Framework de Gestão de Segurança da Informação para Organizações Militares Orientada pelos Principais Vetores de Ataque

José Martins[1], Henrique dos Santos[2], Paulo Nunes[3], Rui Silva[4]

[1] Academia Militar – CINAMIL, Lisboa, Portugal
jose.carloslm@gmail.com

[2] Universidade do Minho – DSI, Guimarães, Portugal
hsantos@dsi.uminho.pt

[3] Academia Militar – CINAMIL, Lisboa, Portugal
pfvnunesam@gmail.com

[4] Lab UbiNET/IPBeja, INESC-ID, Beja, Portugal
rs.beja@gmail.com

RESUMO

Este artigo pretende responder à questão: Quais são as mais relevantes dimensões e categorias de controlos de segurança da informação a aplicar nas organizações militares em ambiente de Guerra de Informação e de que forma a doutrina militar em vigor limita ou promove a aplicação das normas de segurança da informação disponíveis? Deste modo, propõe-se uma *framework* de gestão de segurança da informação para unidades militares, orientada para a proteção deste tipo de organizações face aos principais vetores de ataque à informação e aos Sistemas de Informação. Numa primeira fase da investigação, através da utilização do método de investigação *focus group* percecionam-se as principais dificuldades e os fatores considerados fundamentais para o sucesso na gestão da segurança da informação nas unidades, estabelecimentos e órgãos militares do Exército Português. Numa segunda fase da investigação propõe-se a *framework* de gestão de segurança da informação que vai possibilitar aos decisores militares planear de modo racional e sistemático os controlos de segurança a aplicar nas unidades militares e integrar as diferentes dimensões da segurança da informação.

Palavras Chave: Segurança da Informação Militar, Gestão da Segurança da Informação, Segurança de Sistemas de Informação, Dimensões e Categorias de Controlos de Segurança da Informação.

1. Introdução

A *North Atlantic Treaty Organization* (NATO) define segurança da informação **"***como parte da segurança das operações (OPSEC), cujo objetivo da segurança da informação (INFOSEC) é proteger a informação (armazenada, processada ou transmitida), bem como os sistemas que a suportam, contra a perda de confidencialidade, integridade e disponibilidade, por meio de uma variedade de controlos processuais, técnicos e administrativos. A INFOSEC inclui uma série de medidas de rotina que são aplicadas sob os auspícios da política de segurança para proteger a informação" (AAP-6, 2009, p. 174).*

No entanto, de acordo com os novos conceitos de doutrina militar da NATO o que se pretende garantir, com o contributo da INFOSEC é a *information assurance*, que tem como objetivo central contribuir para a obtenção da superioridade de informação no domínio militar. A *information assurance* segundo a doutrina militar dos EUA, pode ser definida como "*as Operações de Informação que protegem e defendem os Sistemas de Informação e a informação, garantindo a sua disponibilidade, integridade, autenticação, confidencialidade e não-repúdio*" (JP3–13, 1998, pp. GL-7).

Da revisão de literatura efetuada por Martins e Santos (2010) e do *focus group* realizado com especialistas militares não se identifica a existência ou a aplicação de um método de segurança ajustado aos desafios colocados pelo ambiente de Guerra de Informação, suficientemente estruturado para permitir obter uma visão integrada de gestão de segurança da informação para as unidades militares, face aos principais vetores de ataque à informação e aos Sistemas de Informação (SI).

A não identificação de uma visão clara (não implicando necessariamente a sua inexistência) e simultaneamente a relevância do assunto, resultaram no âmbito da investigação em curso neste domínio, na proposta de uma *framework* de segurança da informação para o exército português, que possa contribuir futuramente para o desenvolvimento de um método de segurança da informação e de uma possível doutrina de segurança da informação e de SI (e de cibersegurança) para o Exército Português.

A *framework* de gestão de segurança da informação proposta para as unidades militares, identifica e estrutura de modo integrado as principais dimensões e categorias de controlos que garantem a segurança da informação.

As dimensões e categorias apresentadas têm por base fundamentalmente a norma internacional ISO 27001 e as normas de segurança da NATO, as quais resultam da sua experiência na mitigação do risco em segurança da informação e de SI. Para a estruturação desta *framework*, contribuem também os trabalhos conduzidos no contexto do *focus group* realizado e um estudo exploratório de Martins, Santos e Nunes (2009), elaborado com o objetivo central da construção de uma *framework* de segurança para SI.

De modo a responder à questão central de investigação, o artigo está dividido em quatro secções, a primeira secção apresenta a problemática e enuncia os objetivos principais da sua realização. A segunda secção apresenta as principais limitações e fatores de sucesso na gestão da segurança da informação e SI nas unidades militares, através da realização do *focus group* com especialistas militares de segurança da informação ou de SI. De seguida, na secção três propõe-se a *framework* de gestão de segurança da informação para as unidades, estabelecimentos e órgãos militares do Exército Português. Para finalizar o estudo, apresenta-se na quarta secção, as conclusões do estudo, algumas das limitações do mesmo e trabalhos futuros a realizar.

