e autenticação de utilizador Todos os utilizadores devem ter um identificador único (ID de utilizador) para o seu uso pessoal e exclusivo, e deve ser escolhida uma técnica adequada de autenticação para validar a identidade alegada por um utilizador.								
		Sistema de Gestão de Passwords Sistemas para gestão de passwords devem ser interactivos e devem assegurar senhas de qualidade.								
		Uso de utilidades do sistema O uso de programas utilitários que possam ser capazes de sobrepor os controlos dos sistemas e aplicações deve ser restrito e estritamente controlado.								
		Time-out de sessão Sessões inactivas devem ser terminadas após um período definido de inactividade.								
		Limitação do tempo de ligação Restrições nos tempos de ligação devem ser utilizadas para proporcionar segurança adicional para aplicações de alto risco.								
7.8.5	*Aplicações e Controlo de acesso a informação*	***Para prevenir acesso não autorizado a informação contida nos sistemas de aplicações.***								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Domínio: **7.8 - Controlo de Acessos** (ao sistema informático)

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.8.5.1	Restrição de acesso a informação	O acesso a informação e funções dos sistemas de aplicações por utilizadores e pessoal do suporte deve ser restringido de acordo com a política de controlo de acesso definida. Os sistemas de informação que processam informações pessoais de saúde devem autenticar os utilizadores envolvendo pelo menos dois fatores.								
7.8.5.2	Isolamento de sistemas sensíveis	Sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).								
7.8.6	***Computação móvel e trabalho remoto***	***Para garantir a segurança da informação quando se utiliza computação móvel e recursos de trabalho remoto.***								
7.8.6.1	Computação móvel e comunicações	Uma política formal deve ser estabelecida, e medidas de segurança apropriadas devem ser adotadas para a protecção contra os riscos do uso de recursos de computação e comunicação móveis. As organizações de saúde que processam informações pessoais de saúde, devem dar atenção especial a este ponto.								
7.8.6.2	Trabalho remoto / Teletrabalho	Uma política, planos operacionais e procedimentos devem ser desenvolvidos e implementados para actividades de trabalho remoto. As organizações de saúde que processam informações pessoais de saúde devem: a) Preparar uma política sobre as precauções a serem tomadas quando do teletrabalho; b) garantir que os utilizadores as cumprem								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

8. 7.9_Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Dominio: **7.9 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
	Requisitos de Segurança de Sistemas de Informação	***Para garantir que segurança é parte integrante dos sistemas de informação.***								
7.9.1		**Análise e especificações de requisitos de segurança** Devem ser especificados os requisitos para controlo de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.								
7.9.2	***Processamento correcto em Aplicações***	***Para prevenir a ocorrência de erros, perdas, modificação não autorizada ou uso indevido de informação em aplicações.***								
7.9.2.1	Identificação exclusiva de assuntos de cuidados de saúde	Os sistemas de informação que processam informações pessoais de saúde devem: a) garantir que cada objecto de cuidados de saúde é identificado exclusivamente dentro do sistema; b) ser capaz de juntar registos duplicados ou múltiplos se, se verificar que vários registos do mesmo assunto foram criados involuntariamente ou durante uma emergência médica.								
7.9.2.2	Validação de dados de entrada	Os dados de entrada de aplicações devem ser validados para garantir que são correctos e apropriados.								
7.9.2.3	Controlo de processamento interno	Devem ser incorporadas nas aplicações verificações de validação para detectar qualquer corrupção de informação, por erros de processamento ou por actos deliberados.								
7.9.2.4	Integridade da mensagem	Requisitos para garantir a autenticidade e proteger a integridade da mensagem em aplicações e os controlos apropriados devem seridentificados e implementados.								
7.9.2.5	Validação de dados de saída	Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas é correcto e apropriado às circunstâncias. Os sistemas de informação que processam informações pessoais de saúde devem fornecer informações para auxiliar os profissionais de saúde na confirmação de que o registro eletrônico de saúde corresponde ao objecto recuperada do cuidado de saúde em tratamento.								
7.9.3	***Controlos de criptografia***	***Para proteger a confidencialidade, autenticidade ou integridade da informação por meios criptográficos.***								
7.9.3.1	Política sobre o uso de controlos criptográficos e gestão de certificados	Deve ser desenvolvida e implementada uma política sobre o uso de controlos criptográficos para protecção da informação. Para as organizações de saúde a orientação sobre a política para a emissão e uso de certificados digitais nos cuidados de saúde e na gestão de chaves podem ser verificadas na ISO 17090-3								
7.9.3.2	Gestão de chaves	Um processo de gestão de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.								
7.9.4	***Segurança dos arquivos de sistema***	***Para garantir a segurança de ficheiros de sistema.***								
7.9.4.1	Controlo de software Operacional	Devem existir procedimentos para controlar a instalação de software em sistemas operacionais.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.9 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.9.4.2	Protecção de dados de teste do sistema	Os dados de teste devem ser seleccionados com cuidado, e protegidos e controlados. As organizações de de saúde que processam informação pessoal de saúde não devem utilizar a informação real sobre a saúde pessoal, como dados de teste.								
12.4.3	Controlo de acessos ao código-fonte dos programas	O acesso ao código-fonte dos programas deve ser restrito.								
7.9.5	***Segurança nos processos de Desenvolvimento e Suporte e Gestão de Vulnerabilidades Tecnicas***	***Para manter a segurança do software do sistema de aplicações e informação e para reduzir os riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.***								
		Mudança do controlo de processos A implementação de mudanças deve ser controlada utilizando procedimentos formais de controlo de mudanças.								
		Revisão técnica de aplicações após mudanças no Sistema Operativo Aplicações criticas do negócio devem ser analisadas e testadas quando os sistemas operativos são mudados, para garantir que não há qualquer impacto adverso na operação ou segurança da organização.								
		Restrições para alterações em pacotes de software Modificações a pacotes de software não devem ser incentivadas, devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.								
		Fugas de informação Devem ser prevenidas oportunidades para fugas de informações.								
		Desenvolvimento de software por terceiros A organização deve supervisionar e monitorizar o desenvolvimento de software por terceiros.								
		Controlo de vulnerabilidades técnicas Deve ser obtida informação em tempo útil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a essas vulnerabilidades, e devem ser tomadas as medidas apropriadas para lidar com os riscos associados.								
	...									
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

