Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Segurança de Informação na Estratégia Empresarial - BSC

Estudo de caso

Carmen Lúcia Nunes Marcelino

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientadora: Professora Doutora Maria Leonilde dos Reis

Setúbal, 2014

Não devemos dar a conhecer o local onde queremos combater, para que o inimigo tenha de se preparar para ataques vindos dos mais diversos sítios.

Sun Tzu

Agradecimentos

Antes de mais gostaria de agradecer à minha orientadora, Professora Doutora Maria Leonilde Reis, pela disponibilidade, compreensão, paciência, assertividade e exigência com que encaminhou o trabalho desenvolvido. Um obrigado também às observações construtivas de outros Docentes na fase inicial do plano de dissertação, nomeadamente à Professora Doutora Ana Mendes e ao Professor Doutor Hernani Mourão.

Agradeço também a todos os Professores da parte curricular do Mestrado de Sistemas de Informação, especialmente aos Docentes das disciplinas de Segurança de Informação (Professor Doutor José Gaivéo), de Estratégia em Sistemas de Informação (Professor Doutor José Rascão) e de Inovação, Estratégia e Competitividade (Professor Doutor Silva Ribeiro), com quem tive a oportunidade de aprender grande parte do conhecimento depositado no trabalho desenvolvido.

A família, como sempre, também representou um papel fundamental. Um muito obrigado pela paciência em dias menos bons, pela ajuda que direta ou indiretamente me concedeu e pelo facto de ter sido privada da minha presença em muitas circunstâncias. Um peculiar reconhecimento a quem me forneceu grande parte das informações para o desenvolvimento do estudo de caso.

Por fim, agradeço também aos colegas do primeiro ano de Mestrado, que me auxiliaram fornecendo informação e orientação na fase inicial. Um especial agradecimento ao colega Helder Mira pelo encorajamento também nessa fase.

Índice

Índice de Figuras

Índice de Quadros

Lista de Acrónimos

SI – Sistema de Informação

BSC - *Balanced Scorecard*

HR – *Human Resources*

RH – Recursos Humanos

SGSI – Sistema(s) de Gestão de Segurança da Informação

ISO – *International Standard Organization*

IEC – *International Electrotechnical Commission*

LCAG - Learned, Christensen, Andrews e Guths

SWOT – *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças)

ANECRA - Associação Nacional das Empresas de Comércio e Reparação Automóvel

I&D – Investigação e Desenvolvimento

SOA - *Statement of Aplicability*

Resumo

Vivemos na era da informação e é com base nesta que são tomadas importantes decisões, mas nem sempre lhe é dada a devida importância enquanto recurso estratégico, descurando-se também a área de segurança de informação. A informação é essencial e conduz à aquisição de vantagens competitivas por parte das organizações, o que implica impreterivelmente garantir a sua segurança.

Com este trabalho académico pretendeu-se aferir a importância da segurança de informação na prossecução dos objetivos estratégicos de determinada empresa, cujo desempenho foi medido recorrendo ao *Balanced Scorecard* (BSC), com a respetiva definição de indicadores e ações a tomar para alcançar a visão definida pela empresa.

O BSC foi precedido do mapa estratégico que levou em consideração os objetivos estratégicos, a missão, a visão e valores da entidade alvo de estudo, estabelecendo relações causa-efeito entre os vários objetivos das quatro perspetivas, dando especial ênfase à vertente de segurança de informação.

O estudo teve em linha de conta as boas práticas dos principais referenciais de segurança de informação, nomeadamente a ISO/IEC 27002:2013, que apresenta uma vasta lista de controlos a verificar para que um sistema de gestão de segurança de informação (SGSI) se considere bem implementado.

Como metodologia, recorreu-se à revisão de literatura através da qual se pretendeu evidenciar o estado de arte dos temas abordados, recorrendo tanto a fontes internas como externas. Aplicou-se também o estudo de caso realizado acerca da empresa Motor, procedendo à recolha de materiais empíricos por observação direta e por entrevista.

Através da sua análise pôde-se concluir que a empresa reconhece a importância da informação enquanto recurso intangível de suma importância na prossecução dos seus objetivos. Como tal, o valor da segurança de informação é também reconhecido, já que aplica a maior parte dos controlos da norma ISO 27002:2013 adequados à estratégia. No entanto, será necessário dar maior atenção à sensibilização/formação dos funcionários acerca da temática da Segurança de Informação.

Os tempos são extremamente competitivos e muito facilmente os competidores poderão tentar explorar as imperfeições da informação, tornando-a numa arma letal a nível estratégico. É cada vez mais crucial que a informação crítica de negócio seja protegida.

Palavras-chave: Estratégia, Informação, Segurança de Informação, Mapa Estratégico, *Balanced Scorecard*

Abstract

We live in the information age and important decisions are taken based on that, but it is not always given due importance as a strategic resource, neglecting also the information security area. Information is essential and leads to competitive advantages acquisition for organizations, which implies imperatively ensure their safety.

With this academic work was intended to approach the Information Security importance in the company strategic goals achievement, whose performance was measured using the Balanced Scorecard, which was preceded by the strategic map including the respective indicators and actions taking to achieve the company´s vision.

The BSC was preceded by the strategic map, which considered the company strategic goals, mission, vision and values and established cause-effect relations between the several four perspectives goals, emphasising the security information dimension.

The study considered the principal security information good practices, such as ISO/IEC 27002:2013, that includes a large controls list to verify in order to guarantee a good Security Information System Management implementation.

It was used as a methodology, not only the literature review in these areas, which was intended to show the state of art about the topics, using both internal and external sources, but also the Case Study applied to the company "Motor", using the collection of empirical materials through direct observation and interviews.

Through its analysis it was concluded that the company recognize the information importance as intangible resource in achieving its strategic objectives. The information security value is also recognized in the organization, which applies most part of the ISO 27002:2013 controls according to its strategy. However, it will be necessary to give more attention to the employees training/ awareness in security information thematic.

The circumstances are extremely competitive and rivals easily could try to explore the information imperfections, making it a lethal weapon on the strategy significance. The business critical information should be more and more protected.

Keywords: Strategy, Information, Information Security, Strategy Maps, *Balanced Scorecard*

1. Introdução

Neste capítulo pretende-se apresentar de uma forma global em que consiste este trabalho académico. Estando dividido em cinco partes, a primeira é uma breve apresentação do tema, seguindo-se a problemática que deu origem ao estudo, assim como os objetivos e metodologia do trabalho, e por fim, a forma como o presente documento está estruturado.

1.1. Contextualização do Tema

Vivemos presentemente na era da informação, numa economia que é permanentemente alimentada pela partilha de conhecimento, de tal forma que passaram a existir empresas detentoras de redes sociais que prestam este serviço à sociedade em geral de forma gratuita, apenas com o intuito de recolher informação preciosa ao desenvolvimento de ferramentas de *webmarketing* personalizado que são um verdadeiro sucesso de vendas.

A disponibilização da informação em tempo útil pode transformar-se numa arma letal, quando bem utilizada contra os concorrentes, já que e é com base nesta que são tomadas decisões importantes no que concerne às mais variadas áreas da gestão.

Porém, nem sempre lhe é dada a devida importância enquanto recurso estratégico, que deverá estar sempre disponível, de forma íntegra e atempada. É neste sentido que se torna imperativo proteger este recurso valioso, seguindo as boas práticas existentes na área de segurança de informação e definindo métricas que auxiliem na sua avaliação de desempenho.

Segundo Gaivéo (2009) a informação é essencial a uma tomada de decisão eficaz e conduz à aquisição de vantagens competitivas por parte das organizações, o que implica impreterivelmente garantir a segurança dessa mesma informação.

A informação poderá permitir alcançar vantagem estratégica quando bem utilizada e salvaguardada, como também se poderá revelar uma desvantagem quando desperdiçada ou transmitida a potenciais inimigos, seja de forma negligente ou intencionalmente. Este dano torna-se crescente quando associado à velocidade com que a informação circula, podendo “cair nas mãos erradas”, como sucedeu no célebre caso do *wikileaks*.

1.2. Problemática

A informação atempada permite às organizações obter posições estratégicas benéficas, embora muitas não reconheçam o poder deste valioso recurso. Outras empresas constatam a relevância da informação enquanto recurso intangível de suma importância na prossecução da sua visão, missão e respetiva estratégia, assim como o valor da Segurança de Informação. No entanto, no tecido empresarial em muitas circunstâncias alocam-se os recursos que se têm ao dispor a outros fins entendidos como prioritários.

Segundo Ferreira (2010), citando Reis (2001), é preciso dar importância relativamente ao facto de várias organizações correrem riscos mal avaliados, por não se aperceberem do valor da informação crítica de negócio.

Torna-se então necessário evidenciar alguns riscos a que a informação crítica de negócio está exposta e entender como poderá esta ser salvaguardada, ou seja, investigar que atividades deverão ser alvo de controlo em termos de desempenho. Só por esta via se conseguirá demonstrar qual a importância que a segurança da informação poderá ter em termos de estratégia de negócio, igualando assim ou até mesmo superando as tais demais tarefas entendidas como prioritárias.

1.3. Objetivos

Pretende-se com o presente trabalho identificar quais as atividades críticas de negócio tendo em consideração a missão, visão, valores e os objetivos estratégicos a atingir pela empresa. Após selecionar as atividades críticas de negócio, pretende-se perceber de que forma estas poderão estar ameaçadas, revelando em simultâneo algumas vulnerabilidades, o que permitirá concluir acerca dos objetivos de Segurança de Informação e controlos da ISO 27002:2013 a aplicar. Por fim, proceder-se-á à elaboração do mapa estratégico, a partir do qual se definirão alguns indicadores e metas, que deverão ser alvo de monitorização através da ferramenta estratégica do BSC, que avaliará a sua *performance*.

Após esta análise, conforme é sugerido pelo título do trabalho, pretende-se investigar como a segurança de informação poderá influenciar a estratégia da empresa, tendo em consideração também as restantes perspetivas do BSC.

Este trabalho de investigação pretende então atingir os seguintes objetivos:

- Avaliar a importância dada à segurança de informação como elemento essencial na prossecução dos objetivos estratégicos da empresa;
- Fazer uma adequada valorização das atividades chave para o negócio;
- Revelar algumas vulnerabilidades e ameaças;
- Selecionar os controlos a aplicar, por forma a garantir o nível de segurança necessário à informação crítica de negócio;
- Demonstrar como se pode salvaguardar informação relacionada com o *cuore business* da empresa;
- Medir o desempenho dessas ações;
- Evidenciar o peso da segurança de informação na estratégia da empresa.

1.4. Metodologia

Existem diversas formas de conduzir uma investigação. Porém, a escolha daquela que será a mais indicada deverá ser feita depois de conhecermos todas as alternativas e irá depender dos objetivos e do contexto da investigação. A forma como são colocadas as questões iniciais de investigação e outros factos ajudarão a determinar qual a melhor opção. A figura 1 evidencia as principais alternativas que poderão ser consideradas no momento de decidir o método mais adequado de investigação.

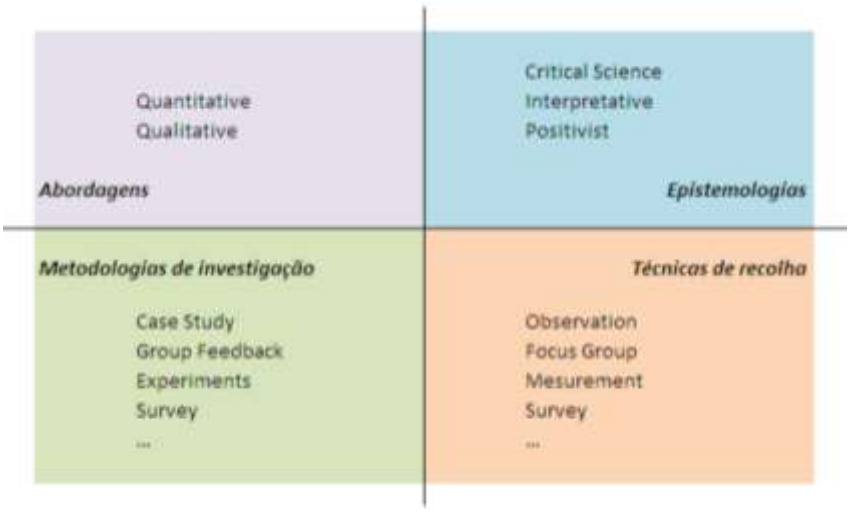

Figura 1 – Elementos de investigação em Sistemas de Informação (SI)

Fonte: "Investigação em Sistemas de Informação Organizacionais – Teses e Dissertações em Portugal", Grilo, 2008: 16

No que se relaciona com o tipo de abordagem, esta poderá ser qualitativa ou quantitativa. A primeira diferencia-se da segunda porque enfatizando questões sociais, permite estudar a interação das pessoas em determinado contexto, por exemplo organizacional.

Segundo Grilo (2008:17) "métodos de investigação quantitativa foram originalmente desenvolvidos em ciências naturais para o estudo de fenómenos naturais. Exemplos de métodos quantitativos são os *Survey, Experiments, Formal Methods* e *Numeric Methods*, em que os dados são recolhidos através de inquéritos, medições ou métodos matemáticos conhecidos, como é o caso de modelação".

Grilo refere também que "métodos de investigação qualitativa foram desenvolvidos em ciências sociais, para permitir aos investigadores o estudo de fenómenos sociais e culturais. São exemplos de métodos qualitativos *Action Research, Case Study* e Ethnography, onde as origens de dados qualitativos incluem observação, trabalho de campo, entrevistas ou documentos".

O autor refere também que o intuito das investigações em SI tem enfatizado cada vez mais questões relacionadas com a gestão em si, em detrimento de questões tecnológicas, o que poderá

explicar a preferência por métodos qualitativos. Na seguinte figura é possível visualizar o tipo de questão que é respondida em cada um dos métodos.

	Abordagem Qualitativa	Abordagem Quantitativa
1	O que é que os meus informadores sabem sobre a sua cultura que eu possa descobrir?	O que é que eu sei sobre um problema que me permitirá formular e testar uma hipótese?
2	Que conceitos os meus informadores usam para classificar as suas experiências?	Que conceitos posso usar para testar esta hipótese?
3	Como é que os meus informadores definem estes conceitos?	Como consigo definir estes conceitos de forma operacional?
4	Que teoria popular os meus informadores usam para explicar as suas experiências?	Que teoria científica pode explicar os dados?
5	Como deverei traduzir o conhecimento cultural dos meus informadores, de forma a criar uma descrição cultural e que seja possível os meus colegas perceberem?	Como deverei interpretar os resultados para posteriormente apresentá-los na linguagem que os meus colegas usam?

Figura 2 – Contraste de Axiomas nas Abordagens

Fonte: "Investigação em Sistemas de Informação Organizacionais – Teses e Dissertações em Portugal", Spradley, 1979, citado por Grilo, 2008: 16

Designa-se por triangulação a aplicação das duas abordagens em simultâneo, o que é pouco comum, pois normalmente opta-se apenas por uma delas. No entanto, uma vez que têm pressupostos bastante distintos, isto poderá enriquecer a obtenção de resultados numa investigação.

"A produção de conhecimento através da investigação pode ser definida como uma atividade que contribui para a compreensão de um fenómeno" (Lakatos 1978, citado por Grilo, 2008:13). Assim, do ponto de vista organizacional torna-se substancialmente mais enriquecedor estudar o fenómeno no seu contexto.