2. Focus Group

Neste estudo de orientação epistemológica interpretativista, utiliza-se o método de investigação *focus group* (Liamputtong, 2011). Na aplicação do *focus group* foram realizadas duas reuniões com um grupo de seis oficiais do Exército, com experiência de cinco anos, no mínimo, na temática da gestão da segurança da informação ou dos SI. O estudo foi realizado no Instituto de Defesa Nacional, durante os meses de Outubro e Novembro de 2011. As reuniões tiveram como objetivo principal, percecionar algumas das dificuldades e fatores considerados fundamentais para o sucesso na gestão da segurança da informação na organização militar e identificar o modelo ou método atualmente utilizado para realizar a sua gestão.

Para atingir os objetivos propostos foi colocada aos participantes a seguinte questão nuclear: "*Podem falar-me da experiência das vossas organizações (i.e., unidades, estabelecimentos ou órgãos militares do Exército Português) na gestão da segurança da informação e dos SI (e.g. dificuldades, fatores fundamentais para o sucesso, método utilizado)*", questão esta que orientou cada reunião durante aproximadamente duas horas.

Os resultados obtidos do *focus group* justificam a relevância deste assunto no âmbito da organização militar Exército e a sua preocupação permanente e atual com esta temática. Na aplicação deste método de investigação obtiveram-se os seguintes resultados, os quais

contribuem para a construção da *framework* de gestão de segurança da informação e, posteriormente na construção de um método para a gestão da segurança:

- A gestão de segurança da informação deve ter em atenção a cultura da organização militar, onde existe um misto de civis e de militares e entre os militares, de colaboradores do quadro permanente e contratados, com perceções diferentes da segurança da informação e dos SI.
- Embora exista a preocupação com a gestão do risco (PDE5-00, 2007), não se identifica um modelo ou um processo de gestão de segurança da informação suficientemente estruturado e sistemático que integre as diferentes dimensões da gestão da segurança da informação. Utilizam-se fundamentalmente um conjunto de manuais de boas práticas de segurança que resultam da aplicação de normas de segurança militar (RAD280-1, 2003; SEGMIL1, 1986) e de orientações da NATO (segundo site restrito, versão 2.2 de março de 2011), mas sem um carácter impositivo que permita deduzir a existência de indicadores ou métricas de eficiência na segurança da informação. Na organização militar está consolidada a dimensão da segurança física e a gestão da segurança da informação está focada essencialmente na implementação de controlos técnicos de segurança tecnológica (e.g. *firewalls*, antivírus).
- Constata-se que as unidades militares possuem um sistema de gestão orientado por processos (e.g., de acordo com a ISO 9001) ou por normas de execução permanente (NEP). A abordagem utilizada para o planeamento e a implementação da segurança da informação é essencialmente *bottom-up* e deriva principalmente de procedimentos técnicos, sem uma visão global e integrada de todas as dimensões da segurança da informação, comum aos vários níveis da organização militar (i.e., nível estratégico, de gestão e operacional). Existe a perceção nos níveis superiores da organização militar que a segurança da informação é uma área essencialmente de cariz tecnológico, competindo aos "*técnicos*" a identificação dos problemas, o planeamento operacional e a execução das tarefas associadas à gestão da segurança da informação, embora o poder de decisão (e a responsabilidade) esteja centrado nos níveis estratégico e de gestão da organização militar.
- Excetuando o Regulamento de Catalogação e Armazenamento de Informação do Exército (RCAE), não existe um processo definido para a classificação da informação em formato digital e dos ativos críticos na maioria das unidades militares, ou pelo menos evidências que o mesmo seja realizado. Consequentemente, para atingir os objectivos a que nos propomos com o levantamento desta *framework* é obrigatório conhecer em profundidade a organização, bem como os processos que estão formal ou informalmente implementados e ter devidamente levantados e classificados os ativos críticos e a informação nos diversos formatos.
- Constata-se que existem algumas dificuldades na aquisição e consolidação de competências específicas neste domínio, fator que pode condicionar o desenvolvimento de uma eficiente segurança da informação (e.g. na administração de redes de computadores, no desenvolvimento seguro de software, na implementação e manutenção de tecnologias de segurança, na construção e implementação de políticas de segurança da informação). Existe simultaneamente alguma falta de formação e até de consciencialização para a importância crescente da gestão da segurança da informação em muitos quadros situados aos vários níveis da cadeia de comando militar.
- Existe a necessidade de uma taxonomia ou de um modelo para a classificação de incidentes de segurança da informação e de SI. Atualmente não existe nas unidades militares um processo que permita normalizar o registo de incidentes de segurança da informação, a solução dos problemas e a partilha das lições aprendidas pelos colaboradores a todos os níveis da organização.
- Existe a perceção nos participantes do *focus group* de que não existe uma "*receita*" única de segurança da informação, para todas as unidades militares. É unanimemente aceite