9. 7.10_Gestão de Incidentes de segurança da Informação

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

*Histórico do Documento >>> **Versão:** _____ Data: ____/____/____ Responsável: _____ Descrição da Atualização: _____*

Dominio: **7.10 - Gestão de Incidentes de Segurança da Informação**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.10.1	***Notificação de Eventos e Fraquezas de Segurança da Informação***	***Para asssegurar que fragilidades e eventos de segurança da informação associados ao sistema de informação sejam comunicados de maneira a permitir a tomada de acção corretiva em tempo útil.***								
		Notificação de eventos de segurança da Informação Eventos de segurança da informação devem ser comunicados o mais cedo possível, através canais de gestão apropriados. As organizações de saúde que processam informações pessoais de saúde devem estabelecer as responsabilidades da gestão de procedimentos de incidentes de segurança.								
		Notificação de fraquezas de segurança Todos os funcionários, contratados e terceiros, que utilizem sistemas de informação e serviços, serão obrigados a anotar e reportar quaisquer falhas de segurança, observadas ou suspeitas , nos sistemas ou serviços.								
7.10.2	***Gestão de Incidentes de Segurança da Informação e Melhorias***	***Para garantir que uma abordagem consistente e efectiva seja aplicada à gestão de incidentes de segurança da informação.***								
7.10.2.1	Responsabilidades e procedimentos	Devem ser estabelecidas responsabilidades e procedimentos de gestão, para garantir uma resposta rápida, eficaz e ordenada sobre incidentes de segurança da informação.								
7.10.2.2	Aprendizagem por incidentes de segurança da Informação	Deverá haver mecanismos para permitir que o tipo, quantidade, e custo dos incidentes de segurança da informação possam ser quantificados e monitorizados.								
7.10.2.3	Recolha de provas	No seguimento de uma acção contra uma pessoa ou organização após um incidente de segurança da informação que involva acção legal (quer civil ou criminal), as provas devem ser recolhidas, mantidas e apresentadas em conformidade com as regras para provas, definidas na jurisdição relevante.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

MDPSIOS [Pag. 1 de 1]

10. 7.11_Gestão Continuidade do Negócio

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.11 - Gestão da Continuidade do Negócio**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
		Para contrariar interrupções a actividades do negócio e para proteger os processos críticos do negócio contra efeitos de falhas graves de sistemas de informação ou desastres, e assegurar o seu recomeço em tempo útil. Nas organizações de saúde é cada vez mais reconhecida como um requisito prioritario e desafiador para os profissionais da segurança da informação.								
7.11	***Aspectos de Segurança da Informação de Gestão da Continuidade do Negócio***	**Incluir a Segurança da Informação no processo de gestão da continuidade do Negócio** Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.								
		Continuidade do Negócio e Avaliação de Risco Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto com a probabilidade e impacto de tais interrupções e as suas conseqüências para a segurança da informação.								
		Desenvolvimento e implementação de planos de continuidade incluindo segurança da informação Devem ser desenvolvidos e implementados planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.								
		Quadro de planeamento de continuidade de Negócio Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação, e para identificar prioridades para testes e manutenção.								
		Testar, manter e re-avaliar os planos de continuidade do Negócio Os planos de continuidade do negócio devem ser testados e actualizados regularmente, de forma a assegurar sua permanente actualização e efectividade.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I:** Não Implementado, **IPM:** Implementado Parcialmente, **IEC:** Implementação Em Curso, **IMP:** Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

MDPSIOS [Pag. 1 de 1]