Gummesson (1991:4) argumenta que "metodologias qualitativas fornecem ferramentas poderosas no estudo e investigação em gestão e administração empresarial", enfatizando que este tipo de método tem a sua origem na psicologia, sociologia, educação, antropologia/etnografia e por isso é rico em exemplos de estudo da sociedade em geral. O autor refere também que "este tipo de pesquisa deveria ser inspiradora para qualquer gestor enquanto cidadão preocupado e não somente enquanto homem de negócios", já que se está a lidar com a vida humana em diferentes tipos de cenários, com diferentes objetivos e perspetivas. É também salientado o facto de que os estudos em gestão têm como intuito compreender ou melhorar o desempenho organizacional e podem ser feitos com o fim de fornecer recomendações/soluções para determinados problemas, o que se aproxima de um trabalho de consultoria.

Existem várias metodologias que se podem utilizar, algumas delas referenciadas na figura 1. No entanto, a mais utilizada no âmbito dos SI´s é a do *Case Study*, que é uma metodologia caracteristicamente qualitativa e permite estudar os processos que lhes estão inerentes e que envolvem sempre questões do foro social, pelo que se considerou ser a mais adequada para o desenvolvimento do trabalho académico em questão.

O estudo de caso é uma investigação realizada no âmbito das ciências sociais, que permite estudar comportamentos associados a determinados fenómenos no seu real contexto, respondendo a questões de "como" ou "porquê", a que outras metodologias de investigação quantitativas não poderiam dar resposta. Recorre-se a este tipo de metodologia principalmente quando não se consegue isolar o fenómeno do seu contexto (Yin, 2009).

Yin (2009) aponta como competências essenciais a deter pelo investigador ser bom ouvinte, colocar boas questões e saber interpretar as respostas, ser flexível para poder encontrar novas pistas, ter domínio do assunto que investiga para se cingir ao que é relevante e deixar de parte ideias pré-concebidas acerca do assunto.

Segundo Yin (2009) o estudo de caso apresenta algumas condicionantes, entre as quais: a impossibilidade de generalizar os resultados obtidos; o facto de o investigador poder ser influenciado por ideias pré-concebidas, o que afetará bastante a sua imparcialidade; a falta de objetividade e rigor e o tempo que poderão demorar a ser desenvolvidos.

Relativamente à epistemologia, disciplina que estuda a ciência e ajuda a compreender melhor como se processa o conhecimento, existem três interpretações diferentes: *Positivist, Interpretative* e *Critical Science.* "A epistemologia *Interpretative*, por contraste a *Positivist*, assenta na tentativa da compreensão de valores, crenças e conceitos de eventos sociais, através de uma perceção profunda e clara de experiencias e atividades humanas de foro cultural" (Smith e Heshusius, 1986, citados por Grilo, 2008). Como tal, considera-se que epistemologicamente o presente estudo é interpretativo, já que se terá em consideração como questões sociais e comportamentais, bem como a própria cultura organizacional, poderão afetar o correto desempenho e utilização de boas práticas.

O *case study* compreende algumas etapas fundamentais. Como se pode evidenciar na seguinte figura de Yin (2009), todas as etapas podem ser repetidas as vezes necessárias, o que poderá ser justificado pelo facto de se aplicarem diversas técnicas de recolha ou simplesmente pelo facto de o investigador considerar insuficientes ou não fiáveis os dados de que dispõe. Por este motivo se afirma que o processo é interativo, podendo por exemplo aquando da condução do estudo de caso propriamente dito, ser necessário voltar atrás inúmeras vezes, com o intuito de adaptar a revisão bibliográfica.

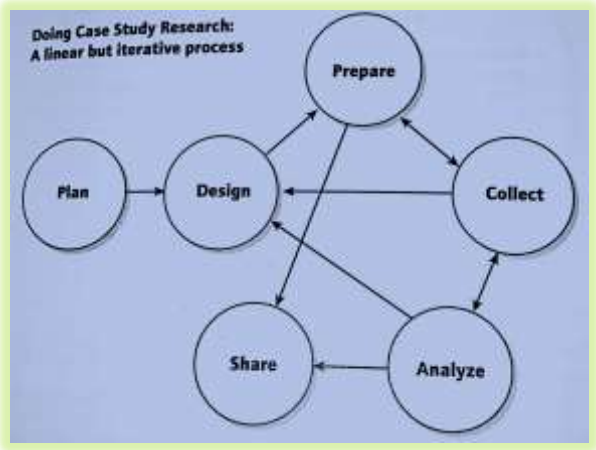

Figura 3 – Processo Interativo de Etapas do Estudo de Caso

Fonte: "Case Study Research – Design and Methods", Yin, 2009:1

O Planeamento envolve a definição das questões de investigação que levarão ao desenvolvimento do trabalho e a decisão pela metodologia do estudo de caso depois de cuidadosamente comparada com outras, tendo sempre presentes os seus pontos fortes e as suas limitações.

A fase de Desenho inclui definir a unidade de análise e o caso provável a ser estudado, selecionar a pertinente teoria que possa suportar o estudo, desenvolver proposições e questões subjacentes que antecipem o estudo, identificar o desenho propriamente dito, ou seja, se será único, múltiplo, holístico ou profundo. Neste caso concreto será um caso único e holístico porque apenas estamos a estudar uma organização, ou seja, somente teremos uma unidade de análise. Isto levará a que possamos considerar o todo pela parte.

Na Preparação há que "afiar" as competências de um investigador, já tendo sido referidas acima algumas delas, treinadas de forma a responder às necessidades de um *case study* específico. É também nesta etapa que se desenvolve o protoloco a seguir, incluindo a triagem de candidatos a entrevistar. É também aconselhado por Yin (2009) uma leitura preparatória de outros estudos de caso já realizados acerca da temática, tendo sido selecionado o do autor Ferreira (2010) como principal, entre outros mencionados na bibliografia. Na preparação escolhem-se as técnicas de recolha de dados mais adequadas.

De acordo com Yin (2009) na metodologia de estudo de caso existem pelo menos seis formas de recolha de dados: a documentação, registos, entrevistas, observação direta ou participativa e artefactos físicos. As entrevistas representam uma das principais fontes de recolha de informação, podendo ser abertas ou não estruturadas, focadas e estruturadas. A observação direta é uma fonte imprescindível já que o estudo de caso implica estudar o fenómeno no seu contexto real.

A metodologia a utilizar neste trabalho de dissertação será baseada na recolha de informação empírica através de entrevistas e observação direta e também na seleção de informação/documentação publicada nos sites da entidade e do grupo. Nas entrevistas recorrer-se-á ao apoio de questionários de resposta aberta. A observação direta será feita recorrendo ao apoio de *checklists*, que serão elaboradas com base nos controlos das normas de boas práticas. O encadeamento desta metodologia pode ser evidenciado na figura 4.

Figura 4 - Metodologia de Pesquisa

Depois da preparação, conduz-se a recolha de dados propriamente dita na qual é recomendado seguir o protoloco definido, usar várias fontes de evidência, criar uma base de dados e manter sempre uma cadeia ou "fio condutor" no que respeita às evidências.

Na fase de Análise dos Resultados é importante relacionar a teoria com o restante, selecionar a abordagem de análise de dados e explorar diferentes explicações dos factos. Mas o crucial é expor as evidências livre de qualquer interpretação. A análise dos resultados será qualitativa, uma vez que é a abordagem por excelência do *case study*.

Por fim, no Reporte do Estudo, há que ter em consideração o público-alvo, de forma a produzir material textual e visual adequado, dispor de evidências suficientes para o leitor de forma a enriquecer as conclusões tiradas do trabalho. E após todas estas etapas reler e reescrever, se necessário, antes de finalizar.

1.5. Estrutura do Trabalho

O presente documento está dividido em cinco capítulos, sendo objetivo do presente subcapítulo evidenciar os principais assuntos referentes ao trabalho realizado.

No primeiro capítulo, **Introdução**, é descrito o tema sobre o qual a pesquisa se debruçou e o porquê da sua abordagem, assim como os seus Objetivos e Metodologia utilizada.

A **Revisão da Literatura**, segundo capítulo, apresenta o estado de arte do tema investigado, e tem como objetivo abordar a temática, recorrendo a definições e opiniões dos entendidos, nomeadamente acerca da Importância da Informação enquanto Recurso Estratégico, Estratégia, Estratégia para Sistemas de Informação, Segurança da Informação, Segurança da Informação, Segurança de Informação e as Pessoas, Vulnerabilidades e Ameaças, Estratégia e Segurança de Informação e, por fim, *Balanced Scorecard*.

No terceiro capítulo, **Apresentação da Organização**, procede-se a uma exposição aprofundada da empresa relativamente ao que se revela importante para o Estudo de Caso. É feita uma breve Caracterização do grupo do qual faz parte o concessionário em questão e são evidenciados outros elementos, entre eles: Objetivos Estratégicos, Missão, Visão, Valores, Serviços Prestados, Recursos Humanos e Sistemas de Informação/Tecnologias de Informação.

O **Estudo de Caso**, capítulo quatro, apresenta inicialmente uma Introdução do Estudo de Caso, Âmbito e Pressupostos, seguidos da Recolha, Tratamento e Análise dos Dados e dos Resultados. Na penúltima fase procede-se a uma recolha inicial de dados. Posteriormente faz-se o Tratamento e Análise de Dados, englobando Uma Análise de Pontos Fortes e Fracos da Empresa, as áreas Críticas de Sucesso a Proteger, a Identificação dos Ativos cruciais de Informação, Mapa estratégico para a Organização, a Identificação dos Controlos a aplicar, a elaboração de um Novo Mapa Estratégico já incluindo a perspetiva de segurança de informação Por fim, elabora-se o Mapa Estratégico para a organização e o BSC de segurança de informação. Por fim, faz-se uma Análise de Resultados relativa ao peso da segurança de informação no desempenho organizacional.

No quinto capítulo, **Conclusões e Perspetivas de Trabalho Futuro**, procede-se a uma reflexão sobre o tema apresentado, em forma de conclusão. São ainda identificadas linhas orientadoras para estudos futuros de forma a consolidar todo o trabalho desenvolvido.

Por fim, são apresentadas as **Referências** cujo intuito é evidenciar todos os artigos, livros, publicações *online* e outros documentos consultados para a elaboração deste trabalho.

2. Revisão da Literatura

Neste capítulo é feito o enquadramento teórico das temáticas consideradas no estudo, nomeadamente acerca de Informação enquanto Recurso Estratégico, Estratégia, Estratégia para SI, Segurança da Informação, Gestão de Risco e, por fim, *Balanced Scorecard*.

2.1. Importância da Informação enquanto Recurso Estratégico

Na conjuntura económica atual de crise em que se encontra o país todos os recursos devem ser rentabilizados no seu máximo. A informação, apesar de ser um recurso intangível não deverá ser exceção, até porque é nestes momentos que se torna fulcral proteger a informação de negócio dos concorrentes.

Entender a importância da informação é um imperativo no mundo dos negócios, face à internacionalização e globalização dos mercados. Esse entendimento passa pelo uso racional da informação suportada pelas novas tecnologias e pelo seu impacto nas pessoas e nas organizações (Rascão, 2004).

Também de acordo com Kaplan e Norton (2004), o capital da informação é de certa forma a matéria-prima que nos permite criar de valor na nova economia. Os autores realçam também que este capital só possui valor se inserido na estratégia.

No que respeita ao alinhamento do capital da informação com a estratégia, estes autores consideram que quem lidera as empresas tem que garantir que o seu portefólio de aplicações correspondentes ao capital da informação se alinha com os processos internos estratégicos constantes no mapa estratégico. Mencionam também o facto de várias organizações terem garantido o sucesso depois do desenvolvimento dos primeiros mapas estratégicos.

Tendo por base Rascão (2000), pode-se afirmar que boa informação na organização é um dos capitais mais importantes que esta pode deter, sendo contudo um ativo intangível ou invisível, mas que é cada vez mais valorizado.

O mesmo autor numa publicação de 2008 refere que só é possível tirar partido de uma oportunidade se existir informação oportuna e relevante associada a uma estratégia.

Também de acordo com Gaivéo (2008) a informação e o conhecimento devem ser aceites como ferramentas básicas e essenciais para o desenvolvimento económico e para a criação de emprego que pode ser fundamental para as pessoas, para as organizações e para a sociedade onde estão incluídas.

A informação de negócio deverá então ser rentabilizada enquanto recurso estratégico, mas acima de tudo protegida, pois no mundo dos negócios de hoje em que toda esta está suportada em sistemas de informação, esta ferramenta só poderá ser utilizada como vantagem competitiva se usada de forma certa e no momento certo.

2.1.1. Estratégia

Qualquer organização necessita ter uma estratégia que lhe permita atingir a visão, missão e valores a que se propõe a médio e longo prazo, que deverá dar origem a linhas orientadoras de ações ao nível operacional, ou seja, de curto prazo.

De acordo com Santos (2008) citando Mintzberg (1988), não existe uma única definição universalmente aceite do conceito de estratégia.

Strategor (2000) refere que proceder à elaboração da estratégia da empresa é escolher os domínios de atividade em que a empresa entende que deve estar presente e empregar recursos de modo que se sustente e se possa desenvolver com eles.

Cruz (2006) define estratégia como sendo um caminho que se escolhe para realizar a viagem que se faz entre a "realidade atual" da empresa e a "realidade desejada", representando assim uma opção, uma hipótese ou uma teoria acerca de como poderemos ter sucesso, por forma a concretizar a visão. O autor alerta para o perigo de gerir uma organização sem destino, citando Mintzberg (em Safari da Estratégia) no que respeita à excessiva preocupação com a eficiência, "com o decorrer da expedição na selva, sem nunca nos perguntarmos se (…) estamos a viajar na selva correta".

Santos (2008) refere que etimologicamente estratégia deriva da palavra grega *strategos*, que significa chefe ou líder do exército (general). O autor menciona que neste contexto, estratégia deverá ser entendida como "a arte do general".

São vários os autores que estabelecem o paralelo entre a estratégia empresarial e a militar, sendo que a finalidade militar é vencer o inimigo, em tudo idêntica ao objetivo empresarial, que é criar uma vantagem competitiva que permita superar a concorrência.

Segundo o general Sun Tzu: "Se conhecermos o inimigo e a nós próprios, não precisamos temer o resultado de cem batalhas. Se nos conhecemos a nós próprios, mas não ao inimigo, por cada vitória ganha, vamos também sofrer uma derrota. Se não conhecermos nem o inimigo, nem a nós vamos sucumbir em todas as batalhas".

Neste sentido, em 1979 Porter criou o Modelo das Cinco Forças, que é referido desde então em várias publicações suas e de outros autores no âmbito da temática da estratégia. O modelo destina-se a analisar a competição entre empresas do mesmo setor ou indústria.

Porter (1999) defende que a vantagem competitiva de uma empresa deve considerar regras relativas à concorrência, que definirão se uma indústria pode ser considerada atrativa. A atratividade da indústria considera então: o Potencial de Novas Entradas, Produtos Substitutos, Poder Negocial dos Clientes, Poder Negocial dos Fornecedores e Rivalidade entre Concorrentes Atuais.