pelos intervenientes no *focus group*, a necessidade da existência de *baselines* de segurança da informação, em função da tipificação das unidades militares e dos possíveis cenários de incidentes de segurança da informação. Pode posteriormente ser realizada uma identificação e avaliação do risco de segurança da informação para as exceções.

Em conclusão, embora exista uma preocupação crescente na maioria dos decisores militares com esta temática, constata-se fundamentalmente pelos dados empíricos obtidos do *focus group*, que existe a necessidade de um modelo ou método que garanta um processo comum de gestão de segurança da informação a todas as unidades militares do Exército Português.

Este modelo ou método, deve possibilitar que todos os níveis da cadeia de comando da organização militar possam ter a mesma visão da segurança da informação, de modo a garantir a celeridade na seleção e implementação dos controlos de segurança da informação, de acordo com os possíveis vetores de ataque de um adversário e a consequente operacionalização do princípio militar da *Unidade de Comando*.

3. Gestão de Segurança da Informação

Nesta secção, propõe-se a *framework* de gestão de segurança da informação. A construção desta *framework* é orientada pela necessidade de proteção da organização face aos principais vetores de ataque de um possível adversário. Estes vetores no âmbito da Guerra de Informação e das Operações de Informação podem ser realizados e ter efeitos fundamentalmente a três níveis ou dimensões de atuação, que são predominantemente: um nível físico, um nível da informação e um nível cognitivo (Alberts, Garstka, Hayes, & Signori, 2001; Andress & Winterfeld, 2011; Martins, et al., 2009; Waltz, 1998).

3.1 Norma Internacional de Gestão de Segurança da Informação – ISO / IEC 27001

A norma Internacional ISO/IEC 27001 considera a gestão de segurança da informação, como um processo de gestão estruturado que permite garantir os principais requisitos de segurança da informação, fornecendo um modelo para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) (ISO/IEC27001, 2005). Ao mesmo tempo, fomenta a adoção de uma abordagem por processos, que tem por orientação a utilização de um modelo que permite planear, executar, verificar e atuar sobre todos os processos do SGSI, conhecido como modelo PDCA (*Plan-Do-Check-Act*) (ISO/IEC27001, 2005).

Por análise de conteúdo da norma internacional ISO/IEC 27001, identificam-se na Figura 1 as principais dimensões onde se integram os controlos de segurança que são sugeridos numa perspetiva de auditoria pela norma para garantir a segurança da informação nas organizações.

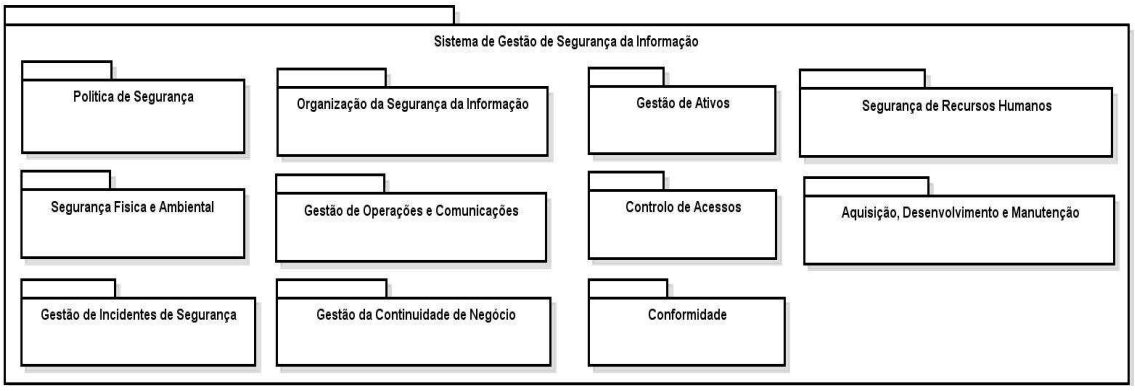


Figura 1 - ISO / IEC 27001 – dimensões de segurança da informação

Estas dimensões de segurança são a principal orientação para o planeamento e a implementação do SGSI, de acordo com a especificidade da organização, quer em termos de requisitos de negócio, quer nas leis e regulamentos que necessita aplicar (ISO/IEC27001, 2005). No entanto, esta norma é demasiado genérica na interligação entre os possíveis incidentes de segurança da informação e os controlos de segurança da informação a aplicar na organização. Em rigor, não possui um modelo ou método que permita orientar a operacionalização do que se deve fazer face a possíveis métodos de ataque de um adversário.