11. 7.12_Conformidade

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade
" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.12 - Conformidade**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
7.12.1	***Geral***	***As organizações de saúde deve colocar um programa de auditoria de conformidade que aborda o ciclo de vida completo de operações, ou seja, não apenas daqueles processos que identificam problemas, mas também daqueles em que os resultados de revisão decidem sobre atualizações para o SGSI...***								
7.12.2	***Conformidade com Requisitos Legais***	***Para evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.***								
7.12.2.1	Identificação de legislação aplicável, Direitos de Propriedade Intelectual (DPI), Protecção de registos organizacionais	**Identificação de legislação aplicável** Todos os requisitos estatutários, regulamentares e contractuais relevantes e a abordagem da organização para atender a estes requisitos devem ser explicitamente definidos, documentados e mantidos actualizados para cada sistema de informação e para a organização.								
		Direitos de Propriedade Intelectual (DPI) Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contractuais no uso de material, em relação ao qual pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.								
		Protecção de registos organizacionais Registos importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.								
7.12.2.2	Protecção de Dados e privacidade de informações pessoais	A privacidade e protecção de dados devem ser asseguradas conforme o exigido nas legislações relevantes, regulamentações, e, se aplicável, nas cláusulas contratuais. As organizações de saúde que processam informações pessoais de saúde devem gerir o consentimento a informação sobre assuntos de cuidados de saúde.								
7.12.2.3	Prevenção do mau uso das instalações de processamento de informação, Regulamentação de controlos criptográficos	**Prevenção do mau uso das instalações de processamento de informação** Os utilizadores devem ser dissuadidos de usar as instalações de processamento de informação para propósitos não autorizados.								
		Regulamentação de controlos criptográficos Controlos de criptografia devem ser usados em conformidade com todas as leis, acordos e regulamentações relevantes.								
7.12.3	***Conformidade com Políticas e Normas de Segurança, e conformidade Técnica***	***Para garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança. Nas organizações de saúde deve existir uma especial atenção para o cumprimento do propósito de interoperabilidade técnica.***								
		Conformidade com a política de segurança Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados correctamente para garantir a conformidade com as normas e políticas de segurança.								

LOGOTIPO

MDPSIOS - Documento de Objectivos / Aplicabilidade

" Organização "

Morada

DATA : ____/____/_____ **Versão:** _____ Responsável: _____ Class. Informação: _____ Aprovado por: _____ Em: ____/____/_____

Histórico do Documento >>> ***Versão:*** _____ *Data:* ____/____/____ *Responsável:* _____ *Descrição da Atualização:* _____

Dominio: **7.12 - Conformidade**

ISO 27799:2008 - Objectivos de Controlo			Controlo (Situação)	Observações	Controlos Selecionados e Razões para a selecção					Metodo / Observações (visão geral e considerações) Documento AAM
					RL	ENR	RN/MP	RAR	ACP	
Secção	**Objectivo**	**Controlo / Descrição**								
		Verificação de conformidade técnica Os sistemas de informação devem ser periodicamente verificados relativamente à sua conformidade com as normas de implementação de segurança.								
7.12.4	***Considerações de Auditoria do Sistema de Informação num ambiente de saúde***	***Para maximizar a eficácia de, e minimizar a interferência para/de, o processo de auditoria dos sistemas de informação.***								
		Controlos de Auditoria do Sistema de Informação Os requisitos e actividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planeados e acordados para minimizar os riscos de interrupção dos processos do negócio.								
		Protecção das ferramentas de auditoria de sistemas de informação O acesso às ferramentas de auditoria do sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.								
...										
...										

Legenda

"Controlo (Situação)" :

N/A: Não se Aplica, **N/I**: Não Implementado, **IPM**: Implementado Parcialmente, **IEC**: Implementação Em Curso, **IMP**: Implementado

"Controlos Selecionados e Razões para selecção" :

RL: Requisitos Legais, **ENR**: Exigência da Norma de Referência, **RN/MP**: Requisitos de Negócio / Melhores Práticas adoptadas, **RAR**: Resultados da Avaliação de Risco, **ACP**: Até Certo Ponto

Anexo I – MPDSIOS – Descrição do MARSI adaptada do MARAT

O **MARSI** como método resultante da adoção e adaptação do MARAT permite, quantificar a magnitude dos riscos existentes e, como consequência, hierarquizar de modo racional a prioridade da sua eliminação ou correção [72][73][74].

Os conceitos chave da avaliação são:

- A probabilidade de que determinados fatores de risco (perigos ou tão somente *ameaças* que explora uma ou mais *vulnerabilidade*) se materializam em danos.
- A magnitude dos danos (também designado por severidade ou tão somente *consequências*).

No MARAT, tendo em conta que estamos no campo dos *acidentes laborais* temos a seguinte definição [72][74][75]:

- O risco é, em termos gerais, o resultado do produto da probabilidade pela *severidade*.
- A probabilidade traduz a medida do desencadeamento do acontecimento inicial. Integra em si a duração da exposição das *pessoas* ao *perigo* e as *medidas preventivas* existentes.

  Em resumo, pode-se afirmar que a probabilidade é função do nível de exposição e do conjunto das deficiências (que é o oposto das *medidas preventivas* existentes para os fatores em análise) que contribuem para o desencadear de um determinado acontecimento não desejável (acidente).

No **MARSI** (método adaptado para o **MDPSIOS**), isto é transpondo para o campo dos *incidentes/eventos de segurança da informação*, teremos a seguinte definição:

- O risco é, em termos gerais, o resultado do produto da probabilidade pela severidade (*consequência/dano/impacto)* na organização.
- A probabilidade traduz a medida do desencadeamento do acontecimento inicial. Integra em si a duração da exposição da *vulnerabilidade* a uma *ameaça* e os *controlos* existentes.

  Em resumo, pode-se afirmar que a probabilidade é função do nível de exposição e do conjunto das deficiências (que é o oposto dos *controlos* existentes para os fatores em análise) que contribuem para o desencadear de um determinado acontecimento não desejável (incidente/evento).