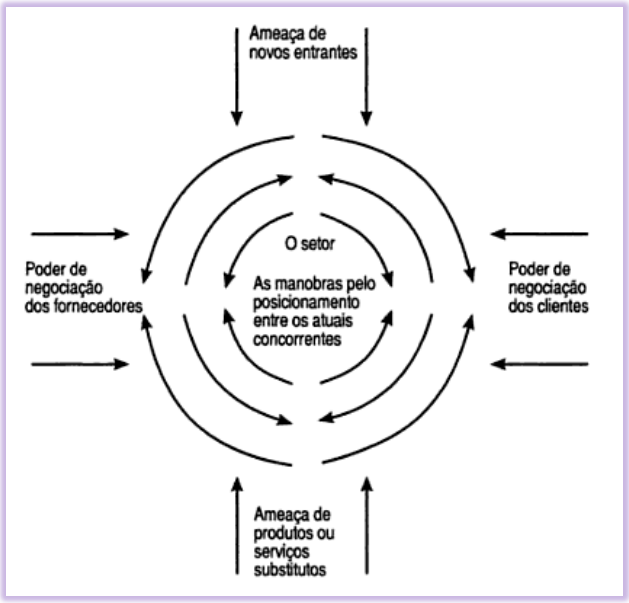

Figura 5 – Forças que governam a competição num setor

Fonte: "Competição: Estratégias Competitivas Essenciais", Porter, 1999: 28

O potencial de novas entradas pode fazer com que a rentabilidade estrutural do negócio diminua substancialmente. Este é tanto menor, quanto maiores se verificarem as barreiras à entrada e a expetativa de retaliação. São exemplos de barreiras à entrada: economias de escala, diferenciação do produto, requisitos de capital, acesso a canais de distribuição, entre outros.

Considera-se que há rivalidade entre concorrentes atuais quando começa a existir uma guerra de preços, fazendo recurso a constantes campanhas publicitárias, algumas com *dumping*, ou seja, vendendo abaixo do preço de custo só para conquistar quota de mercado. Há também quem compita por fazer meras extensões de garantia nos produtos ou serviços prestados.

O domínio dos produtos substitutos poderá impor limites máximos ao preço de venda, gerando altas rentabilidades se provarem ao consumidor alcançarem melhor relação qualidade-preço. O poder negocial dos fornecedores influencia a rentabilidade estrutural da indústria através das suas políticas de preços de venda, de cobrança, de entrega e de qualidade dos produtos. E, por fim, os clientes podem afetar a atratividade de uma indústria através das suas políticas de preços de compra, de pagamento e de exigências de qualidade.

Como se referiu, a análise acima mencionada é aplicada a uma determinada indústria. Porém, se se quiser "afunilar" esta análise estratégica, restringindo-a apenas a um grupo de competidores significativos que sigam em geral a mesma estratégia, é adequado considerar os Grupos Estratégicos considerados por Freire (1995). Grupos Estratégicos são conjuntos de empresas de um dado setor de atividade que adotam estratégias idênticas ou semelhantes, tendo em consideração diferentes variáveis. Na figura seguinte é visível um exemplo para a indústria automóvel considerando a gama de produtos e a cobertura geográfica.

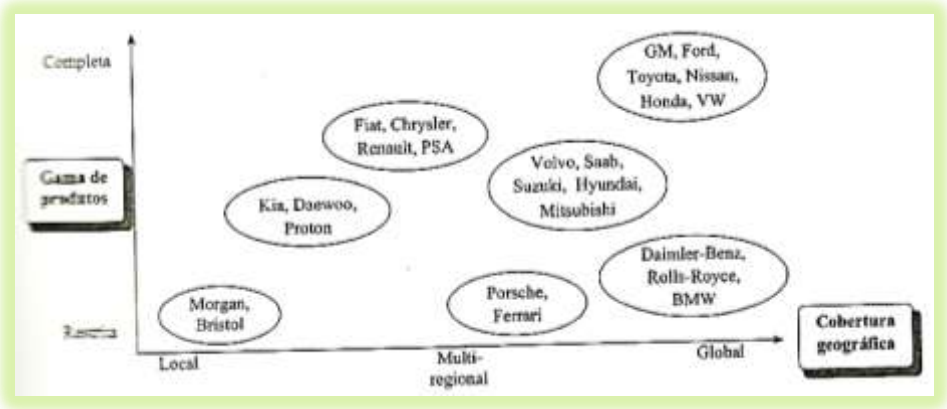

Figura 6 – Mapa de Grupos Estratégicos na Indústria Automóvel
Fonte: "Estratégia – Sucesso em Portugal", Freire, 1995: 101

Em 1995, tendo em conta estas variáveis, Freire considerou que o grupo PSA, produtor da Peugeot e Citroen, fazia parte do mesmo grupo estratégico da Renault e da Chrysler. A performance de uma empresa depende, não só das características estruturais da indústria, mas também das do seu grupo estratégico e da posição que assume dentro dele.

As diferentes variáveis a analisar na conceção de mapas de grupos estratégicos estão englobadas nas quatro dimensões estratégicas de Freire (1995), podendo ser especialização, imagem da marca, cais de distribuição, nível de qualidade, grau de integração vertical, nível de serviço, política de preços, relações com outras empresas ou grupos, etc..

Freire (1995) referiu que "para sustentar o desenvolvimento da organização a longo prazo, a estratégia empresarial deve indicar com clareza" a natureza do negócio em que deseja atuar - Diversificação, os segmentos de mercado que deseja servir e com que produtos/serviços - Produtos-mercados, as atividades operacionais que deseja realizar internamente - Integração Vertical (figura 7) e os mercados geográficos em que deseja atuar - Internacionalização. São estas as quatro dimensões estratégicas nas quais se baseia o modelo de gestão estratégica do autor.

Figura 7 – Exemplo de Integração Vertical Completa
Fonte: "Estratégia – Sucesso em Portugal", Freire, 1995: 101

A integração vertical reveste-se de particular valor na estratégia empresarial, uma vez que envolve decisões a nível operacional que poderão alto impacto a nível estratégico, tanto benéfico, como prejudicial. A figura acima evidencia um exemplo de integração vertical completo. Como principais benefícios de internalizar podem-se apontar as economias operacionais, de informação e de coordenação, assim como o aumento de barreiras à entrada. Como condicionantes destacam-se as deseconomias de escala, menor acesso a processos tecnológicos especializados e a diluição da estratégia da empresa.

Rascão (2006) advoga a existência de escolas filosóficas, a partir das quais cada um dos seus autores define estratégia segundo determinadas premissas. A escola de Carnegie ou Planeamento Estratégico de Ansoff é considerada a escola base para todas as outras. O autor desta escola define estratégia "como sendo o melhor posicionamento do conjunto de produtos e mercados da empresa no meio envolvente sistémico e competitivo", conjugando estes fatores numa matriz Produto/Mercado como evidencia a seguinte figura.

Figura 8 - Matriz Produto/Mercado de Ansoff

Fonte: "Análise Estratégica", Ansoff Igor 1977 (Citado por Rascão, 2001: 58)

Esta matriz evidencia qual a estratégia a adotar, cruzando a decisão de produzir novos produtos/serviços ou manter os mesmos com a decisão de investir em novos mercados. Como analisado anteriormente, Freire (1995) considera também no seu modelo de gestão estratégica como uma das quatro dimensões a matriz de Produtos/Mercados.

De acordo com Freire (1995:99), "o primeiro passo na formulação estratégica consiste na identificação das tendências do meio envolvente contextual e transacional, bem como das suas implicações para a indústria". É no meio envolvente transacional que faz sentido considerar o estudo dos concorrentes.

Neste sentido, um dos primeiros modelos de análise estratégica, surgidos nos Estados Unidos nos anos sessenta, desenvolvido na *Harvard Business School* pelos professores *Learned, Christensen, Andrews e Guths (LCAG)*, que continua a evidenciar uma lógica subjacente às abordagens mais recentes da estratégia, confronta a empresa com o seu ambiente concorrencial avaliando a maior ou menor adaptação das competências e recursos próprios da empresa aos condicionalismos que esse ambiente lhe impõe (Strategor: 2000).

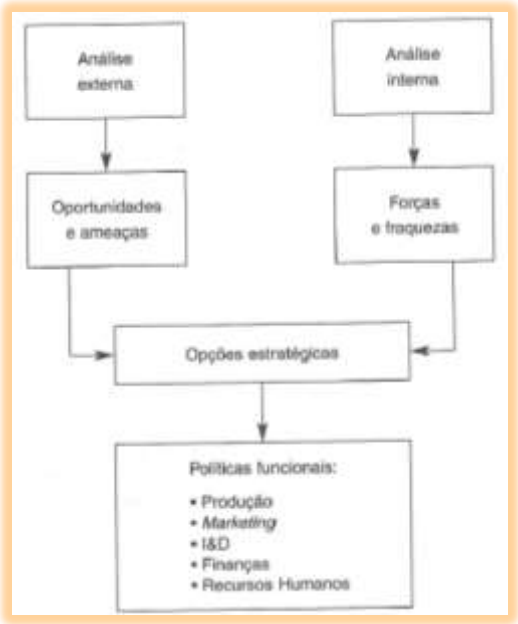

Figura 9 – Modelo LCAG/SWOT

Fonte: "Strategor: Política Global da Empresa", trad. de Freitas e Silva, 2000: 26

A figura acima evidencia o modelo LCAG, que faz a confrontação entre a análise interna (recursos da empresa) e a análise externa (ambiente concorrencial). Focado na avaliação das forças e fraquezas, por um lado, e na identificação das oportunidades e ameaças, por outro, o modelo é também conhecido pelo acrónimo *Strengths, Weaknesses, Opportunities, and Threats* (SWOT) (Strategor, 2000).

Por sua vez é acrescida a importância de identificar os fatores críticos de sucesso de cada segmento de mercado, que normalmente só se conseguem identificar após uma criteriosa análise SWOT. Freire (1995:96) define fatores críticos de sucesso como "variáveis que mais proporcionam aos clientes e que melhor diferenciam os concorrentes na criação desse valor".

A ferramenta de *Bechmarking* torna-se particularmente útil neste aspeto porque as empresas, com o intuito de privilegiar a melhoria contínua, devem comparar constantemente os seus processos de negócio e medidas de desempenho com as melhores práticas existentes. Esta técnica pode ser executada de três formas: internamente, relativamente aos concorrentes ou às empresas de outros setores.

Strategor (2000:60) define *Bechmarking* como um método que "consiste em analisar os desempenhos da empresa num determinado fator-chave de sucesso e em procurar uma base de comparação que permita à empresa melhorar consideravelmente o seu grau de domínio".

Segundo Freire (1995) o *Bechmarking* que é feito internamente, pode ser realizado tendo em consideração o passado, ou seja, analisando a evolução da empresa nos últimos 3 anos.

Apresenta como vantagem o facto de se poder ter acesso fácil à informação e uma visão dinâmica. Porém, poderá revelar-se insuficiente por ausência de referências externas.

O *Bechmarking* realizado com base em normas do setor proporciona uma visão mais alargada do desempenho relativo da empresa. Porém, o sucesso da aplicação desta medida depende da disponibilidade, credibilidade e rigor dos dados. A diversidade de estratégias dentro de empresas da mesma indústria e a impossibilidade de comparação também poderão inviabilizar este tipo de *Benchmarking.*

Por fim, o *Benchmarking* que é efetuado relativamente à concorrência poderá surtir muito mais efeito, já que à partida, a estratégia será semelhante. Apresenta como condicionantes o facto de não se poder ter acesso fácil à informação com facilidade, a menos que haja cooperação entre empresas, o que é raro e também o risco de se poder apenas a copiar os competidores.

Segundo Freire (1995), o *Bechmarking* assume um caráter estratégico quando tem um impacto direto sobre os fatores críticos de sucesso do negócio. Quando se limita a seguir apenas boas práticas em questões de apoio, como nos processos de faturação por exemplo, não se refletindo benéficos nas competências centrais, mas permitindo reduzir custos de forma significativa, o que vai surtir efeito em termos de resultados. O autor defende que a melhor forma de começar um programa de *benchmarking* estratégico é selecionar o competidor que apresenta melhor quota de mercado no segmento em que a empresa atua e procurar perceber as diferenças que poderão estar na origem de um melhor desempenho comercial.

São vários os modelos e teorias de estratégia desenvolvidos pelos “gurus” da temática. Porém, na sua essência apresentam muitas semelhanças quando evidenciam a importância de tirar partido dos recursos internos da empresa e da adaptação ao meio empresarial. Estes dois fatores podem ser alvo de diversos estudos, todos com o intuito de fundamentar a orientação estratégica da empresa.

2.1.2. Estratégia para os Sistemas de Informação

A estratégia para os SI´s deverá estar perfeitamente enquadrada na estratégia global da empresa, permitindo que a forma como se processa e suporta a informação seja um veículo que auxilie o alcance dos objetivos estratégicos de negócio e não que representem apenas um peso em termos de custos, sem qualquer criação de valor.

De acordo com Simon Lardera e Bernard Quinio (1996), citados por Rascão (2001: 149) “os gestores das empresas têm hoje a sensação de gastar cada vez mais com os seus SI´s computurizados sem contudo retirarem daí vantagens estratégicas importantes”.

No entanto são conhecidos no mercado verdadeiros exemplos de empresas de sucesso justamente devido ao facto de conseguirem tirar o máximo partido dos SI´s. Porém, dada a crescente diversidade de ofertas no mercado, muitas vezes não é tarefa fácil escolher a melhor opção, o que torna a tarefa dos gestores de SI´s bastante árdua.

Simon Lardera e Bernard Quinio (1996), citados por Rascão (2001) referem que a evolução da tomada de consciência da importância da informação enquanto sistema se pode sintetizar em três etapas: Interesse, Visão e Determinação, como é evidenciado na figura seguinte.

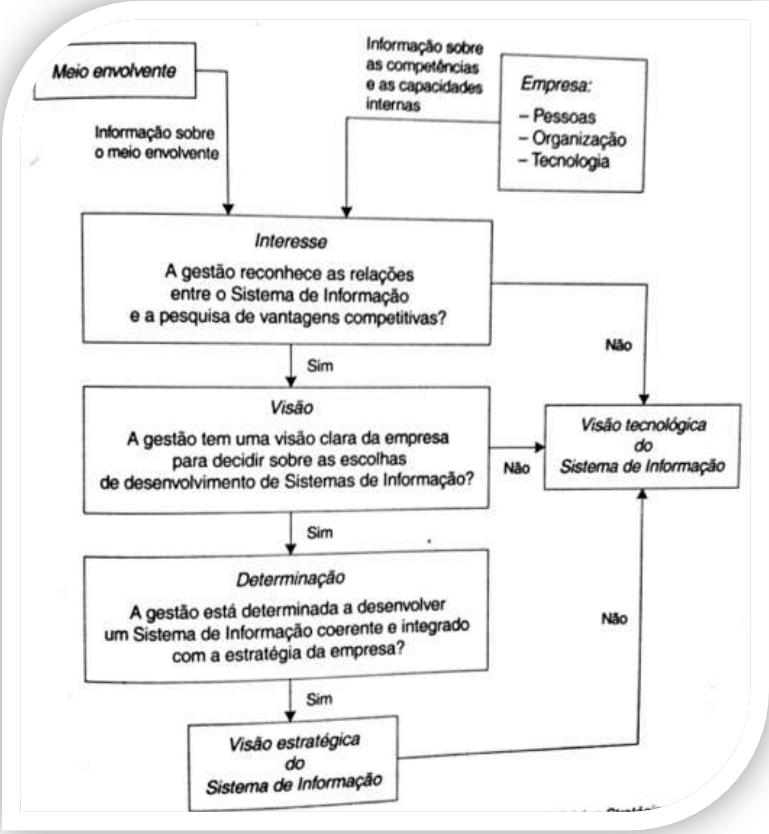

Figura 10 – Visão Estratégica do Sistema de Informação

Fonte: "Análise Estratégica- Sistema de Informação para a Tomada de Decisão Estratégica", Rascão, 2001: 151

Este fluxograma enfatiza o facto de ser de extrema importância a empresa reconhecer a pertinência e estar interessada em alterar os SI´s de forma a obter vantagem competitiva e desenvolvê-los a esse nível.