Em conclusão, esta norma tem com objetivo principal a realização de auditorias de segurança da informação e a sua estruturação reflete esse mesmo objetivo, não a sua operacionalização em função dos vetores de ataque de um adversário. É apoiada na seleção dos controlos de segurança da informação a implementar na organização pela ISO 27002, na gestão do risco pela ISO 27005 e na orientação da sua aplicação pela ISO 27003.

3.2 Gestão de Segurança da Informação no Exército Português

As unidades militares do Exército Português suportam a gestão da segurança fundamentalmente através das dimensões apresentadas na Figura 2, obtidas por análise do SEGMIL 1 (1986), documento de segurança militar com a classificação de segurança reservado. O SEGMIL 1, apresenta fundamentalmente os princípios básicos, as normas e os procedimentos destinados a garantir a proteção das matérias classificadas contra possíveis incidentes de segurança, como seja a título exemplificativo ações de sabotagem ou espionagem.

No SEGMIL 1 sobressai a preocupação com a coordenação da segurança e a comunicação dos incidentes de segurança, sendo estas atividades realizadas através de dois canais de comunicação, um hierárquico e outro técnico. Verifica-se também a importância de uma coordenação estreita com os Serviços de Informações (i.e., *intelligence*), os quais são fundamentais na identificação e avaliação do adversário, o que pressupõe o planeamento e a implementação não apenas de controlos de segurança reativos, i.e., uma segurança defensiva, mas também uma segurança ofensiva.