No desenvolvimento do método não se utilizarão valores absolutos mas intervalos discretos pelo que se utilizará o conceito de nível. Assim o nível de risco (NR) será função do nível de probabilidade (NP) e do nível de severidade/consequência (NS). O nível de controlo/intervenção (NC) hierarquiza de modo racional a prioridade da sua eliminação ou correção. Esta metodologia é representada pelo fluxograma seguinte [72][73][74]:

1. Nível de Deficiência (ND)

   Designa-se por nível de deficiência (ND), ou nível de ausência de medidas preventivas (controlos), a magnitude esperada entre o conjunto de fatores de risco considerados e a sua relação causal direta com o incidente/evento [72][73][74].

   Deve ser determinado com base numa lista de verificação, definida pela organização, que analise os possíveis fatores de risco de cada situação, e desta forma evita subjetividade ou ambiguidade na avaliação do nível de deficiência resultante.

   A tabela que se segue enquadra a avaliação num determinado nível de deficiência:

Nível de Deficiência	***ND***	*Significado*
1. Aceitável	**1**	Não foram detetadas anomalias. O perigo está controlado.
2. Melhorável	**2**	Foram detetados fatores de risco de menor importância. É de admitir que o dano possa ocorrer algumas vezes.
3. Dificente	**6**	Foram detetados alguns fatores de risco significativos que precisam de ser corrigidos. O conjunto de medidas preventivas existentes tem a sua eficácia reduzida de forma significativa.
4. Muito Deficiente	**10**	Foram detetados fatores de risco significativos que determinam como muito possível a ocorrência de falhas. As medidas preventivas existentes são ineficazes. O dano ocorrerá na maior parte das
5. Deficiência Total	**14**	Medidas preventivas inexistentes ou desadequadas. São esperados danos na maior parte das situações.

2. Nível de Exposição (NE)

O nível de exposição é uma medida que traduz a frequência com que o ativo está exposto ao risco. Para um risco concreto, o nível de exposição pode ser estimado em função dos tempos de permanência perante a ameaça [72][73][74].

Deve ser determinado com base num histórico ou numa lista de verificação, definida pela organização, que analise os possíveis fatores de risco de cada situação, e desta forma evita subjetividade ou ambiguidade na avaliação do nível de exposição resultante.

A tabela que se segue enquadra a avaliação num determinado nível de exposição:

Nível de Exposição	***NE***	*Significado*
1. Esporádica	**1**	Irregularmente. Uma vez por ano ou menos e por pouco tempo (minutos)
2. Pouco Frequente	**2**	Alguma vez por ano e por periodo de tempo determinado.
3. Ocasional	**3**	Alguma vez durante o período laboral e com um período curto de tempo, algumas vezes por mês.
4. Frequente	**4**	Várias vezes durante o período laboral, ainda que com tempos curtos – várias vezes por semana ou diário.
5. Continuada	**5**	Várias vezes por dia com tempo prolongado ou continuamente.

3. Nível de Probabilidade (NP)

O nível de probabilidade é função das medidas preventivas existentes (controlos) e do nível de exposição do ativo ao risco. Pode ser expresso num produto de ambos os termos (**ND**x**NE**) apresentado na tabela abaixo [72][73][74]:

Nível de Probabilidade	***NP***	*Significado*
Muito Baixa	**[1;3]**	Não é de esperar que a situação perigosa se materialize, ainda que possa ser concebida.
Baixa	**[4;6]**	A materialização da situação perigosa pode ocorrer.
Média	**[8;18]**	A materialização da situação perigosa é possivel de ocorrer pelo menos uma vez com danos.
Alta	**[24;30]**	A materialização da situação perigosa pode ocorrer várias vezes durante o período de trabalho.
Muito Alta	**[40;70]**	Normalmente a materialização da situação perigosa ocorre com frequência.

4. Nível de Severidade (NS)

Foram considerados cinco níveis de severidade/consequências em que se categorizaram os danos referentes a ativos de informação e os danos referentes a ativo material.

Ambas as categorias podem ser consideradas em conjunto ou independentemente, neste caso tendo sempre mais peso os danos que forem definidos no contexto da gestão de risco.

Quando os danos da informação forem desprezíveis ou inexistentes deve-se considerar os danos materiais no estabelecimento das prioridades.

Há que ter em conta que, no que se refere a severidade/consequência dos incidentes/eventos, apenas se consideram os que forem normalmente esperados em caso de materialização do risco. O nível de severidade do dano refere-se ao dano mais grave que é razoável esperar de um incidente envolvendo a ameaça avaliada.

A tabela que se segue enquadra a avaliação num determinado nível de severidade:

Nível de Severidade	***NS***	*Significado*	
		Danos na informação	*Danos Materiais*
1. Insignificante	**10**	Pequenas perdas de informação, sem qualquer impacto.	Pequenas perdas materiais
2. Leve	**25**	Pequenas perdas de informação, com ligeiro impacto.	Reparação sem necessidade de paragem do processo ou actividade.
3. Moderado	**60**	Perda de informação que pode ser recuperavel.	Para efetuar a reparação, requer a paragem do processo ou actividade.
4. Grave	**90**	Perda informação que podem ser irrecuperavel ou irreparaveis.	Destruição parcial do sistema (reparação complexa e onerosa).
5. Catastrófico	**155**	Perda de informação total e/ou pernamente.	Destruição total do sistema (difícil renovação ou reparação).