Simon Lardera e Bernard Quinio (1996), citados por Rascão (2001:152) defendem também que "a estratégia empresarial pode ser tratada como um problema que se divide em três partes: a Informação, a Estratégia e as Tecnologias de Informação e Comunicação".

Rascão (2008) defende que a gestão de informação necessita de uma nova identidade, deixando de ser tão somente o alinhamento da estratégia das TIC´s com a estratégia do negócio. Esta preconiza uma coisa, a gestão das TIC´s outra. “A gestão da informação é a essência da construção do sentido da própria organização (a sua razão de ser)” (Rascão 2008:288).

Só com um bom processo de gestão de informação devidamente implementado na organização e liderado por gestores de informação e não por gestores de TIC´s se conseguirá explorar convenientemente as imperfeições deste recurso tão rentável de forma estratégica, de acordo com com Rascão (2012).

Também segundo Lopes *at al* (2005) evidenciam numa expressão o resumo deste processo: “Poder-se-á dizer que não há organização sem informação, nem sistema de informação sem informação e, consequentemente, não há organização sem sistema de informação”. Os autores fazem menção num dos capítulos da sua publicação que os SI´s são um importante catalisador na mudança organizacional urgente a este nível.

Wilson (2002) advoga que é justo comparar a importância de gerir a informação à de obtenção de lucro, pois efetivamente se gerirmos bem a informação, mas não tivermos lucro, a empresa encerra. Porém, a obtenção de lucro depende de uma boa tomada de decisão baseada numa informação precisa.

Com a colocação em prática de uma ferramenta bastante importante como o *benchmarking* é possível que os concorrentes consigam ter acesso às mesmas tecnologias e retirar partido destas da mesma forma. No entanto, a estratégia ao nível da gestão dos SI´s envolve mais do que simples aquisição de tecnologia, já que a experiência e conhecimento acerca dos processos também é crucial. E esta a concorrência não consegue imitar, pelo menos com tanta facilidade.

2.2. Segurança de Informação

A segurança de informação emerge cada vez mais como uma função crítica de negócio talvez devido a fatores como a crescente dependência da internet ou o aumento da concorrência feroz motivada pela diminuição da procura em grande parte dos setores. Este facto torna a gestão da segurança de informação num desafio cada vez maior.

Segundo Herrmann (2002) a segurança de informação pode ser entendida como um conjunto de operações que protegem e defendem a informação e os SI´s, assegurando a sua disponibilidade, integridade, autenticação e confidencialidade, incluindo o fornecimento dos SI´s para reparação, englobando ainda a proteção, deteção e capacidade de reação.

É impreterível preservar a integridade de um ativo intangível tão precioso como a informação estratégica. É igualmente fulcral garantir a disponibilidade da informação, no sentido de torná-la acessível sempre que necessário àqueles que estão devidamente autorizados, sem

colocar em causa a sua confidencialidade e de forma a salvaguardar a sua veracidade, complementaridade e métodos de processamento.

Whitman e Mattord (2004) defendem que a afirmação de Sun Tzu feita há mais de 2400 anos atrás, acerca da importância de conhecermos o inimigo, continua a ter relevância direta na filosofia da segurança de informação hoje em dia. Referem também que a estratégia e táticas da segurança de informação são de muitas formas similares àquelas que foram empregues na guerra convencional.

Os autores referem que seja qual for o tipo de organização existe sempre risco associado. Então uma vez conhecidas as nossas fraquezas, os gestores podem dedicar-se à segunda máxima de Sun Tzu: conhecer o inimigo.

Assim sendo, visto que estas práticas estratégicas são partilhadas pelo tecido empresarial em geral, é fundamental protegermos toda a informação, principalmente aquela que é diretamente alvo de interesse para a concorrência.

Segundo Chaplain (2009), o suporte para as recomendações de segurança pode ser encontrado tanto em controlos lógicos como físicos. Os primeiros impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrónico, e que de outra forma, ficaria exposta à alteração não autorizada por pessoas com mau intuito. São exemplos mecanismos de controlo de acesso, de criptografia, de certificação, de assinatura digital, etc.. Os controlos físicos, por sua vez, são barreiras que limitam o contato ou acesso direto à informação ou à infra-estrutura que suporta e gera essa informação, existindo mecanismos de segurança que os apoiam, tais como portas, trancas, paredes, blindagem, vigilantes, etc ..

Martins (2008) advoga que a segurança de informação deve ser encarada como um processo que deve englobar várias dimensões interligadas como se evidencia na seguinte figura.

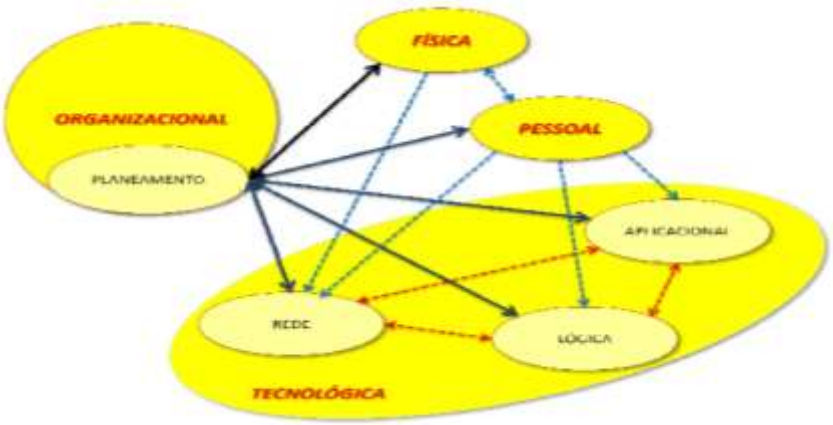

Figura 11 – Dimensões da Sistema de Informação

Fonte: "Framework de Segurança de um Sistema de Informação", Martins, 2008: 70

A vertente organizacional prende-se com a cultura organizacional de cada entidade que em tudo contribui para a tomada de decisão a qualquer nível, sendo essencial o comprometimento da gestão de topo com a segurança de informação de forma a englobar esta vertente no planeamento.

A dimensão tecnológica é deveras importante porque é a que dá suporte ao processamento e gestão informacional, englobando a segurança de aplicações, a rede e a vertente lógica. Já segundo Carneiro (2001) a segurança lógica abrange a gestão e controlo de acessos, gestão dos SI´s informatizados e da rede e segurança dos sistemas aplicacionais. Estas duas perspetivas não são contraditórias, já que todo o processo é recíproco.

A segurança física, também segundo Carneiro (2001), engloba a proteção a nível pessoal e no que respeita às instalações. A vertente pessoal por si só poderá ter grande impacto no desempenho da segurança de informação porque são as pessoas que fazem uso dos SI´s e do que os suporta.

É imperativo que o tecido empresarial em massa pondere considerar a importância da segurança de informação enquanto estratégia de peso, já que vivemos em momentos em que a concorrência é tudo menos perfeita. Dessa imperfeição surgem oportunidades de grande valor acrescentado para as entidades em geral, se bem aproveitadas. Quem primeiro tiver acesso à informação privilegiada, conseguirá estar na dianteira do mercado, deixando a léguas alguns dos competidores mais desatentos e que descuram a segurança da sua própria informação, não explorando convenientemente as imperfeições ou fugas deste “metal precioso”.

2.2.1. Pessoas e Segurança de Informação

Porque as situações criadas e existentes entre humanos e sistemas organizacionais são únicas, as pessoas desempenham um papel fundamental na segurança de informação, uma vez que não há processamento de informação sem que exista a sua intervenção.

De acordo com Oliveira (2001) “segurança de informação define-se como o processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados”. Porém, o autor enfatiza também o facto de a segurança de informação não se prender apenas com uma questão técnica, mas também com questões estratégicas e humanas. Pode-se então concluir que a segurança de informação liga TI´s, processos e pessoas, como aliás já se tinha considerado no subcapítulo anterior.

Também Mamede (2006) refere a problemática fundamental a considerar na segurança de informação, ou seja, a falta de sensibilidade dos utilizadores para questões de segurança. É então a esta questão que os profissionais de segurança tentam dar resposta, entre outras.

O fator humano emerge como um dos principais elementos a considerar quando se assume a indispensabilidade da colaboração das pessoas para manutenção da segurança do SI, independentemente da sofisticação e preço dos meios e dispositivos disponibilizados (Carneiro, 2002). Neste âmbito, Carneiro (2002) também refere a importância de ser proporcionada às pessoas a formação adequada, abrangendo igualmente os gestores, considerando assim que a proteção não deve basear-se apenas em meios físicos e lógicos.

Relativamente à segurança dos recursos humanos a norma ISO/IEC 27002:2005 recomenda boas práticas, entre as quais a inclusão de termos de confidencialidade nos contratos de trabalho, a remoção de direitos de acesso e a sensibilização dos colaboradores para a importância da segurança de informação, acima de tudo dos gestores, que deverão dar o exemplo.

Questões culturais também poderão contribuir em larga escala para mudança de comportamentos necessários à segurança de informação. E a questão da estabilidade no posto de trabalho também poderá influenciar motivações e comportamentos, mesmo que involuntários.

Figura 12 – Grau de dificuldade na mudança organizaional

Fonte: Adaptado de Schein 1992:70

A mente humana requer estabilidade. Portanto, qualquer desafio de um dado adquirido resultará em ansiedade e resistência. Neste sentido, as premissas básicas que compõem a cultura organizacional pode ser encarada em dois níveis - individual e de grupo - como mecanismos de defesa, que permitem que o grupo continue a funcionar. O reconhecimento desta conexão é importante quando há necessidade de mudar a cultura de um grupo, pois não é mais fácil mudar o comportamento grupal do que o individual.

Trabalhadores motivados e sensibilizados contribuirão para uma implementação de um SGSI de forma mais consciente e encararão a empresa como um todo, considerando-se estes parte dela.

2.2.2. Vulnerabilidades e Ameaças

A dependência em relação a sistemas e serviços de informação implica uma maior vulnerabilidade das organizações a ameaças de segurança. A informação, como outros ativos importantes, possui um grande valor e exige proteção adequada. A devida identificação e classificação desses ativos e a avaliação sistemática das ameaças e vulnerabilidades permitem à organização escolher as metodologias adequadas para gerir os riscos.

De acordo com Gaivéo (2008), é essencial que a definição da política de segurança da informação na organização proceda à caracterização desses riscos, permitindo responder adequadamente às ameaças e reduzindo simultaneamente as vulnerabilidades identificadas.

O autor refere que vulnerabilidade pode ser entendida como uma fraqueza ou falha num sistema ou mecanismo de proteção que expõe ativos de informação a ataques ou danos (Whitman and Mattord, 2005), como uma debilidade num sistema, aplicação ou infra-estrutura, que pode ser explorada para violar a integridade do sistema (Peltier, 2005). Pode-se então definir vulnerabilidade como uma condição ou conjunto de condições que podem permitir que uma ameaça afete um ativo. Gaivéo (2008) refere como exemplos de vulnerabilidades as seguintes:

- **Pessoais**: ausências, morte, insanidade, competência, ética, erros, sensibilidade, comunicação, nº insuficiente;
- **Equipamento:** mau funcionamento, falhas de energia, portabilidade, depreciação;
- **Informação:** portabilidade, formato, vida limitada, única, conformidade.

Whitman e Mattord (2005) entendem ameaça como um objeto, pessoa ou outra entidade que representa um perigo constante para um ativo, sendo que ameaça pode também ser entendida como um evento com potencial para causar acessos não autorizados, modificações ou destruição dos recursos de informação, de aplicações ou de sistemas (Peltier, 2005). Pode-se então definir ameaça como uma causa potencial da ocorrência de um incidente que possa prejudicar um sistema ou organização. Gaivéo (2008) refere, com base em Whitman e Mattord (2004), como exemplos de ameaças as seguintes:

- Atos de falhas ou erros humanos;
- Comprometimento da propriedade inteletual;
- Atos deliberados de espionagem ou invasão;
- Atos deliberados de extorsão de informação;
- Atos deliberados de sabotagem ou vandalismo;
- Atos deliberados de roubo;
- Ataques deliberados de *software*;
- Desvios na qualidade dos serviços por parte dos fornecedores;
- Forças da natureza;
- Erros ou falhas técnicas de *hardware*;

- Erros ou falhas técnicas de *software*;
- Obsolescência tecnológica.

Torna-se cada vez mais imperativo que a empresa identifique as vulnerabilidades da informação crítica de negócio, que facilmente poderão ser exploradas por qualquer uma das ameaças acima referidas e causar danos graves num recurso intangível de importância economicamente elevada.

2.2.3. Estratégia e Segurança de Informação

A definição de políticas de segurança de informação deverá ter em linha de conta os aspetos culturais da organização como já se viu. Neste sentido a segurança de informação pode ser encarada como um conjunto de medidas que constituem a política de segurança (Gaivéo, 2009).

Um SGSI pode ser considerado uma parte do sistema geral de gestão da organização, baseando-se então numa abordagem do risco de negócio para estabelecer, implementar, operar, monitorizar, rever, manter ou melhorar a segurança de informação (ISO 27002:2013).

Gaivéo (2009) considera que a identificação das políticas de segurança mais adequadas à organização deverá ter em linha de conta fatores humanos, recursos técnicos e financeiros disponíveis, procurando assim responder às necessidades do negócio.

Muitas vezes o valor da implementação de um SGSI não é reconhecido pelas empresas. Assim sendo, de acordo com Gaivéo (2008), "a segurança entendida como uma componente global, deve ser parte integrante do projeto inicial de SI, incorporando na sua estratégia a estratégia dos SGSI", como é evidenciado na seguinte figura.

Figura 13 – Integração da estratégia dos SGSI na estratégia da organização

Fonte: "As Pessoas nos Sistemas de Gestão da Segurança da Informação", Gaivéo, 2008: 132

O autor realça a importância de adequar a estratégia do SGSI à estratégia de SI e TI, que por sua vez deverá ter em linha de conta a estratégia de negócio da empresa. A implementação de políticas de segurança envolve como já foi referido recursos humanos e financeiros, mas também comporta mudanças na estrutura organizacional, que muitas vezes não são entendidas no seio das organizações por falta de informação.

Selig (2008) também destaca a importância da mudança que é forçada muitas vezes por pressões externas que influenciam o ambiente organizacional, tais como os próprios concorrentes, legislação, economia, estilos de vida do consumidores, nova tecnologia, etc.. Quem lidera tem que estar preparado para responder rapidamente a estes estímulos e atualizar-se, nomeadamente quantos aos SI´s. A figura seguinte de LeVeque (2006) evidencia este raciocínio.

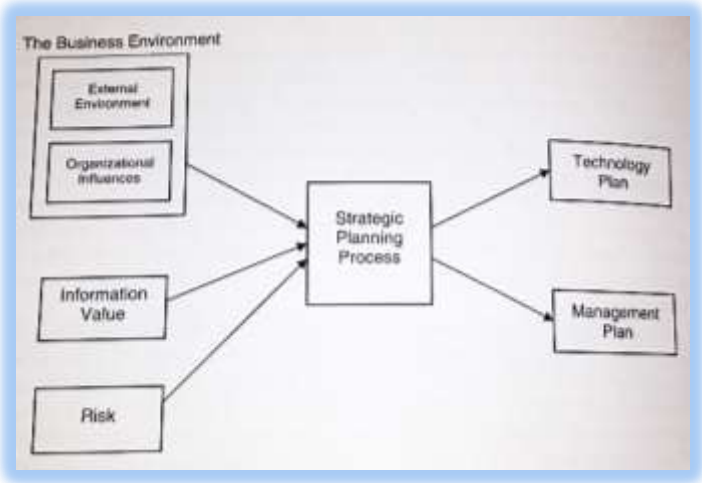

Figura 14 – *Information Security Strategic Planning Model*
Fonte: "Information Security: a Strategic Aproach", LeVeque, 2006:4

O ambiente organizacional define qual o nível de segurança que é necessário para alcançar os seus objetivos estratégicos. Por isso, neste processo deve ser sempre considerado o valor da informação e qual é que impreterivelmente se tem que proteger, tendo em consideração o risco a que está exposta.