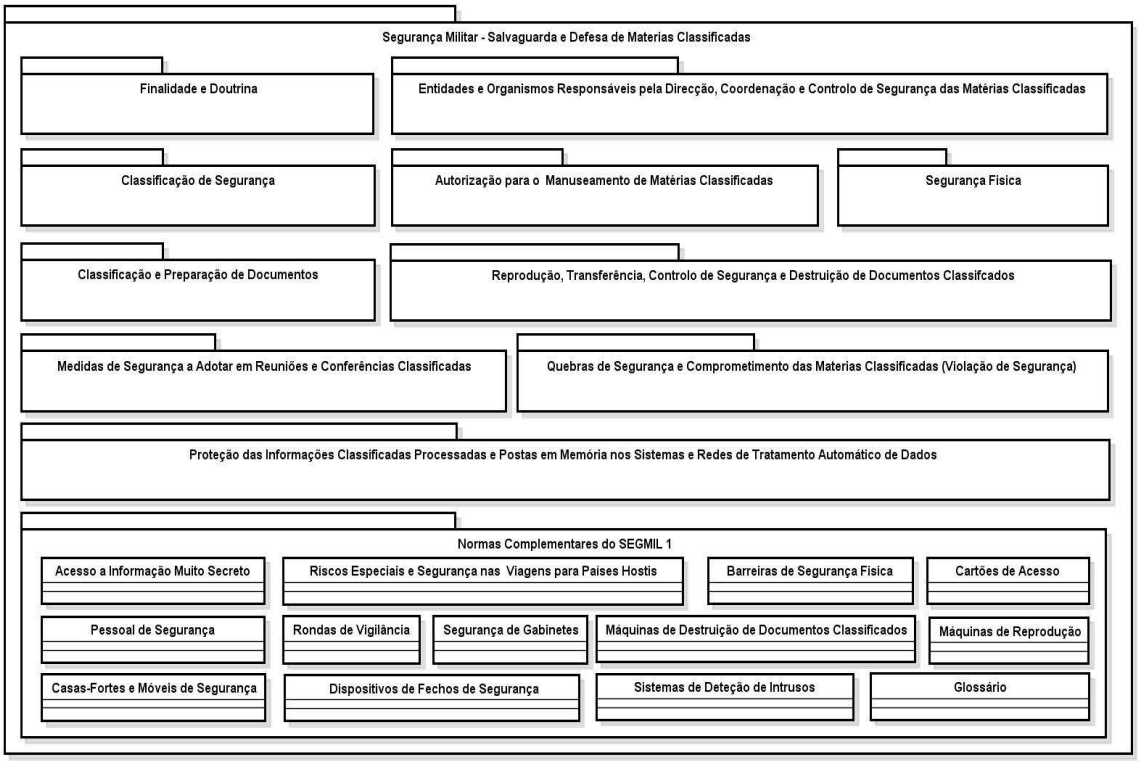


Figura 2 - SEGMIL 1 – dimensões de segurança militar

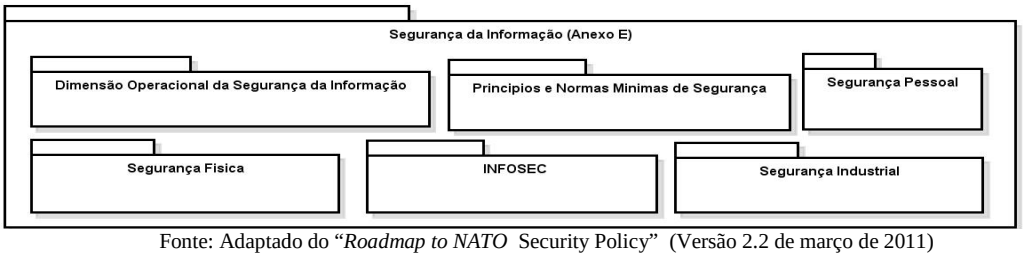
Este documento refere que a segurança é da responsabilidade de todos oficiais, sargentos, praças e funcionários civis. Sendo esta, orientada principalmente pelo princípio da "*defesa em profundidade*", da "*necessidade de conhecer*" e da credenciação do pessoal militar ou civil que necessita de aceder às matérias classificadas.

Nestas instruções, um dos aspetos centrais de planeamento e implementação, é a necessidade de combinar medidas de segurança de diversos tipos e de garantir uma defesa em profundidade, onde a segurança realizada "*sempre que possível deve concentrar-se nos interesses a proteger de forma a poderem beneficiar de uma segurança mais eficaz*" (SEGMIL1, 1986, p. I.2), embora não apresente um modelo ou o processo de planear e realizar essa combinação de medidas.

A segurança militar abordada no SEGMIL 1 centra-se fundamentalmente nas matérias classificadas em suporte físico (e.g. papel) e na dimensão física da segurança. Formaliza os processos para a classificação, o manuseamento, a transferência e a destruição de documentos classificados, bem como os procedimentos para lidar com as quebras de segurança das matérias classificadas.

Da análise das instruções do SEGMIL 1, pode-se constatar que estas não descrevem um processo racional e sistemático, i.e., um método para garantir a seleção dos controlos adequados para proteger a informação classificada em formato digital ou os ativos críticos dos SI que suportam as ações realizadas sobre a informação, interligando os possíveis incidentes de segurança com os controlos de segurança a aplicar, face aos possíveis vetores de ataque de um adversário.

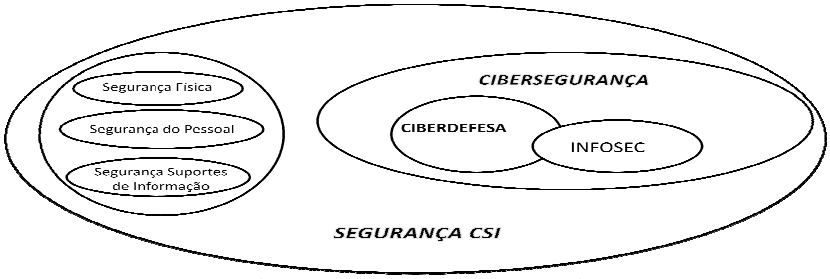
Para além do SEGMIL 1, as unidades militares do Exército Português, têm complementado a gestão da segurança da informação com as normas de segurança definidas na NATO (Figura 3).



Fonte: Adaptado do "*Roadmap to NATO* Security Policy" (Versão 2.2 de março de 2011)

Figura 3 - Segurança da NATO - dimensões de segurança militar

A gestão de segurança da informação deve ser suportada se possível num modelo, o qual possa posteriormente orientar um processo sistemático e racional de efetuar a gestão da segurança da informação. Um dos modelos militares possíveis de utilizar é o modelo atual da NATO de *information assurance* apresentado na Figura 4 e que se prevê que possa orientar nos próximos anos a gestão da segurança da informação e de SI da NATO e consequentemente do Exército Português.



Fonte: Adaptado da *framework* de capacidades de ciberdefesa da NATO (28FEV2011)

Figura 4 - Modelo de i*nformation assurance* da NATO

Neste modelo surgem como principais dimensões de segurança, a dimensão Física, a Pessoal e a Segurança de Suportes de Informação. Existe a dimensão da ciberesegurança a qual integra as dimensões de ciberdefesa e a INFOSEC, sendo esta constituida pela segurança dos computadores e das comunicações. Se em relação à INFOSEC, o assunto está descrito em normas e procedimentos da NATO, a ciberdefesa é perspectivada como resultando da articulação sinérgica entre as *Computer Network Operations (CNO)* e a Segurança dos Computadores (COMPUSEC). Adicionalmente é possível também observar-se uma preocupação com o estado final a atingir, ou seja a segurança das Comunicações e dos SI (CSI).