5. Nível de Risco (NR)

O nível de risco é o resultado do produto do nível de probabilidade pelo nível de severidade (consequências) [72][73][74]:

Nível de Risco (NR) = Nível Probabilidade (NP) x Nível Severidade (NS)

Sendo o resultado apresentado na tabela a seguir (anexo F.5 – MPDSIOS - Níveis de Risco):

Nível de Risco (NR) = NP x NS A matriz do nível de risco indica a prioridade de intervenção, a qual é expressa em cinco níveis. (Fonte: "Avaliação de Riscos" de Cristina P Amador)		- Não é de esperar que a situação perigosa se materialize, ainda que possa ser concebida.		- A materialização da situação perigosa pode ocorrer.		- A materialização da situação perigosa é possivel de ocorrer pelo menos uma vez com danos.		-A materialização da situação perigosa pode ocorrer várias vezes durante o período de trabalho.		- Normalmente a materialização da situação perigosa ocorre com frequência.	
Danos na Informação e/ou materiais	**NS \ NP**	**1 a 3**		**4 a 6**		**10 a 18**		**24 a 30**		**40 a 70**	
- Pequenas perdas de informação, sem qualquer impacto. - Pequenas perdas materiais	**10**	V 10	V 30	V 40	V 60	V 80	IV 180	IV 240	IV 300	III 400	III 700
- Pequenas perdas de informação, com ligeiro impacto. - Reparação sem necessidade de paragem do processo ou actividade.	**25**	V 25	V 75	IV 100	IV 150	IV 200	III 450	III 600	III 750	III 1000	II 2400
- Perda de informação que pode ser recuperavel. - Para efetuar a reparação, requer a paragem do processo ou actividade.	**60**	V 60	IV 180	IV 240	III 460	III 480	III 1080	II 1440	II 1800	II 2400	I 4200
- Perda informação que podem ser irrecuperavel ou irreparaveis. - Destruição parcial do sistema (reparação complexa e onerosa).	**90**	IV 90	IV 270	III 360	III 540	III 720	II 1620	II 2160	II 2700	I 3600	I 6300
- Perda de informação total e/ou pernamente. - Destruição total do sistema (difícil renovação ou reparação)	**155**	IV 155	III 465	III 620	III 930	II 1240	II 2790	I 3720	I 4650	I 6200	I 10850

6. Nível de Controlo (NC)

Da análise da matriz de níveis de risco caracterizam-se diferentes níveis de intervenção ou de controlo (NC) [72][73][74].

O nível de controlo pretende dar uma orientação para implementar programas de eliminação ou redução de riscos atendendo à avaliação do custo - eficácia.

E que pode apresentar-se na tabela a seguir (anexo F.6 – MPDSIOS - Níveis de Controlo):

Nivel de Risco (NR)		*Nível de Controlo (NC)*	*Significado*
[3600; 10850]	**Muito Alto**	**I = 1**	Situação Critica. Intervenção Imediata. Eventual paragem imediata. Isolar o perigo até serem adotadas medidas de controlo permanentes.
[1240; 3100]	**Alto**	**II = 2**	Situação a Corrigir. Adotar medidas de controlo enquanto a situação. Perigosa não for eliminada ou reduzida.
[360; 1080]	**Médio**	**III = 3**	Situação a melhorar. Deverão ser elaborados planos ou programas documentados de intervenção.
[90; 300]	**Baixo**	**IV = 4**	Melhorar se possível justificando a intervenção
[10; 80]	**Muito Baixo**	**V = 5**	Intervir apenas se uma analise mais pormenorizada o justificar.

No caso dos valores não constantes nos intervalos deve-se considerar o cenário a medida mais rigorosa [72][73][74].

Anexo J – MPDSIOS – Avaliação Crítica e Construtiva

1. Engº. José Casinhas – Information Security Manager

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

Questionário de Avaliação Crítica e Construtiva

Nome do Perito ou Consultor: JOSÉ MANUEL VIEIRA CASINHA
Função: INFORMATION SECURITY MANAGER *Nº de Anos na Função (ou área SI):* + 15
Formação: LICENCIATURA / MBA / CISA / ISO27001LA ITIL / ISO22301LI *Empresa (Facultativo):* ORS
Data: 2012 / 12 / 06 *Local:* LISBOA

Objetivo

Para finalidade da tese de mestrado em Sistemas e Tecnologias de Informação para Saúde, o presente questionário tem por objetivo formalizar a avaliação critica e construtiva do modelo criado, MDPSIOS (Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde) por peritos ou consultores experientes em implementações e monitorização de SGSI (Sistemas de Gestão da Segurança da Informação), através de resposta aberta a um conjunto de 10 questões e um espaço de conclusão para apreciação global do estado e viabilidade do modelo em causa.

Questionário

Depois de ter acompanhado a apresentação feita sobre o MDPSIOS (não olhando para ferramenta em que esta atualmente suportado, '.xls'), gostaria de obter a sua avaliação e opinião critica e construtiva, sobre:

1. – O conceito utilizado?