A estratégia para os SI´s não deverá ser mais do que um processo integrado que envolva todas as suas componentes, dando igual ênfase a todas. Só desta forma se consegue fazer com que os resultados da empresa sejam impulsionados pelos SI´s e não o contrário, ou seja, que sejam os SI´s a pesar na estrutura de custos de tal forma que baixem consideravelmente o lucro – objetivo máximo dos acionistas. São estes os argumentos a utilizar para comprometer a gestão de topo com os SI´s e com a sua segurança.

2.3. *Balanced Scorecard* (BSC)

O controlo de gestão envolve um conjunto de instrumentos que permitem medir desvios entre o que foi planeado e os resultados finais, visando motivar os gestores a atingir os objetivos estratégicos da empresa. Neste sentido, privilegia-se a ação e a tomada de decisão em tempo útil, favorecendo a delegação de autoridade e responsabilidade.

Rascão (2006) realça também a importância da existência de hierarquias a nível estratégico e da definição de sub-estratégias para que a nível operacional se consigam alcançar as estratégias de topo, não descurando porém do processo de comunicação que deverá existir entre as unidades de negócio e o nível de grupo económico.

No processo de controlo de gestão existem instrumentos que são utilizados à priori, como o planeamento ou definição de objetivos e a orçamentação, e instrumentos utilizados à posteriori, como o controlo orçamental e quadros de indicadores.

De acordo com Kiyan (2001), os tradicionais sistemas de informação para a gestão utilizados pelas empresas são variados: sistemas de indicadores, *tableaux de bord*, sistemas de contabilidade financeira ou de gestão, etc. Porém, de acordo com o mesmo autor, os objetivos destes sistemas centram-se demasiado na medição da eficiência operacional e numa ótica financeira e contabilística, não existindo relacionamento entre estes e os objetivos estratégicos da empresa.

Kaplan e Norton (2004) procuraram desenvolver um modelo que incorporasse o valor de ativos intangíveis e intelectuais, como as relações com o exterior, a satisfação dos clientes, a capacidade de inovação, as capacidades e qualidades dos trabalhadores e o desenvolvimento de processos internos mais flexíveis.

Surge então o BSC, com o objetivo de complementar as medidas financeiras tradicionais, de modo a facilitar o processo de tomada de decisão e melhorar o desempenho organizacional, tendo em linha de conta os objetivos estratégicos da empresa.

Assim sendo, deve-se ter em consideração missão, valores, visão e objetivos estratégicos para proceder à elaboração do BSC. Por sua vez, através do BSC, procede-se à definição de indicadores, metas e ações a tomar no sentido de alcançar os principais vetores estratégicos: Processos Internos Eficazes com o objetivo de ter Acionistas e Clientes satisfeitos e colaboradores motivados. (figura 15)

O BSC é definido como um sistema complementar às medidas financeiras tradicionais, fornecendo um conjunto de informações que propicia, à gestão, uma rápida e melhor compreensão do negócio e da estratégia organizacional. Estas medidas visam permitir uma avaliação de desempenho das organizações, através de um conjunto de indicadores, devendo esta monitorização ser parte integrante do processo de gestão.

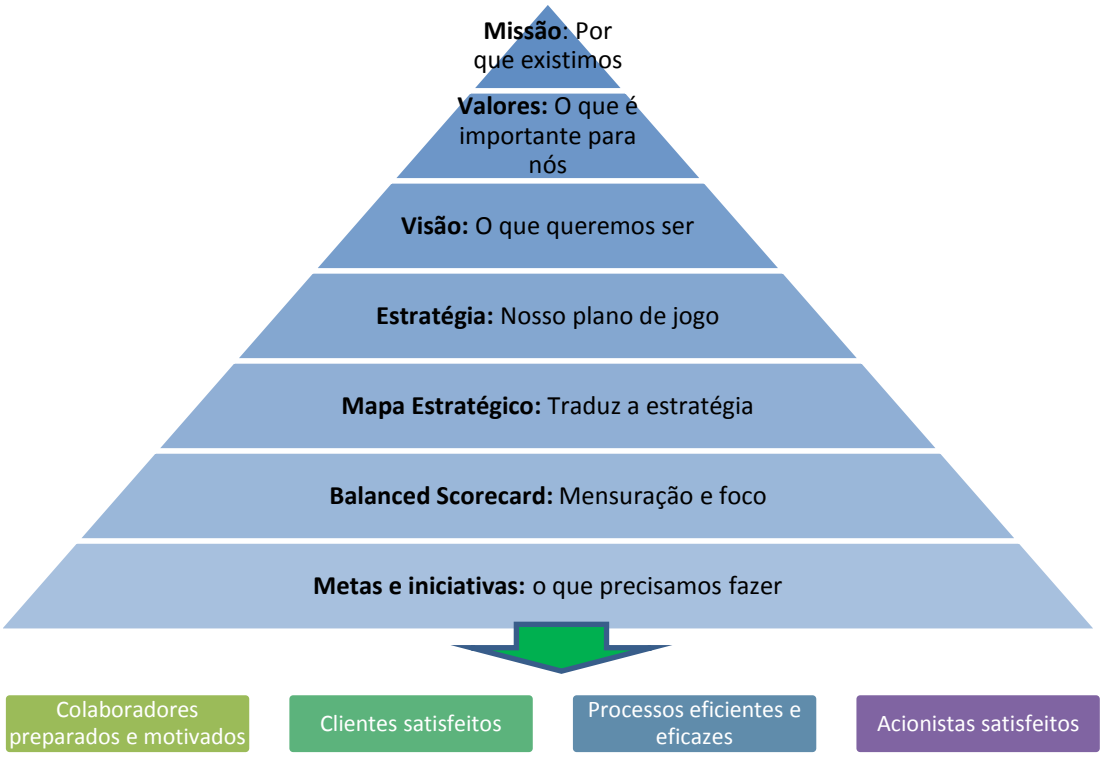

Figura 15 - BSC enquanto etapa de um processo contínuo

Adaptado de "Mapas Estratégicos – convertendo os ativos intangíveis em resultados tangíveis", Norton e Kaplan 2004: 35

De acordo com os autores Norton e Kaplan (2004) existem quatro perspetivas a considerar no sentido de serem alcançados os objetivos estratégicos, que estão todas interligadas entre si. Estas quatro perspetivas são evidenciadas na figura 16.

Figura 16 - As quatro perspetivas do BSC segundo Norton e Kaplan

Adaptado de "Mapas Estratégicos – convertendo os ativos intangíveis em resultados tangíveis", Norton e Kaplan 2004: 8

As quatro perspetivas de Norton e Kaplan resumem-se às seguintes questões:

- **Financeira –** para que a empresa tenha sucesso financeiramente, como deverá ser vista pelos investidores?
- **Processos Internos –** Para satisfazer os clientes, em que processos devemos sobressair?
- **Aprendizagem e Crescimento –** Para alcançar a nossa visão, como devemos sustentar a habilidade de mudar e progredir, motivando também os nossos RH´s?
- **Clientes –** Para alcançar a nossa visão, como devemos ser encarados pelos clientes, deixando-os satisfeitos?

Os mesmos autores defendem que as quatro perspetivas são apenas um modelo e não um teorema matemático, pelo que será normal acrescentar uma ou mais perspetivas, dependendo de várias circunstâncias, tais como o sector e a estratégia da organização.

Norton e Kaplan (2004) enfatizam a importância de elaborar um mapa estratégico (figura 17), já que segundo os autores este mapa " é a representação visual da estratégia, mostrando numa única página como os objetivos nas quatro perspetivas se integram e combinam para descrever a estratégia".

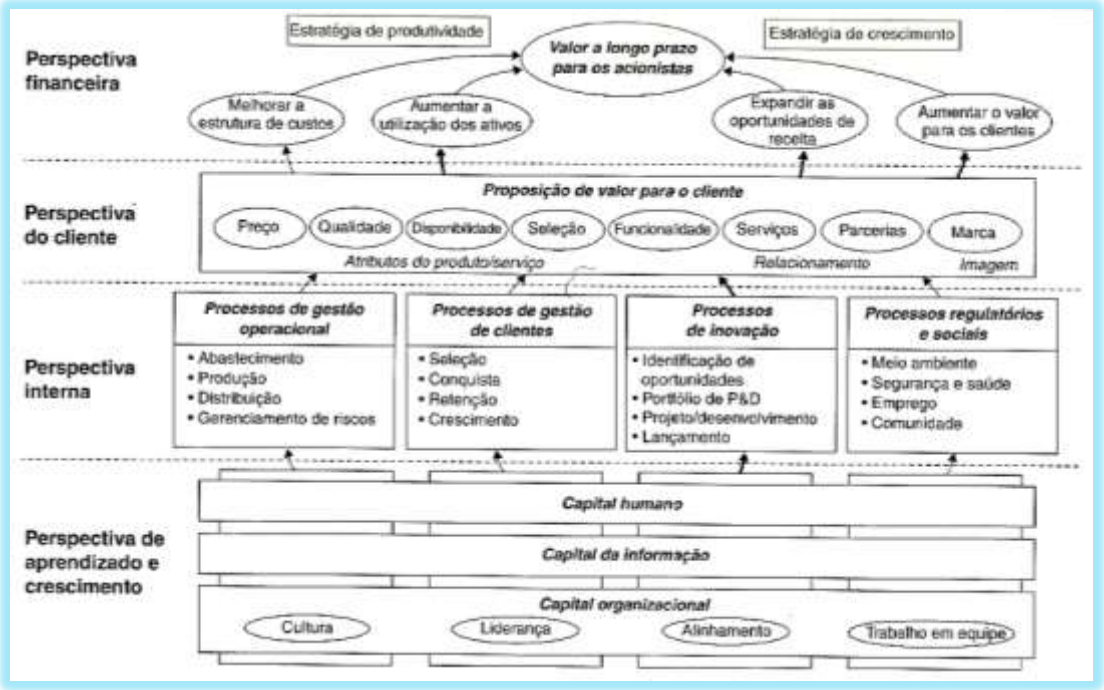

Figura 17 – Mapa estratégico representando como a organização cria valor

Fonte: "Mapas Estratégicos: Convertendo Ativos Intangíveis em Resultados Tangíveis", Norton&Kaplan, 2004: 11

A conceção deste mapa tem como intuito mostrar de que forma se pode gerar valor acrescentando para toda as partes interessadas, evidenciando exemplos muito concretos. Com o exemplo da figura seguinte é visível a sua utilidade.

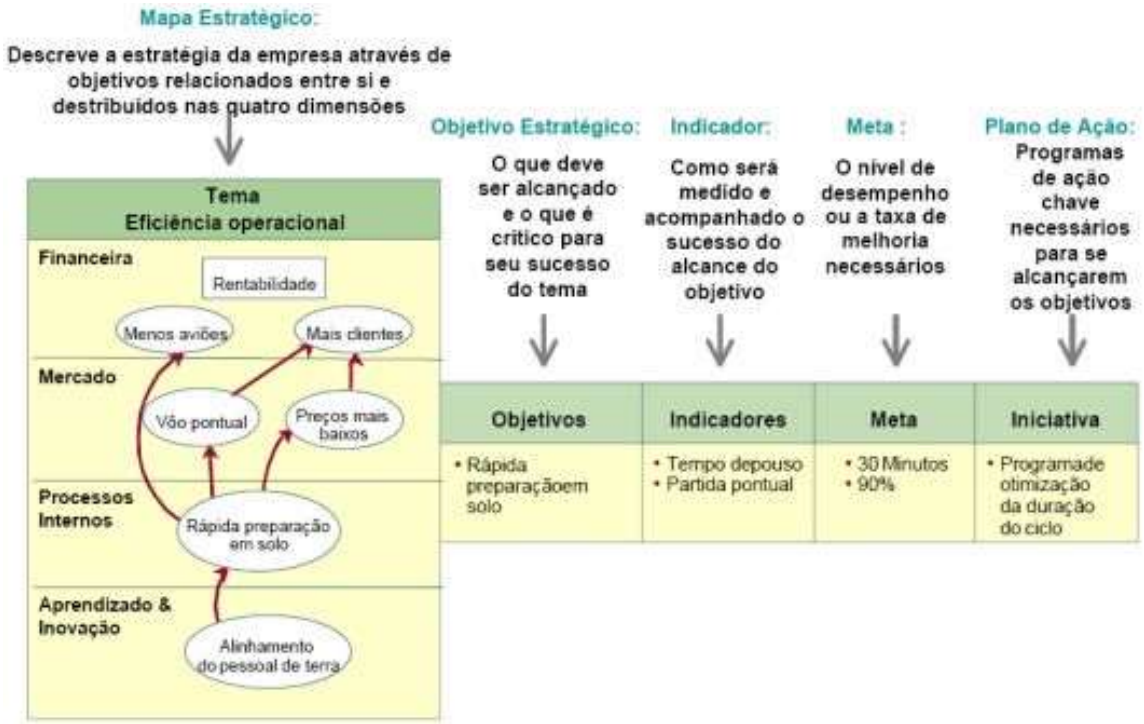

Figura 18 – Processo do *Balanced Scorecard* para a Southwest Airlines

Fonte: "A estratégia em ação: Balanced Scorecard", Kaplan e Norton, 1997

O mapa permite assim concentrar quais os objetivos a seguir, bem como os indicadores, metas e ações a tomar para alcançá-los, tendo em conta as quatro perspetivas de Kaplan e Norton.

Também Cruz (2006) realça a importância de "confrontar os efeitos indesejáveis com os objectivos estratégicos retirados do mapa da estratégia, para salientar que a realidade atual da organização não coincide com a realidade idealizada". O autor considera de suma importância os mapas com relações de causa-efeito, para definir a mudança de ações a levar a cabo para estar em linha com a estratégia anteriormente definida. O mesmo autor realça a importância de fazer o desdobramento da visão até chegar aos indicadores estratégicos, como se evidencia na figura 19.

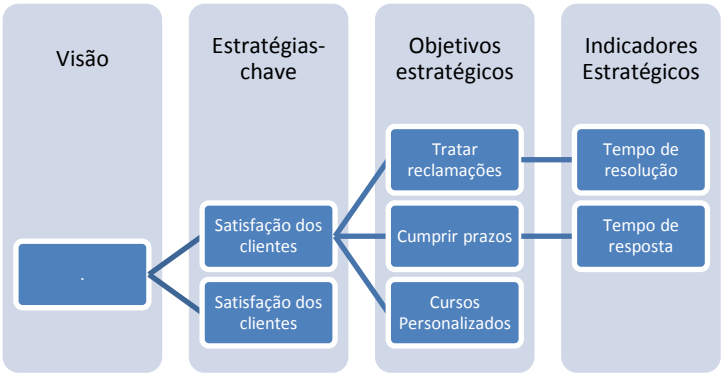

Figura 19 – Desdobramento da visão aos indicadores estratégicos

Fonte: Adaptado de "*Balanced Scorecard* – Concentrar uma Organização no que é Essencial", Cruz, C., 2006: 50

Este desdobramento revela-se importante no sentido de operacionalizar e definir indicadores estratégicos.