Em conclusão, constata-se que não existem evidências nos documentos analisados da existência de um método que oriente de forma integrada a gestão de todas as dimensões da segurança da informação. Ou seja, tal como na norma ISO 27001, o SEGMIL 1 e as normas de segurança da NATO não apresentam formalmente a interligação entre os possíveis incidentes de segurança da informação e de SI e os controlos de segurança a aplicar na organização, com a existência de indicadores ou métricas de eficiência dos controlos aplicados.

3.3 Framework Militar de Gestão de Segurança da Informação

No caso da organização militar, a construção da *framework* deve ter fundamentalmente em consideração os vetores de ataque de um adversário e a possibilidade de rigorosa atribuição de responsabilidade aos vários níveis da organização militar.

A *framework* de gestão de segurança da informação para as unidades militares do Exército Português é proposta na Figura 5. As categorias principais de controlos de segurança são identificadas através do método de análise de conteúdo. A sua construção tem por base fundamentalmente a norma internacional ISO 27001 e as normas de segurança da NATO. Simultaneamente consideraram-se as orientações militares indicadas no SEGMIL 1, na norma nacional NIST 800-53 dos EUA (NIST-SP800-53, 2007), na certificação CISSP (Harris, 2008) e em uma *framework* para segurança de SI proposta por Martins et al. (2009).

A correspondência entre os vetores de ataque e as dimensões de segurança é feita tendo em consideração fundamentalmente que ao vetor de ataque físico corresponde a segurança física e ao vetor de ataque cognitivo corresponde a segurança humana. No caso do vetor de ataque ao nível da informação a dimensão fundamental de segurança é a dimensão tecnológica, a qual tem em consideração a segurança lógica, a segurança das redes de computadores, telecomunicações e internet e a segurança na aquisição, desenvolvimento e manutenção de sistemas e software.

No entanto, para garantir a segurança da informação, é necessária uma integração da dimensão tecnológica, com a segurança física e a humana, bem como garantir a eficiente gestão dos processos que garantem a operacionalização das várias dimensões da segurança e a sua integração. Consequentemente, a dimensão organizacional desempenha a função que permite realizar a gestão da segurança da informação ao nível organizacional.

Na *framework* proposta de gestão de segurança da informação, podem-se referenciar na Figura 5 as principais dimensões e categorias de controlos de segurança da informação e de SI a ter em consideração i.e. a Dimensão Organizacional, a Dimensão Física, a Dimensão Humana e por fim a Dimensão Tecnológica. As categorias indicadas na *framework* representam controlos individuais ou conjuntos de controlos de segurança da Informação e de SI (e.g., Politica de Segurança, Controlo de Acessos Físico, Ações de Sensibilização, Tecnologias de Segurança, Análise do Código Fonte).

Os controlos de segurança a selecionar e a implementar resultam fundamentalmente das dimensões e das categorias de segurança propostas na *framework*. Os controlos selecionados e implementados devem ser utilizados para prevenir, detetar, deter, desviar, recuperar ou reagir a um incidente de segurança da informação ou de SI (Dhillon, 2007; Pfleeger & Pfleeger, 2007).