O conceito utilizado divirá das vista clara das várias fases do PDCA, contudo, a primeira iteração que consiste na implementação do SGSI não está claramente evidenciada as tarefas já executadas das tarefas que faltam executar

2. – Estrutura geral do modelo?

O modelo geral apresentado esta na sua maioria alinhado com os requisitos com a norma ISO27001, contudo sugiro a consulta da ISO27003 que especifica claramente os passos que devem ser seguidos na implementação de um SGSI.

Aluno: Francisco Vilhena A Carvalho – (Aluno nº 9705057)
Orientador: Prof. António Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Lectivo 2011 / 2012

Página 1 de 3

Eng.º José Casinhas - Página 1 de 3

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Políticas de Segurança da Informação em Organizações de Saúde.

3. – Cumpre com os requisitos necessário e essências de um SGSI?

No geral cumpre, mas apresenta alguns aspectos que tem que ser melhorados como sejam a inclusão na SOA além dos controlos do anexo A, os Requisitos regulatórios, de clientes ou outros que influenciem o SGSI

4. – Apresentação e *Layouts* do modelo?

Apresenta um grande trabalho de sistematização, mas em termos de formalidades requeridas no controlo e gestão da documentação não está claro a sua adequação

5. – Apresenta uma abordagem intuitiva na sua utilização?

Não é assim muito intuitiva a utilização pois existem deles que contêm demasiada informação o que torna pouco prático a sua utilização

6. – Funcionalidade do Modelo?

O princípio está lá, a abordagem apontada no PDCA, mas pode ser influenciada recorrendo à ISO 27003 que já tem uma abordagem de implementação do SGSI

7. – Aspetos positivos?

É uma abordagem bastante portável uma vez que só depende do excel

8. – Aspetos negativos?

Num sistema de Gestão é primordial o controlo de Registos, atuais e passados/obsoletos na aplicação apresentada não vão ao encontro de tal visto esta funcionalidade, sendo este um modelo documental parece-me que falta.

9. – Têm algo de novo que não conheça, alguma inovação?

O facto de utilizar o excel para todos os aspetos parece-me inovador

10. – É uma ajuda ou simplifica a implementação de um SGSI em qualquer organização?

Como ferramenta ajuda, mas implementar um SGSI deverá ser feito por profissionais qualificados porque a ferramenta por si só não resolve deverá ser recorrer a ISO 27001 Lead Auditor e/ou ISO 27001 Lead implementer.

Aluno: Francisco Vilhena A Carvalho – (Aluno nº 9705057)
Orientador: Prof. António Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Lectivo 2011 / 2012

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

Conclusão:

A ideia e o conceito parecem-me robustos com a base de conhecimento que foi utilizada, isto é, recorrendo à norma ISO 27001 no seu texto. Não sei se a abordagem que foi seguida seria a mesma se o aluno tivesse contactado com a norma ISO27003, pois esta norma apresenta as "regras" orientadoras do SGSI com as várias tarefas definidas por cada fase, identificando os inputs e outputs de cada tarefa.

Do ponto de vista da sua especificidade, em organizações de Saúde foi bem identificado o capítulo da família ISO 27000 para este sector, mas para tornar este sistema mais adequado questões regulamentares do sector deverão ser incorporadas no sistema de gestão pois parecem-me muito relevantes.

Nas questões relacionadas com o negócio, considero que existe oportunidade e o excel parece-me bem flexível e adaptável / [illegible] é preciso ter cuidado com as questões de segurança do próprio excel sob pena de uma inadequada gestão do controlo de acesso colocar em causa todo o trabalho e um sistema. Isto é um desafio!!! especialmente se houver intenção de certificação por entidade externa.

Para finalizar denota esforço e trabalho por parte do aluno e este claramente um trabalho acima da média que deverá ser melhorado com inputs de profissionais da indústria com experiência de implementação e de gestão de sistemas de segurança.

Bom Trabalho

Os meus agradecimentos pela atenção e disponibilidade prestada.

2. Engº. Luis Martins – *Business Unit Manager - Governance, Risk and Compliance*

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

Questionário de Avaliação Crítica e Construtiva

Nome do Perito ou Consultor: Luis Martins
Função: Business Unit Manager *Nº de Anos na Função (ou área SI):* 13
Formação: Information Security *Empresa (Facultativo):* GLINTT
Data: 11/12/2012 *Local:* Beloura

Objetivo

Para finalidade da tese de mestrado em Sistemas e Tecnologias de Informação para Saúde, o presente questionário tem por objetivo formalizar a avaliação critica e construtiva do modelo criado, MDPSIOS (Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde) por peritos ou consultores experientes em implementações e monitorização de SGSI (Sistemas de Gestão da Segurança da Informação), através de resposta aberta a um conjunto de 10 questões e um espaço de conclusão para apreciação global do estado e viabilidade do modelo em causa.

Questionário

Depois de ter acompanhado a apresentação feita sobre o MDPSIOS (não olhando para ferramenta em que esta atualmente suportado, '.xls'), gostaria de obter a sua avaliação e opinião critica e construtiva, sobre:

1. – O conceito utilizado?
   O conceito utilizado parece-me adequado ao fim a que se destina.

2. – Estrutura geral do modelo?
   A estrutura geral do modelo está bem desenhada e aparenta ser flexível e fluída.