Em suma, o *Balance Scorecard* apresenta diversas vantagens, que se listam seguidamente:

- Permite maior alinhamento entre objetivos estratégicos da organização e objetivos das áreas de negócio operacionais, facilitando a implementação da estratégia;
- Promove uma relação de causalidade entre objetivos da empresa, se bem concebido;
- Permite definir os fatores chave de sucesso para cada perspetiva bem como os indicadores e as relações de causa-efeito entre eles;
- Adota uma perspetiva global, dado que combina objetivos de curto e longo prazo, indicadores monetários e não monetários e informação prospetiva com retrospetiva.
- Correlaciona indicadores e permite a análise, controlo e tomada de decisão, dada a flexibilidade do documento.

No entanto, esta ferramenta de análise estratégica também apresenta condicionantes, tais como os seguintes:

- Poderá existir a necessidade de alteração do modelo com a criação de novas perspetivas de modo a representar a realidade da organização;
- Um mapa estratégico mal concebido, onde as relações causa-efeito não agregam valor, poderá trazer maiores custos que benefícios;
- Caso seja mal difundido, a reação à mudança e a suscetibilidade por parte dos RH poderá provocar entraves;
- Algumas tomadas de decisão poderão não ser exequíveis por custos associados.

Por comparação com o BSC existe o Método *Learn* desenvolvido por Coelho (2005) que se baseia numa filosofia de *learning organization,* ou seja, de melhoria contínua. Este diferencia-se do primeiro porque reduz o grau de subjetividade em todo o processo particularmente nas relações de causa-efeito, já que prioriza uma definição de objetivos que relacione todas as partes interessadas desde o topo até à base, é mais focado numa abordagem por processos, dá ênfase à definição de objetivos individuais e baseia o consenso sobre os objetivos no acordo acerca do desempenho atual da organização.

Para alcançar este consenso é necessário exprimir a estratégia em objetivos e metas. Porém, muitas vezes a estratégia encontra-se apenas expressa em objetivos numéricos que poderão ser interpretados de diversas formas pelos vários departamentos da organização. Isto originará uma falta de uniformidade na motivação de todos os colaboradores em alcançar os objetivos.

De acordo com o Método *Learn* os objetivos deverão ser encarados como orientações a seguir, os indicadores como sendo as variáveis que possibilitem medir e monitorizar os objetivos e as metas como sendo os valores a alcançar pelos indicadores num dado período.

À semelhança do que acontece com o método BSC, o Método *Learn* também tem como ponto de partida a missão e visão da empresa. No entanto em vez de considerar as tradicionais quatro perspetivas, considera quatro motivações de melhoria focadas em processos, como se pode visualizar na seguinte figura.

Figura 20 – Motivações de melhoria

Fonte: Adaptado de "Sistemas de Informação Organizacionais", Coelho, 2005: 164

A estratégia da organização deverá ser influenciada pelo interesse dos investidores em gerar resultados, que consequentemente deverá satisfazer os clientes e motivar colaboradores, dando um contributo à sociedade em que a empresa se insere, evidenciando aqui a importância dos *stakeholders*, por contraposição ao modelo de BSC.

São várias as ferramentas utilizadas para proceder a um controlo de gestão mais eficaz, que permitem avaliar a *performance* organizacional. No entanto, O BSC conjugado com a elaboração dos mapas estratégicos é cada vez mais privilegiado na área de SI por permitir alinhar numa visão integrada SI´s e a restante gestão (Selig, 2008). Norton e Kaplan (2006) designam o alinhamento como uma fonte de valor económico.

O BSC, em detrimento de outras metodologias por dar ênfase na perspetiva de aprendizagem e crescimento ao capital da informação, que embora considerado intangível, contribui largamente para a realização dos resultados quando corretamente alinhado com a estratégia, ganha cada vez mais expressão na medição da *performance* também dos SI´s.

3. Apresentação da Organização

Este capítulo tem por intuito fazer uma caracterização aprofundada da empresa, relativamente ao que se revela importante para o Estudo de Caso, nomeadamente no que se refere aos objetivos estratégicos, serviços prestados, missão, visão, valores, estrutura organizacional, recursos humanos, sistemas e tecnologias de informação e instalações físicas.

A empresa alvo do estudo de caso, Motor, cujo nome é fictício por questões de confidencialidade, é um concessionário automóvel que pertence a um conceituado grupo nacional. Parte da informação que se segue foi retirada do *site* do grupo em questão, uma vez que é transversal a todas as empresas do grupo, nomeadamente no que se refere à caracterização, missão, visão e valores.

3.1. Caracterização

O grupo ao qual pertence o concessionário automóvel em estudo que teve o início da sua caminhada nos anos 40, com o surgimento de uma pequena empresa. Está atualmente concentrado numa SGPS com um *turnover* superior a alguns milhões de euros e é responsável por mais de seis mil postos de trabalho, distribuídos por diversos países.

A empresa mãe controla o grupo e é responsável pela gestão das participações, bem como pela definição da estratégia e da coordenação de todas as atividades de negócio. Esta é constituída por três grandes unidades de negócio: a primeira agrega o negócio industrial e da representação automóvel da marca principal, a segunda engloba o negócio de retalho automóvel multimarca para o mercado ibérico, e por fim, a terceira constitui o negócio na área das tecnologias de informação.

A segunda, na qual está inserida a empresa alvo do estudo de caso, representa o forte investimento que o grupo tem vindo a efetuar no retalho automóvel com o objetivo de ser líder no retalho multimarca ao nível da Península Ibérica, através de um crescimento sustentado assente num plano de aquisições, onde comercializa e tem pontos de assistência de conceituadas marcas automóveis.

O grupo, apesar do longo caminho que percorreu desde o seu início até hoje, continua determinado em crescer e afirmar-se no contexto exigente da Europa e da globalização do mercado mundial, seguindo sempre de perto o lema do seu fundador: “sempre presente na construção do futuro”.

O concessionário em questão existe desde 2001, tendo sido adquirido pelo grupo supra caracterizado em 2006. A marca comercializada na empresa goza de um prestígio de qualidade que se deve ao facto de ser de origem francesa, a par de outra que é igualmente produzida pelo grupo PSA. Esta particularidade coloca as duas no mesmo grupo estratégico.

3.2. Objetivos Estratégicos

Os objetivos deste ano a nível do concessionário refletem os objetivos estratégicos do grupo, uma vez que são sempre parte integrante de uma estratégia formulada a médio-longo prazo ao nível do topo. O Diretor Geral, em conjunto com os Chefes de Vendas e de Oficina, elabora anualmente o orçamento e o plano de objetivos. Estes, por sua vez, são discutidos na sede do grupo junto da Administração em reunião anual.

Tendo em conta a conjuntura económica do país, foram estabelecidas metas menos ambiciosas para o concessionário, comparativamente ao ano transato. Tanto para o departamento de vendas como para a oficina foi perspetivado faturar no mínimo o mesmo que no ano anterior.

Os objetivos estratégicos do concessionário para o ano seguinte são apenas disponibilizados aos colaboradores no último trimestre de cada ano. No decorrer do estudo, que se iniciou em Janeiro e se estendeu até Dezembro de 2013, foi possível recolher informação relativa às metas a alcançar em 2014. Estas, apesar de o contexto de crise não ter apresentado melhoras significativas, mantiveram-se tanto na oficina, como nas vendas. O objetivo seria então igualar no mínimo o ano de 2013, no qual já não se conseguiu alcançar a igualdade relativamente a 2012.

3.3. Serviços Prestados

O concessionário atua em três áreas, sendo estas a comercialização de veículos, a manutenção/reparação automóvel e ainda a comercialização de componentes e acessórios.

No que respeita à comercialização de veículos, o concessionário é apenas responsável pela venda de viaturas novas ou de serviço da Peugeot. As viaturas de serviço normalmente são concedidas aos vendedores e diretores durante alguns meses, sendo posteriormente vendidas por um valor inferior. O concessionário aceita retoma de automóveis usados que são entregues pelos clientes em troca da viatura nova. Estas viaturas também são vendidas, mas por outra empresa do grupo, cujo *cuore business* é a venda de automóveis usados. O gabinete do vendedor de viaturas usadas, que apenas está presente em dias intercalados, localiza-se nas instalações do concessionário.

A manutenção/reparação automóvel e comercialização de componentes e acessórios são realizadas apenas para viaturas da marca. Na parte da manutenção há que considerar que a lavagem das viaturas é efetuada por um funcionário que é subcontratado a outra entidade externa e está presente todos os dias na empresa.

3.4. Missão, Visão e Valores

O grupo rege a sua atividade, tendo por base a sua **missão**: “Assumimos a nossa responsabilidade e o equilíbrio em todos os momentos da nossa atuação, através da inovação e melhoria constante dos nossos produtos e serviços, sustentados em bons relacionamentos e em justas propostas de valor”.

No que se relaciona com a projeção futura a longo prazo, o grupo tem como linha orientadora a **visão**: “Acreditamos que a solidez das nossas relações garante negócios de sucesso” e guia-se por **valores** como a Confiança, Solidez, Evolução, Responsabilidade e Relacionamento.

3.5. Recursos Humanos

A empresa apresenta uma estrutura organizacional centralizada em dois grandes departamentos que respondem ao Diretor Geral, o de Vendas e o de Oficina (figura 21). A chefia da oficina conta com uma linha de apoio especializada de um Conselheiro Técnico, que dá algumas sugestões quando solicitadas e auxilia na resolução de eventuais problemas de cariz mecânico, mas não tem capacidade de decisão. Todas as decisões estratégicas do concessionário são tomadas pelo Diretor Geral.

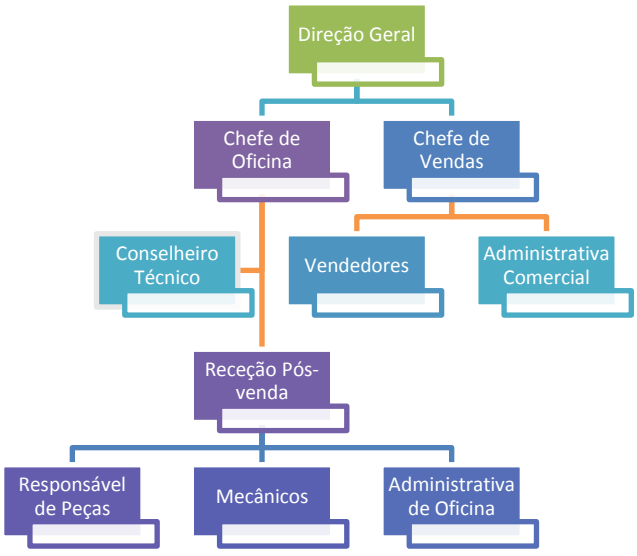

Figura 21 – Organograma do Concessionário

Na dependência do Chefe de Oficina, cujas principais funções são garantir que todos os procedimentos definidos para o departamento são postos em prática e tomar decisões relativamente a questões de maior responsabilidade, como aprovar orçamentos de maior valor,

está a Receção Pós-venda, que tem como objetivo assegurar a manutenção e reparação automóveis e ainda a comercialização de componentes e acessórios para o exterior.

A Receção Pós-venda conta com um Responsável Pós-venda, cuja função é assegurar a relação direta com os clientes de oficina no que toca a marcações de revisão ou reparação, à receção e entrega de viaturas, à inspeção da viatura quando chega e é entregue, ao registo de diagnóstico do problema transmitido pelo cliente inicialmente e à elaboração de orçamentos por solicitação do cliente.

Na dependência do Responsável Pós-venda há um Responsável de Peças, que autoriza todas as entradas/saídas de peças, tanto para incorporação no serviço de oficina como para o cliente externo. A equipa dispõe também de quatro Mecânicos todos certificados pela marca, que diagnosticam numa primeira instância problemas nas viaturas, recorrendo ao Conselheiro Técnico quando necessário, e asseguram todas as revisões e reparações das viaturas, após veredito final também por parte do cliente. Por fim, a Administrativa encarrega-se de toda a documentação relacionada com este setor.

Encarregue da Chefia de Vendas, cujas principais funções são garantir que todos os procedimentos definidos para o departamento são postos em prática e tomar decisões relativamente a questões de maior responsabilidade, como aprovar propostas de clientes, estão três vendedores.

Estes vendedores que tentam angariar novos clientes para conduzir o processo de venda de viaturas novas ou de serviço, tanto durante a semana no concessionário, como em eventuais eventos que decorram no fim-de-semana. O tempo despendido nestes eventos não é considerando no valor da remuneração base, sendo a sua grande vantagem potenciar a probabilidade de vendas, já que são frequentados por pessoas em massa que estão mais predispostas a decidir pela compra em função das campanhas em curso. Apesar de estes profissionais se encontrarem todos diariamente no concessionário repartem em dias intercalados a atribuição das comissões. Este departamento conta também com a Administrativa Comercial, que dá encaminhamento a toda a documentação correspondente às vendas.

A senhora que é Responsável pela Limpeza presta este tipo de serviço aos dois departamentos, pelos que responde às duas chefias. Atende por vezes o telefone, desde que a equipa de rececionistas ficou reduzida a uma pessoa. Esta tarefa apesar de não fazer parte das suas atribuições é de desempenhada com o intuito de ajudar o colega, o que revela um forte espírito de entreajuda fomentativo de um bom ambiente de trabalho.

A equipa do concessionário conta neste momento, após as reduções referidas, com dezasseis funcionários, estando distribuídos da forma pelos departamentos da forma evidenciada no seguinte quadro.

Cargo	Nº
Diretor Geral	1
Chefe de Oficina	1
Chefe de Vendas	1
Conselheiro Técnico	1
Responsável de Receção Pós-venda	1
Responsável de Peças	1
Administrativas	2
Mecânicos	4
Vendedores	3
Responsável pela limpeza	1

Quadro 1 – Quadro de Pessoal

Como é visível no quadro, na empresa apenas se encontram os trabalhadores diretamente envolvidos no *cuore business* da empresa. Todos os serviços de apoio, como Contabilidade, Recursos Humanos, Sistemas de Informação, Marketing, etc. estão centralizados na sede do grupo.

A equipa de recursos humanos é relativamente estável, não havendo grande grau de rotatividade. No entanto, é de referir que entre 2011 e 2012, em função da conjuntura económica, houve redução de pessoal, nomeadamente de um rececionista, um central de reservas, dois mecânicos e três bate-chapas.

A equipa de vendas, por sua vez, manteve-se, estando prevista a contratação de mais vendedores para o ano seguinte (2014). A equipa aumentará, assim como os objetivos individuais de cada vendedor para que lhes sejam distribuídas as comissões, que só são acrescidas ao salário base a partir de um determinado valor de vendas alcançado. A remuneração base de cada vendedor também será reduzida.

A política salarial praticada a nível de concessionário não difere muito da concorrência direta, tanto a nível de venda como de oficina, o que não incentiva muito à rotatividade.

3.6. Caracterização de SI/TIC

Todas as questões relacionadas com Sistemas e Tecnologias de Informação são administradas e por uma empresa do grupo, que se dedica apenas a este setor.

Existem na empresa nove computadores fixos, seis portáteis e cinco impressoras.

Todos os colaboradores têm acesso a todos os computadores, excetuando os mecânicos que dispõem de dois computadores, um localizado no piso 0 e outro na cave, nos quais apenas registam as suas entradas e saídas da empresa e a senhora da limpeza.

Existe também um computador no stand apenas destinado ao acesso de clientes.

O edifício onde está localizado o concessionário é composto por três pisos.

A cave, onde funciona a oficina;

Piso 0, onde opera o stand;

Piso 1, onde estão localizados os serviços administrativos.

O servidor está localizado no primeiro andar na mesma sala que o cofre, na qual qualquer funcionário pode entrar, desde que solicite primeiro a chave à administrativa comercial.