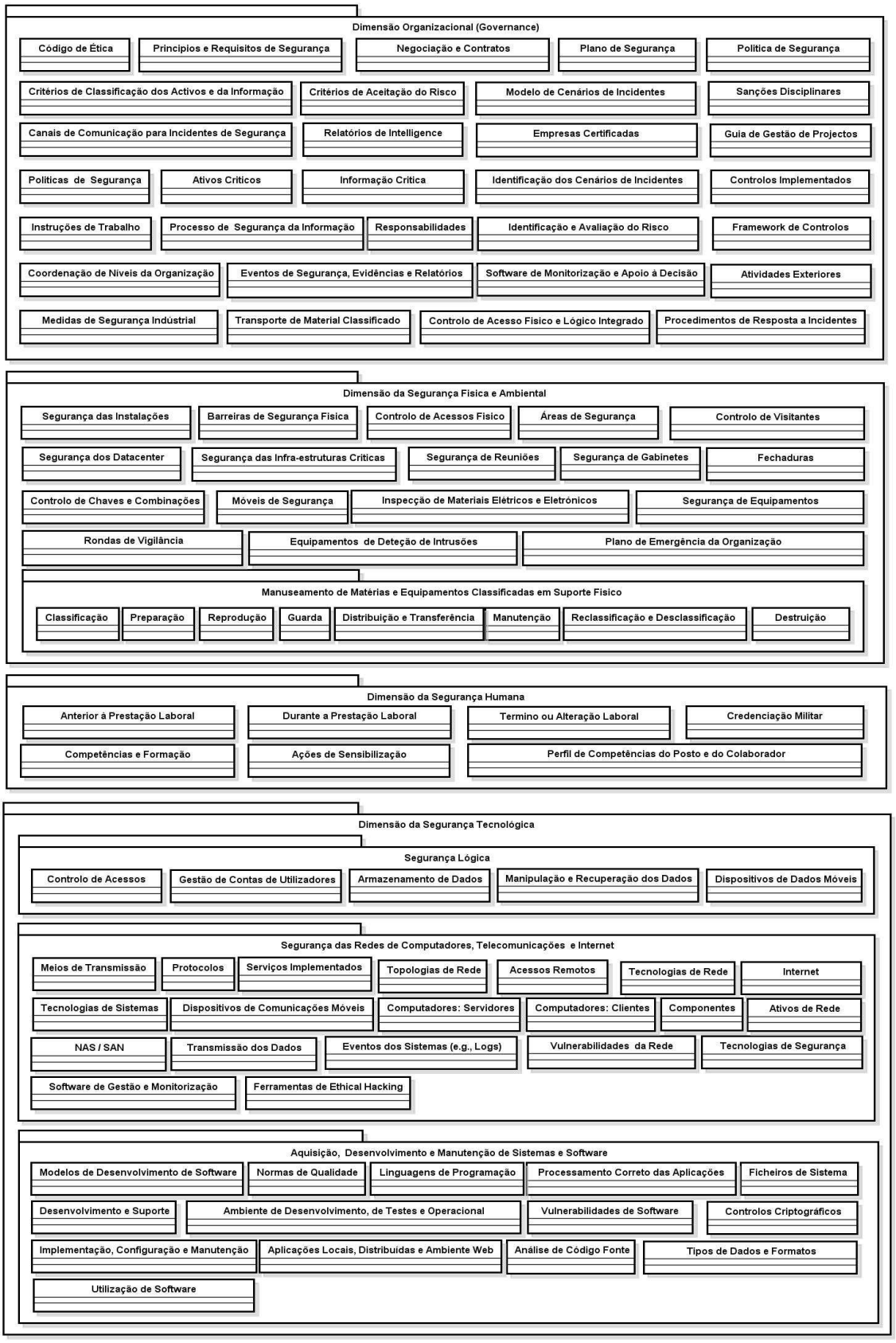


Figura 5 - *Framework* militar de gestão de segurança da informação

No entanto, propõe-se que a sua seleção seja suportada através da aplicação de um modelo de incidentes de segurança da informação e de SI (Martins, Santos, Nunes, & Silva, 2012), o qual permitirá integrar as diferentes dimensões de segurança propostas nesta *framework* com os possíveis métodos de ataque. Esta abordagem permite responder às questões: *o que fazer, porque fazer e como fazer?* Sendo o objetivo principal da *framework* de gestão proposta o de minimizar os riscos de segurança da informação e consequentemente maximizar a segurança da informação ao nível organizacional.

A partir desta *framework* de gestão de segurança da informação, é possível definir e gerir de forma racional e sistemática *baselines* de segurança da informação para as unidades militares tendo em consideração a sua especificidade e todos os possíveis cenários de métodos de ataque definidos através do modelo de incidentes proposto por Martins et al. (2012).

Considera-se que é essencial que as unidades militares do Exército Português possuam uma *baseline* de segurança da informação comum, a qual minimize os riscos de segurança da informação e a partir da qual possam evoluir em termos de maturidade na segurança da informação ou seja na procura da qualidade total em termos de gestão de segurança da informação i.e., zero riscos de segurança da informação.

Os dados empíricos obtidos do *focus group* permitem constatar a importância para as organizações militares das dimensões de segurança da informação apresentadas, bem como a necessidade de possuir uma *framework* de segurança cuja construção é orientada pelos principais vetores de ataque dos adversários e pelos principais cenários de incidentes de segurança da informação,

Em conclusão, constata-se que os controlos de segurança da informação das normas internacionais e das normas militares da NATO e do SEGMIL 1 são na essência semelhantes, embora agrupados de forma diferente nas dimensões de segurança identificadas. A norma internacional ISO/IEC 27001 de gestão da segurança da informação pode contribuir essencialmente na complementaridade dos possíveis controlos de segurança a aplicar e na definição das métricas dos controlos de segurança aplicados nas unidades militares.

A *framework* proposta oferece uma mais fácil perceção das dimensões e das categorias de controlos de segurança da informação, o que sem dúvida permite uma mais fácil integração das dimensões da segurança propostas na resposta a um possível incidente de segurança da informação e a facilidade de escalabilidade, em função do aparecimento de novos métodos de ataque ou de controlos de segurança da informação.