Aluno: Francisco Vilhena A. Carvalho – (Aluno nº 9705057)
Orientador: Prof. António Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Lectivo 2011/2012

Página 1 de 3

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

3. – Cumpre com os requisitos necessário e essências de um SGSI?

SIM, ENGLOBA DE UMA FORMA GERAL TODOS OS REQUISITOS DE UM SGSI.

4. – Apresentação e *Layouts* do modelo?

A APRESENTAÇÃO PARECEU-ME AINDA ALGO CONFUSA E OS LAYOUTS PODEM SER MELHORADOS E CRITERIOS VISUAIS.

5. – Apresenta uma abordagem intuitiva na sua utilização?

DE UMA FORMA GERAL SIM MAS PODE SER MELHORADO.

6. – Funcionalidade do Modelo?

APRESENTA UMA BOA FUNCIONALIDADE COM BASTANTE POSSIBILIDADE DE MELHORIA.

7. – Aspetos positivos?

A CONGREGAÇÃO DE INFORMAÇÃO PODE CONSTITUIR-SE COMO UMA AJUDA MUITO SIGNIFICATIVA PARA QUALQUER ORGANIZAÇÃO QUE EQUACIONE A IMPLEMENTAÇÃO DE UM SGSI.

8. – Aspetos negativos?

ALGUMA IMATURIDADE NA APRESENTAÇÃO E LAYOUTS. PODE E DEVE INCLUIR UMA PERSPECTIVA QUANTITATIVA QUE PERMITA AO DECISOR UMA NOÇÃO DA DIMENSÃO FINANCEIRA.

9. – Têm algo de novo que não conheça, alguma inovação?

A INOVAÇÃO QUE PODERIA IDENTIFICAR PRENDE-SE COM A CONGREGAÇÃO E ORGANIZAÇÃO DA INFORMAÇÃO NUM ÚNICO PONTO.

10. – É uma ajuda ou simplifica a implementação de um SGSI em qualquer organização?

PARECEU SEM DÚVIDA CONSTITUIR-SE COMO UMA POTENCIAL AJUDA PARA QUALQUER ORGANIZAÇÃO QUE ESTEJA A EQUACIONAR A IMPLEMENTAÇÃO DE UM SGSI.

Aluno: Francisco Vilhena A Carvalho – (Aluno nº 9705057)
Orientador: Prof. Antônio Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Letivo 2011 /2012

Página 2 de 3

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Políticas de Segurança da Informação em Organizações de Saúde.

Conclusão:

O MODELO PROPOSTO, DE UMA FORMA GERAL, COMO O QUE ME FOI APRESENTADO ENQUANTO OBJECTIVO E COM OS REQUISITOS DE UM SGSI.
SUGERE-SE A INCLUSÃO, NAS ITERAÇÕES COM A GESTÃO, DE UMA VALORAÇÃO FINANCEIRA QUE POSSA ENQUADRAR E AJUDAR NA DECISÃO DE AVANÇAR OU NÃO COM A EVENTUAL IMPLEMENTAÇÃO DAS MEDIDAS, INICIATIVAS E/OU CONTROLOS PARA FAZER FACE AOS RISCOS IDENTIFICADOS.
O MODELO TEM CLARA MARGEM PARA MELHORIAS, QUER AO NÍVEL DA ESTRUTURA E ORGANIZAÇÃO, QUER AO NÍVEL DA FACILIDADE DE USO E LAYOUT.
SUGERE-SE AINDA UMA REVISÃO AO GRAFISMO E CORES USADAS, QUE PODEM CONSTITUIR-SE COMO UMA AJUDA E UMA MAIS VALIA NA SUA ADOPÇÃO.
É SEM QUALQUER DÚVIDA UMA ABORDAGEM QUE CONSIDERO DE VALIA E MERITÓRIA DE ACOMPANHAMENTO, SEMPRE QUE POSSÍVEL, COM A EVENTUAL POSSIBILIDADE DE TESTAR O MODELO NUM CONTEXTO EMPRESARIAL REAL.

Os meus agradecimentos pela atenção e disponibilidade prestada.

Aluno: Francisco Vilhena A Carvalho – (Aluno nº 9705057)
Orientador: Prof. António Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Lectivo 2011 /2012

Página 3 de 3

3. Dr. Rui Gomes – *Chief Information Officer (CIO)*

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

Questionário de Avaliação Crítica e Construtiva

Nome do Perito ou Consultor: Rui Jorge Meireles Macedo Correia Gomes

Função:CIO *Nº de Anos na Função: > 15 anos;*

Formação: Doutorando em Gestão; Mestre Informática Médica, Licenciatura Engenharia Electrotécnica

Empresa: Hospital Amadora Sintra

Data: _15___/__01__/_2013 *Local:* Lisboa

Objetivo

Para finalidade da tese de mestrado em Sistemas e Tecnologias de Informação para Saúde, o presente questionário tem por objetivo formalizar a avaliação critica e construtiva do modelo criado, MDPSIOS (Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde) por peritos ou consultores experientes em implementações e monitorização de SGSI (Sistemas de Gestão da Segurança da Informação), através de resposta aberta a um conjunto de 10 questões e um espaço de conclusão para apreciação global do estado e viabilidade do modelo em causa.

Questionário

Depois de ter acompanhado a apresentação feita sobre o MDPSIOS (não olhando para ferramenta em que esta atualmente suportado, '.xls'), gostaria de obter a sua avaliação e opinião critica e construtiva, sobre:

1. – O conceito utilizado?