Ao lado da sala encontra-se o gabinete dos vendedores dos usados, que pertencem a outra empresa do grupo. Atrás está uma sala comum, na qual está localizada um arquivo com pastas relativas ao departamento de vendas, que contém processos de clientes. Em frente à sala estão casas de banho e a copa.

A empresa trabalha com três aplicações, sendo estas as seguintes:

- Autoline, que faz a gestão de vendas e de oficina (faturação, gestão de stocks, gestão de clientes e fornecedores);
- Service Box, que faz a gestão do produto (interligação com a marca);
- Intra, que faz a gestão de pessoal (oportunidades de trabalho, direitos e deveres dos trabalhadores, disponibilização de recibos, informação de protocolos com empresas).

4. Estudo de Caso

Este estudo de caso assume-se como uma pesquisa organizacional que pretende evidenciar através de uma apropriada análise, aspetos relevantes a nível de informação e sua segurança que poderão comprometer a estratégia como um todo quando descurados.

4.1. Introdução ao Estudo de Caso

A metodologia mais adequada à investigação e estudo de SI´s, já se tendo justificado anteriormente, é o *case study*. Revela-se ainda mais adequado dadas as formas possíveis de recolha de dados pois não requer controlo comportamental sobre os eventos, focando-se em fenómenos do dia-a-dia.

De acordo com Yin efetuar uma investigação baseada num estudo de caso envolve todas as etapas evidenciadas na seguinte figura de uma forma mais simplista, que vai de encontro aos passos sugeridos pelo mesmo autor noutras publicações, uma delas já referida no subcapítulo da "Metodologia".

Figura 22 – Etapas de um *Case Study*

Fonte: "Investigação em Sistemas de Informação Organizacionais – Teses e Dissertações em Portugal", Yin, 1994, citado por Grilo, 2008: 42

Depois de se ter selecionado a metodologia do estudo de caso, procede-se à pertinente revisão bibliográfica que versa acerca da temática, incluindo teoria e boas práticas, sendo um dos passos do desenho. Seguidamente trata-se da preparação da recolha de dados, que envolve decidir acerca de que informação será necessária e como consegui-la. Nesta fase decide-se que técnicas de recolha de dados se devem utilizar, o que determina o sucesso da etapa de recolha propriamente dita. Na recolha de dados procede-se à condução do estudo propriamente dito, de forma a obter a informação junto dos intervenientes. Por fim, executa-se a sua análise, tiram-se conclusões e reporta-se o estudo de caso de forma a futuramente produzir teoria baseada no mesmo.

4.2. Âmbito

Vimos anteriormente que a empresa tem como objetivo estratégico principal fidelizar clientes, pelo que toda a informação relacionada com os seus contatos, propostas de preços e campanhas promocionais a realizar deverá ser mantida em sigilo, tanto quanto possível.

Tendo em conta que existe um SI em funcionamento na empresa, que abrange todos os setores e atendendo ao facto de toda a informação relativa a clientes ser de suma importância, o estudo incidirá neste âmbito sob os departamentos de Vendas e Oficina.

Pretende-se assim identificar vulnerabilidades e ameaças a que esta informação crítica de negócio esteja sujeita, identificando posteriormente ações que permitam solucionar o problema, que serão alvo de medição de performance recorrendo ao BSC.

4.3. Pressupostos

Uma vez que o estudo foi efetuado sob sigilo, não foi possível obter toda a informação desejável. Yin (2009) recomenda que se escolha um alvo de estudo no qual se possa ter acesso a toda a informação que permita responder às questões colocadas inicialmente.

A primeira entidade alvo do estudo, na qual a autora desta dissertação prestava serviços externos de consultoria/formação foi selecionada pelo facto de, aquando da realização de um pequeno trabalho introdutório de seminário, se ter revelado recetiva e incentivadora deste tipo de iniciativas. No entanto no momento em que lhe foi apresentada o plano de dissertação, a Direção Executiva acabou por gentilmente se demonstrar indisponível para colaborar, o que fez com que a problemática inicial deixasse de fazer sentido, já que esta e o próprio tema tinham sido selecionados de forma a ir de encontro a uma necessidade identificada nesse pequeno trabalho inicial.

Como tal, foi indispensável providenciar um plano alternativo, incluindo algumas reformulações não muito profundas nos objetivos e título, por forma a adaptar o trabalho à nova entidade escolhida. Nesta nova organização optou-se por realizar o estudo sob sigilo, para mais uma vez não correr o risco de não obter autorização.

Assim, não foi possível averiguar a existência de um SGSI na organização, que só seria possível alcançar com autorização por parte da empresa que administra os SI´s. Parte-se do pressuposto que num grupo desta dimensão, com uma subsidiária que se dedica somente à área dos SI´s, disporá de um SGSI, pelo que o objetivo será evidenciar alguns aspetos comprometedores da segurança de informação que possam colocar em causa a execução da estratégia definida para a empresa.

A mesma ordem de ideias será seguida para outras questões às quais não foi possível obter resposta, pois só assim este estudo fará sentido.

4.4. Recolha, Tratamento e Análise dos Dados

Segundo Yin (2009) a recolha de dados é uma tarefa que poderá por vezes ser morosa e levar a coleta de informação que não seja suficientemente relevante para o estudo do fenómeno do *case study*. Assim sendo, é importante que o investigador se foque no importante e para isso é necessário ser bastante conhecedor do assunto em questão e estabelecer listas do que deseja recolher. Esta tarefa facilitará a posterior análise de dados.

4.4.1. Recolha de Informação

É habitual a escolha desta metodologia contemplar a utilização de múltiplas fontes de dados, embora tal não seja obrigatório. Observação e entrevista são as técnicas principais na recolha de dados quando se usa como metodologia o *Case Study*. Dependendo do fenómeno a observação pode ser usada como única técnica de recolha de dados, ou noutros casos, a da entrevista.

De acordo com Yin (2009) as entrevistas podem assumir vários níveis, sendo que neste caso em concreto, como o estudo foi desenvolvido em sigilo, foi entrevistado apenas um dos colaboradores da empresa. As entrevistas foram realizadas a um indivíduo só, mas acerca dos processos da organização. Algumas da entrevistas foram estruturadas tendo por base um guião que reflete tanto as questões iniciais do estudo como os controlos das boas práticas selecionadas; outras foram desenvolvidas pelo fluir da conversa, dando preferência a questões iniciadas por "como" para não criar uma posição defensiva no entrevistado, por recomendação de Yin (2009). Esta técnica apresenta como vantagem o facto de permitir cumprir os tópicos do guião, revelando-se menos benéfica porque o entrevistador pode fazer refletir nas questões algum grau de subjetividade e como consequência o entrevistado pode ter tendência a responder aquilo que o primeiro deseja ouvir.

A observação direta foi a outra fonte de dados, que apresenta como vantagens cobrir os factos em tempo real e no seu contexto, podendo porém ser bastante morosa. Esta técnica foi aplicada de forma discreta através de algumas deslocações às instalações, a título de visita ao colaborador que forneceu grande da informação que tornou possível a realização deste estudo de caso.

O estudo conjugou assim a recolha de informação de forma confidencial com os dados fornecidos de forma voluntária/pública para o exterior através dos sites da empresa e do grupo em questão.

A metodologia de *case study*, apesar de ser a mais adequada ao estudo de SI, e por este motivo ter sido a escolhida, revelou-se muito complicada de executar pois há muita relutância em disponibilizar informação, já que os próprios entrevistados temem pelo seu posto de trabalho ao revelar caraterísticas da empresa. Este facto vai de encontro a algumas das boas práticas relativas à segurança de informação, nomeadamente no que toca a revelar dados acerca da entidade. Por isso houve o cuidado de não recolher dados, nomeadamente acerca de questões que pudessem comprometer a estratégia da empresa.

A fase da recolha de dados também acaba por se revelar árdua porque há acesso a informação relacionada com áreas não diretamente relacionadas com o que se pretende investigar, principalmente aquando das entrevistas informais. Por isso, de acordo com Yin (2009), é importante manter o foco e seguir o protocolo, tanto quanto possível, deixando em simultâneo algum grau de subjetividade de lado.

Seguindo o exemplo de Ferreira (2010), decidiu-se construir um quadro no qual é possível verificar quais as principais fontes de dados do estudo, estando estas repartidas por duas dimensões, interna e externa.

Externas	Revisão Bibliográfica	Estratégia
		Informação estratégica e Estratégia em SI
		Segurança de Informação
		Sistemas de Medição de Performance Organizacional: BSC
	Legislação	Boas Práticas em Segurança de Informação
	Dados acerca de empresas concorrentes	Alguma informação recolhida de forma a fazer breve análise de pontos fortes e fracos da entidade
Internas	Missão, Visão e Valores	Linhas de Atuação da empresa a Médio/Longo Prazo e Relacionamento com Clientes
	Objetivos Estratégicos Anuais	Linhas de Atuação da empresa no Curto Prazo
	Caraterização da empresa	Recursos Internos
	Processos Internos	Formas de alcançar estratégia (observação direta e entrevista)

Quadro 2 – Etapas de um *Case Study*

Por recomendação de Yin (2009) devem-se confrontar as evidencias recolhidas e sua análise com diferentes explicações e interpretações.

Assim, no campo das fontes externas, a revisão bibliográfica proporciona-nos a verificação do estado de arte acerca das temáticas a aplicar no estudo de caso, observando diferentes interpretações; a legislação permite-nos averiguar se estão a ser utilizadas as boas práticas recomendadas para que se proteja a informação crítica; e, por fim, a comparação com a concorrência permite ajudar a identificar pontos fortes e fracos, perceber qual a informação que impreterivelmente terá que ser salvaguardada e até que ponto poderá a concorrência estar interessada nessa informação.

A nível de informação interna, esta permite-nos perceber numa primeira fase, qual a direção que a empresa quer seguir e com que recursos e processos está a tentar alcança-la. A caracterização da empresa permite-nos também, identificar através da sua análise, os seus pontos fortes e fracos.

4.4.2. Tratamento e Análise de Dados

Yin (2009) enfatiza a importância que se deve dar à forma como se irá expor as evidências, pois deverá permitir ao leitor conseguir interliga-las com as questões a que este estudo se propôs responder. É recomendável organizar a informação em quadros ou matrizes para facilitar a sua leitura.

4.4.2.1. Análise de Pontos Fortes e Fracos da Empresa

Apesar de a temática da estratégia fazer parte deste estudo de caso, não é esta a principal. O que se pretende ao referi-la é enquadrar nos seus propósitos a segurança de informação. Assim, a análise de pontos fortes e fracos que se apresenta seguidamente é feita de uma forma não muito aprofundada, somente com o intuito final de apoiar a produção de um possível do mapa estratégico da empresa, e fundamentar a importância de proteger a informação de negócio dos principais competidores.

Caracterização da concorrência para Vendas:

As cinco forças de Porter, já caraterizadas no capítulo da Revisão Bibliográfica permitem fazer uma análise estratégica relativamente ao setor, sendo neste caso o automóvel. É uma importante etapa em termos de avaliação concorrencial, mas acaba por ser muito abrangente.

Neste sentido, torna-se adequado recorrer à análise por grupos estratégicos, que se foca somente nos concorrentes significativos dentro da indústria automóvel, ou seja, nos que seguem estratégias semelhantes. Müller-Stewens e Lechner (2005), relacionando as variáveis de Preços Médio do Produto vs Largura da Linha de Produtos, consideram o mapa de grupos estratégicos evidenciado na figura seguinte.

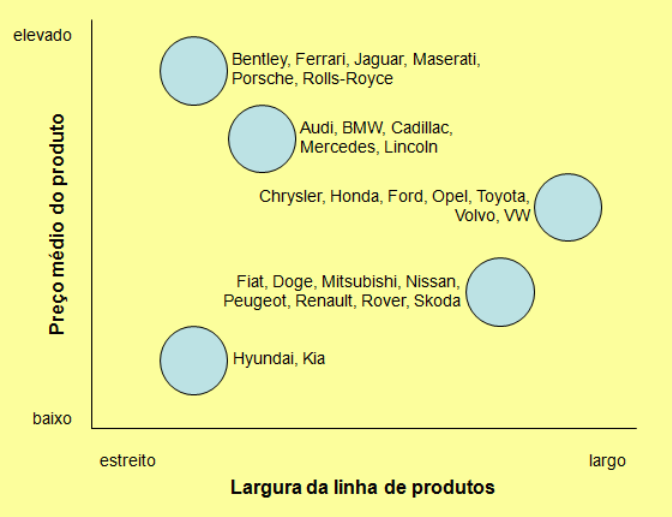

Figura 23 – Grupos estratégicos dentro do setor automóvel

Fonte: "Strategisches Management", Müller-Stewens e Lechner, 2005

Tendo em consideração os critérios do autor são considerados como concorrentes diretos os detentores das marcas Fiat, Doge, Mitsubishi, Nissan, Renault, Rover e Skoda. No contexto português seria de considerar também a Citroen, considerada aliás por Freire (1995), no que toca às viaturas em estado novo, já que que é do mesmo produtor e segue a mesmo modelo de construção. A Seat poderia ser incluída, no que toca ao preço médio do produto, não tendo porém uma gama de produtos tão alargada.

De acordo com Freire (1995), depois de analisar cuidadosamente os recursos internos da empresa, tarefa que foi efetuada no capítulo da caracterização da empresa, há que comparar sistematicamente a empresa com os seus competidores, recorrendo à técnica do *Benchmarking.* Só após a conclusão destas etapas, se está em condição de listar os principais pontos fortes e pontos fracos.

Como pontos fortes, a Peugeot tem a seu favor o facto de ser uma marca produzida em França, o que a faz gozar de um certo prestígio já que normalmente isto é sinónimo de qualidade. Porém, esta vantagem deixa de ser um ponto forte quando comparada com a Renault ou Citroen. No entanto, a Citroen, antes de se juntar ao grupo PSA era vista como inferior, desvalorizando muito no mercado dos usados em comparação com a Peugeot e com a Renault. Comparativamente com todas as outras marcas do mesmo grupo estratégico, a par mais uma vez da Renault e da Citroen, apresenta uma diversificada gama de produtos que é bastante comercializável. Como competência distintiva, a Peugeot apresentou no ano de 2014 um modelo que foi considerado como carro do ano.

Como pontos fracos, em programas e fóruns da especialidade são apontadas as questões estéticas, superando ainda assim a Skoda. No entanto, o modelo utilitário que foi considerado

como carro do ano, destaca-se justamente pelo *design*, qualidade e baixo consumo, segundo publicação online da Deco Proteste (2014).

No que toca ao grupo, este tem como pontos fortes o facto de ter anos de experiência no ramo automóvel, tendo inclusivamente sido considerado como um caso de sucesso a nível de estratégia de acordo com Freire (1995). Não foram encontrados pontos fracos relativamente a outras concessões da marca em Portugal, excetuando as desvantagens que o grupo possa apresentar relativamente ao importador da Peugeot, já que em termos de integração vertical este terá vantagens a montante que o grupo em questão não tem, por não ser produtor da marca. Tais benefícios poderão traduzir-se em economias operacionais na distribuição, acesso à informação e em poder negocial. No entanto esta não integração vertical no que respeita ao processo de I&D (Investigação e Desenvolvimento) e produção também têm vantagens, que foram focadas no capítulo da revisão bibliográfica.

Caracterização da concorrência para Oficina:

De acordo com um relatório emitido pela ANECRA (Associação Nacional das Empresas de Comércio e Reparação Automóvel) (2013) houve menos procura por serviços de reparação ou manutenção na marca. Tal deve-se ao surgimento de algumas oficinas de reparação multimarca *low cost*, sendo estas mais procuradas no atual panorama económico.