4. Conclusões

Neste estudo, propõe-se uma *framework* de gestão de segurança da informação para as unidades militares do Exército Português, orientada pela necessidade de garantir proteção face aos principais vetores de ataque à informação e aos SI e que tem por base fundamentalmente a norma internacional ISO 27001 e as normas de segurança da NATO.

Perceciona-se também neste estudo, que as principais propriedades da segurança da informação a ser garantidas nas unidades militares são a disponibilidade e a confidencialidade. Sendo que a informação é vista não só numa perspetiva de possível alvo, mas também de arma e que a preocupação da seleção dos controlos de segurança a aplicar é centrada na sua eficácia para evitar a diminuição do potencial de combate ou capacidade para o cumprimento da missão.

A *framework* proposta permite definir futuramente protocolos entre as dimensões de segurança, identificar claramente quais os serviços prestados por cada nível da organização e uma mais fácil monitorização e atribuição de responsabilidades ao longo da cadeia de comando.

Permite simultaneamente orientar a análise e o desenho de um curso de gestão de segurança da informação para as Forças Armadas Portuguesas, pois identifica as principais dimensões e

categorias de controlos de segurança da informação e é um contributo para o planeamento estruturado e sistemático da temática da cibersegurança no Exército Português, pois os fundamentos teóricos principais da cibersegurança são certamente a segurança da informação e dos SI.

Neste estudo, não se identificou a existência ou a aplicação de um modelo ou método de gestão de segurança da informação e de SI para as unidades militares, não se assegurando consequentemente um processo de planeamento racional e sistemático, mas deixando ao critério "*dos técnicos*" da organização ou de consultores externos à organização o planeamento dos controlos de segurança mais eficientes para mitigar o risco identificado.

Neste estudo não foram validadas as categorias de segurança, resultando estas apenas da análise de conteúdo realizada com base nos documentos referidos, ficando consequentemente em aberto a sua validação através de um painel de especialistas e de um Estudo de Caso a realizar numa unidade do Exército Português durante o ano de 2013.

Fica também em aberto para um próximo estudo a proposta de um método de gestão de segurança da informação para as unidades militares do Exército Português, tendo como suporte o modelo de incidentes de segurança da informação apresentado na *11th European Conference on Information Warfare and Security* (Martins et al., 2012) e a *framework* de gestão de segurança proposta. A integração da *framework* com o modelo de incidentes deve permitir minimizar o risco de segurança da informação nas unidades militares e responder às três questões: o que fazer, o porquê e o como fazer?

Para garantir a gestão eficiente da segurança da informação, a responsabilidade é de cada colaborador da organização e é fundamental que todos saibam o que fazer e tenham competências para o fazer.

Referências Bibliografias

AAP-6 (2009). *NATO Glossary of Terms and Definitons*.

Alberts, D., Garstka, J., Hayes, R., & Signori, D. (2001). *Understanding Information Age Warfare, CCRP Publication Series, Washington, United States of America*.

Andress, J., & Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*: Syngress Media Inc.

Dhillon, G. (2007). *Principles of Information Systems Security - Text and Cases*: WILEY.

Harris, S. (2008). *CISSP All-in-One Exam Guide, Fourth Edition, McGraw-Hill, New York, United States of America*.

ISO/IEC 27001 (2005). Information technology – Security techniques – Information Security Management Systems - Requirements.

JP3–13 (1998). *Joint Doctrine for Information Operation, United States of America*.

Liamputtong, P. (2011). *Focus Group Methodology - Principles and Practice*: SAGE.

Martins, J., & Santos, H. (2010). *Methods of Organizational Information Security - A Literature Review.* Paper presented at the 6th International Conference On Global Security, Safety and Sustainability, Braga.

Martins, J., Santos, H., & Nunes, P. (2009). *Security Framework for Information Systems.* Paper presented at the 8th European Conference on Information Warfare and Security, Lisboa.

Martins, J., Santos, H., Nunes, P., & Silva, R. (2012). *Information Security Model to Military Organizations in Environment of Information Warfare.* Paper presented at the 11 th European Conference on Information Warfare and Security, Laval, France.

NIST-SP 800-53 (2007). Information Security. USA.

PDE 5-00 (2007). Planeamento Táctico e Tomada de Decisão: Ministério da Defesa Nacional - Exército Português - Comando da Instrução e Doutrina.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Securiy in Computing, Prentice Hall, 4ª ed, United States of America*.

RAD 280-1 (2003). Segurança da Informação Armazenada, Processada ou Transmitida nos Sistemas de Informação e Comunicação do Exército: Estado Maior do Exército / Exército Português /Ministério da Defesa Nacional.

SEGMIL 1 (1986). *Instruções para a Segurança Militar, Salvaguarda e Defesa de Matérias Classificadas (Reservado), EMGFA, Portugal.*

Waltz, E. (1998). *Information Warfare: Principles and Operations, Artech House.*