Depois de uma analise ao documento Estrutura_Geral SGSI V1, verifico que a forma como este documento foi trabalhado tem valor. Está estruturado e embora o modelo PDCA seja uma pequena variante, não estando 100% alinhado com a ISO20001/27002, penso que reflecte um bom trabalho de investigação.

2. – Estrutura geral do modelo?

A estrutura parece bem. Na página 4, a forma como está apresentada, tem informação que sem outro contexto parece pouco dedutível, ou seja, como as informações são cruzadas, de

Aluno: Francisco Vilhena A Carvalho – (Aluno nº 9705057)
Orientador: Prof. António Carvalho dos Santos / Coorientador: Prof. João Almeida
MSTIS - Ano Lectivo 2011 / 2012

Página 1 de 4

Dr. Rui Gomes - Página 1 de 4

onde vem, o que se pretende, etc.. talvez esteja fora de ordem. No final do documento estaria mais enquadrada.

3. – Cumpre com os requisitos necessário e essências de um SGSI?

Eu diria que os estudo é propriamento isso. Nas páginas 5,6,7 é uma "compilação" mais personalizada do que deveriam ser os objetivos da implementação. Neste caso também não está alinhado com os objetivos definidos em 27001/27002. Poderia ter citado por exemplo os objetivos para cada domínio (os tais 11 capitulos), porque cada domínio contém um objetivo de controlo que deve ser atingido, assim como os respectivos controlos (que aparecem mais a frente do trabalho). Neste caso estes devem ser aplicados/optimizados para que se alcancem os objetivos.

4. – Apresentação e *Layouts* do modelo?
   Nada a assinalar. Boa apresentação e maquetes de layout com bom *look & feel*

5. – Apresenta uma abordagem intuitiva na sua utilização?
   _____
_____
_____

6. – Funcionalidade do Modelo?

A dimensão do modelo está bem colocada, que é o que está descrito na 27799 (muito parecida com a 27002), apresentando com um guia funcional de implementação. Todo o esforço na proteção da informação está centrado na confidencialidade, integridade e disponibilidade. Eu não colocaria no mesmo nível estas três características e denominava responsabilização ao invés de responsabilidade/autoria, autenticidade, não-repúdio e credibilidade.
Das páginas 8 até à 26 fiquei confuso com alguma mistura dos conceitos. Onde estão os domínios da norma, estão colocados como objectivos. Depois onde se tem controlo/descrição, há efetivamente a tradução do objetivo do domínio e depois a tradução dos controlos específicos de cada domínio. Os controlos selecionados e razões da sua aplicabilidade são um ponto muito positivo nesta abordagem.

7. – Aspetos positivos?

Das paginas 57 à 66 é mais informativo do que explicativo mas é um excelente valor na recolha de dados. Da pagina 68 até à 79 apresenta a documentação apurada no trabalho, que são:

- controlo de documentos e registos;
- concelho de segurança da informação;
- segurança da informação regulamento interno;
- segurança da informação termo de responsabilidade;
- objetivos do sistema de segurança;
- política de segurança da informação; (duplicado do 3º ???)
- formação e sensibilização das pessoas;
- inventário dos ativos.

8. – Aspetos negativos?

As paginas 27, 28 e 29 parecem iguais às 5, 6 e 7. Não compreendo porque foram duplicadas. A única alteração é a substituição da 27002 por 27799. Na última coluna há uma relação entre os capítulos das normas, exatamente, e mantendo-se a mesma numeração. Não compreendi portanto a mais-valia disto, seria talvez para aceder diretamente a ISO27XXX?
Das páginas 30 até à 53 corresponde o mesmo da 8 a pagina 26. Parece-me que como a 27799 tem 35 controlos e a 27001/27002 tem 133, onde existem os respectivos controlos da primeira, simplesmente são repetidos os controlos da 27002. A razão desta duplicidade, não sei.

9. – Têm algo de novo que não conheça, alguma inovação?

Na apresentação do projecto pelo aluno pareceu-me haver uma temática que desconhecia. Contudo, do documento que me foi disponibilizado e que estudei os temas são todos conhecidos.

10. – É uma ajuda ou simplifica a implementação de um SGSI em qualquer organização?

Sem qualquer duvida. Extremamente útil e uma ferramenta valiosíssima. Deveriam ser mapeados as matrizes para uma solução efectiva de Controlo Audit como a MODULO Security; Symantec, ou outra…etc..

Mestrado em Sistemas e Tecnologias da Informação para a Saúde
Instituto Politécnico de Coimbra
Escola Superior de Tecnologia da Saúde de Coimbra – Instituto Superior de Engenharia de Coimbra

Tese: - Modelo Documental para Politicas de Segurança da Informação em Organizações de Saúde.

Conclusão:

O trabalho está muito orientado para a documentação, e tal como o nome indica "Modelo Documental para a Política de Segurança da Organização em Organizações de Saúde". É útil, pertinente e matéria essencial para a implementação de um modelo documental de SGSI. Faltaria um modelo para a implementação das políticas, mecanismos de controlo e a gestão desses mesmos mecanismos de controlo Mas parece-me insignificante face ao bom trabalho que já foi preconizado pelo aluno.