Este tipo de oficinas, apesar de não fazer parte do mesmo grupo estratégico, mas sim do mesmo setor, faz concorrência aos concessionários das marcas. Neste caso faz sentido analisar as cinco Forças de Porter. A concorrência entre competidores atuais, uma vez que se tem verificado uma guerra aberta de preços através de constantes campanhas publicitárias e extensões de garantia. Algumas barreiras à entrada neste setor, nomeadamente no que se relaciona com requisitos de capital e economias de escala fazem com que a quantidade de concorrentes com um nível de serviço próximo do da marca não aumente. O poder negocial dos fornecedores pesa aqui bastante, principalmente se os competidores aplicarem no serviço por solicitação do cliente, peças da marca, pois os preços e prazos de entrega poderão ser superiores. Pesa aqui o fator da cadeia de valor. Por fim, também o poder negocial dos clientes se mostra importante num momento em que a oferta supera a procura e o preço de compra tem que apresentar a melhor relação qualidade-preço, principalmente numa sociedade de consumidores bem informada com a de hoje.

Algumas destas oficinas estão associadas a hipermercados, como é o caso da Roady que pertence ao grupo do Intermarché ou da oficina do Jumbo. A Precision, Midas e a Norauto prestam um nível de serviço superior semelhante ao da marca, seguindo também os seus requisitos de revisão oficial do construtor para efeitos da garantia. Porém, há muitos clientes a recorrer a oficinas multimarcas que não pertencem a grupos ou *franchisings*, sendo de

particulares, que poderão prestar um bom serviço, mas na sua maioria não cumprem requisitos a qualquer nível.

Como pontos fortes por fazer a manutenção/reparação na marca referem-se os seguintes: os mecânicos e conselheiros técnicos têm formação específica na marca que é constantemente atualizada, os equipamentos de diagnóstico e restantes estão direcionados para a marca, as peças utilizadas são sempre da marca, é concedida ao cliente uma garantia tanto relativa às peças como ao serviço da marca e cumpre todos os requisitos certificados pela APCER no que respeita a instalações e tratamento de resíduos. Estes têm um encaminhamento adequado, ou seja, para que não sejam derramados no solo são recolhidos por entidades externas como é o caso da Safetykleen Portugal, que recicla muitos destes resíduos.

Como ponto fraco principal a apontar, refere-se o preço que é cobrado pelos serviços de manutenção e reparação, facto esse que se prende com a especialização que é fornecida pela marca.

4.4.2.2. Áreas Críticas de Sucesso a Proteger

Da análise da missão, visão e valores, bem como dos objetivos estratégicos, apenas fornecidos em termos de valores, se pode inferir que a fidelização e conquista de clientes são alvos do concessionário.

Neste sentido, são realizadas constantemente campanhas promocionais a nível da marca, do grupo ou só do concessionário, sendo algumas permanentes e outras temporárias. A título de exemplo de campanha permanente, a marca concede a todos os clientes detentores de viaturas com mais de cinco anos, direito a desconto de 30% na manutenção, já que é a partir deste momento que, em regra, deixam de recorrer à marca para fazer reparação e manutenção automóvel. Para além desta campanha permanente, ao longo do ano vão surgindo outras que duram normalmente entre um a dois meses, como é exemplo a campanha que está neste momento a decorrer na compra do modelo 208, que a marca dá três mil euros na troca do carro antigo. Todas as campanhas supra descritas são do conhecimento geral.

Existem, no entanto, outras campanhas para frotistas, que poderão ser pessoas particulares ou empresas, desde que possuam pelo menos três viaturas da marca. A este tipo de clientes poderão ser dadas condições especiais personalizadas, que normalmente são acordadas em reunião com a respetiva direção.

Para além disso, quando uma determinada viatura é seguida no concessionário, há sempre a vantagem de possuir um histórico que permita que em cada revisão de ano para ano se substitua apenas o que é estritamente necessário. Tal não acontece quando se muda para a concorrência direta em termos de manutenção.

Como já foi mencionado, Freire (1995) evidencia a importância dos grupos estratégicos e a empresa alvo do estudo de caso faz parte de um grupo estratégico. Como tal, há o perigo de concorrentes que façam parte do mesmo grupo estratégico tentarem, recorrendo ao *Bechmarking* Estratégico, comparar a sua *performance* com a da empresa, repetindo as suas boas práticas relativamente às áreas críticas de sucesso.

Este tipo de *Bechmarking* é designado como concorrencial e normalmente é o mais difícil de concretizar, já que teria que existir cooperação por parte do competidor, o que raramente acontece por razões óbvias. Assim sendo, os competidores interessados em fazer uso desta ferramenta estratégica, vendo o acesso à informação dificultado, poderão tentar obtê-la de outras formas.

Pelo que, toda a informação relacionada com contatos de clientes, orçamentos e propostas efetuados de forma personalizada, histórico, etc.. deverão ser alvo de uma proteção especial.

4.4.2.3. Identificação dos Ativos de Informação

A identificação dos ativos de informação a proteger corresponderá a uma listagem de tudo o que a organização assume como relevante, relacionado com Informação e SI, para as atividades críticas de negócio (ISO/IEC 27002:2013). Assim sendo, passam-se a listar estes ativos no seguinte quadro.

Grupo	Ativo
Informação	1. Estudos de Mercado
	2. Propostas de Bancos
	3. Protocolos e Acordos
	4. Outra Documentação em Papel
Bases de Dados	1. Produtos
	2. Vendas
	3. Clientes
Hardware	1. Servidores
	2. Computadores fixos
	3. Portáteis
	4. Impressoras
Software Aplicacional	1. Autoline

	2. Service Box
Software Operacional	1. Correio Eletrónico
	2. Gestão de Acessos
Pessoas	1. Diretor Geral
	2. Responsáveis Vendas/Oficina/Peças
	3. Responsável de Oficina
	4. Administrativos
	5. Mecânicos
	6.Vendedores
	7. Conselheiro Técnico
Outros Ativos Físicos	1. Espaço físico
	2. Instalação Elétrica

Quadro 3 – Lista de Ativos de Informação

O quadro acima evidenciado tem como objetivo final identificar tudo o que poderá estar vulnerável ou sujeito a ameaças e que, por sua vez, possa comprometer todo o processo de proteção da informação crítica de negócio.

4.4.2.4. Mapa Estratégico para a Organização

Seguidamente é apresentado um possível Mapa Estratégico com exemplos de indicadores a considerar no caso da Motor, tendo em conta as quatro perspetivas consideradas por Kaplan e Norton (2004) e toda a informação a que se teve acesso relativamente à missão, visão, valores e objetivos estratégicos.

Na figura são evidenciadas também as relações de Causa-Efeito, que segundo os autores Kaplan e Norton são um dos três princípios fundamentais do BSC. Estas relações são essenciais, pois como refere Norreklit (2000), com base nas medidas concebidas para áreas não financeiras é possível fazer prognósticos para medidas financeiras futuras.

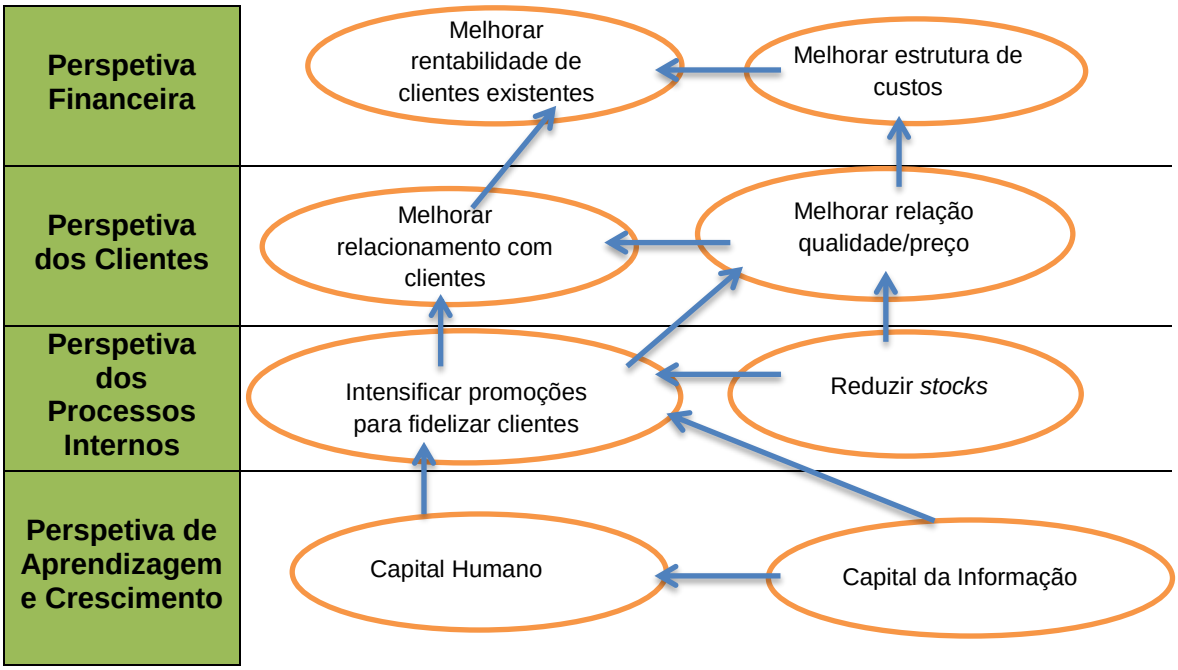

Figura 24 – Possível Mapa Estratégico da "Motor"

Perspetiva de Aprendizagem e Crescimento

A questão do Capital Humano reveste-se de crucial importância, pois a motivação dos colaboradores é essencial e estes deve sentir-se valorizados. O facto de os objetivos de vendas se terem tornado mais ambiciosos poderá eventualmente gerar desmotivação e mais rotatividade de vendedores, uma vez que foram estabelecidas metas elevadas. Estes poderão sentir necessidade de procurar empresas concorrentes nas quais tenham um salário base mais elevado e objetivos mais atingíveis, que levarão à consequente atribuição mais facilitada das comissões.

No entanto, o grupo promove o desenvolvimento de uma cultura dinâmica, aberta à mudança, fomentando a criatividade interna e participação de todos os colaboradores.

O Capital da Informação torna-se importante pelo já explanado na revisão bibliográfica e ao longo de todo o trabalho. Aqui poderá incluir-se o compromisso de desenvolver um ambiente propício à inovação e à melhoria continua preconizado pelo grupo como um dos seus pilares, numa vigilância sistemática do mercado e da tecnologia, em colaboração com uma rede de parceiros.

Perspetiva dos Processos Internos

Esta perspetiva reveste-se de particular importância porque determina ou impacto direto n perspetiva seguinte (Clientes). Nesse sentido, intensificar as campanhas promocionais é importante para fazer face à concorrência, que apesar de apresentar um nível de serviço inferior quando comparado com o da marca, no contexto atual ganhou expressividade pelo preço. Desta

forma, consegue-se apresentar ao cliente uma proposta de valor acrescentado, com melhor relação qualidade/preço do que a concorrência consegue apresentar. Aqui o capital da informação ganha expressividade, já que o acesso a informação privilegiada ajuda bastante na decisão relativamente às campanhas a levar a cabo. Estudos de mercado poderão mostrar-se particularmente úteis.

Reduzir *stocks,* sem no entanto comprometer o negócio, poderá ser útil, uma vez que ajudará a reduzir custos e logo o preço cobrado ao cliente. Uma vez que o grupo detém quatro concessionários poderá reduzir os modelos disponíveis no *stand,* fazendo circular as viaturas conforme seja solicitado pelo cliente ou acompanhar o cliente a outro concessionário. Efetivamente o concessionário já teve em *stock* noutros tempos um número substancialmente maior, tendo reduzido entretanto. Porém, pode minimizar mais o valor investido em inventários.

Perspetiva dos Clientes

O grupo afirma estar atento às necessidades dos clientes e consumidores e estimula a cooperação com parceiros estratégicos, no sentido de criar valor para os clientes. O objetivo será melhorar a relação qualidade/preço para atrair e fidelizar clientes, já que na atual conjuntura económica é fator primordial de decisão.

A face seguinte será prestar-lhes um atendimento personalizado, melhorando a relação com os mesmos. Para atingir este objetivo a empresa tem por hábito solicitar aos clientes o preenchimento de um inquérito após a prestação dos serviços.

Perspetiva Financeira

No que se refere ao objetivo de rentabilizar os clientes atuais, já foram explicadas as relações causa-efeito que poderão levar a isso.

Na melhoria da estrutura de custos, a questão de redução de *stocks* ajudará como já foi referido. Não haverá muito mais custos que o concessionário possa reduzir, já que dispensou todo o pessoal que poderia. E mais uma vez a falta de integração vertical a montante não permite reduzir os custos de produção.

O grupo também poderia optar por, numa fase posterior depois de rentabilizar os clientes atuais, tentar conquistar novos mercados através da estratégia de internacionalização da marca Peugeot em África, uma vez que já se encontra lá fortemente representado em dois países, mas com outras marcas.

4.4.2.5. Identificação dos Objetivos dos Controlos e dos Controlos

Depois de identificadas as áreas críticas de negócio e os ativos de informação, considera-se que estão reunidas as condições para selecionar os controlos da norma ISO/IEC 27002:2013 que deverão ser alvo de medição em termos de *performance* no BSC. Estes são visíveis no seguinte quadro.

Controlos	Controlo/Descrição	Objetivos
7. Segurança nos Recursos Humanos	7.1.2. Termos e condições dos contratos	Os contratos dos funcionários/terceiros deverão incluir cláusulas de confidencialidade e demais responsabilidades relativamente à segurança de informação
	7.2.2. Formação, educação e sensibilização sobre a Segurança de Informação	Todos os colaboradores deverão frequentar ações de formação/educação adequada acerca da temática da segurança de informação e respetivas atualizações em políticas e procedimentos organizacionais
9. Controlo de Acessos	9.3.1. Uso das *passwords*	Os utilizadores deverão seguir as práticas da empresa e fazer uso das suas *passwords*
	9.4.1. Restrições de acessos às Aplicações	O acesso à informação e às funções dos sistemas de aplicações deve ser restrita de acordo com a política de controlo de acessos
11. Segurança Ambiental e Física	11.1.2. Controlo físico das entradas	As áreas seguras deverão ser protegidas por controlos apropriados que assegurem que somente as pessoas autorizadas tenham acesso
	11.1.3. Segurança de escritórios, salas e outras instalações	A segurança física de escritórios, salas e outras instalações deverá estar definida e ser aplicada

Quadro 4 – Lista de controlos da norma ISO/IEC 27002:2013 a considerar na perspetiva de Segurança de Informação

Obviamente que quando a empresa tem um SGSI devidamente implementado, os controlos deverão ser aplicados na sua maioria, justificando a sua não aplicação no SOA (*Statement of Aplicability*). Aqui pretende-se apenas destacar os controlos, que por sua vez dão lugar a indicadores, alvo de medição no BSC. Procede-se no subcapítulo do BSC para a Segurança da Informação a uma justificação detalhada da escolha de cada controlo e respetivo indicador selecionado para medir a sua *performance*.

4.4.2.6. Novo Mapa Estratégico para a Organização

De acordo com Norton e Kaplan (2004), o capital da informação e tudo o que lhe está relacionado é abrangido na perspetiva de Aprendizagem e Crescimento. Os autores defendem simultaneamente que poderão ser criadas outras perspetivas para além das quatro principais, assim se justifique no seio de cada empresa. Pelo que, de forma a facilitar a evidenciação do peso da segurança informação na estratégia da empresa, quando comparado com as restantes vertentes, optou-se por criar uma perspetiva apenas para a segurança de informação.

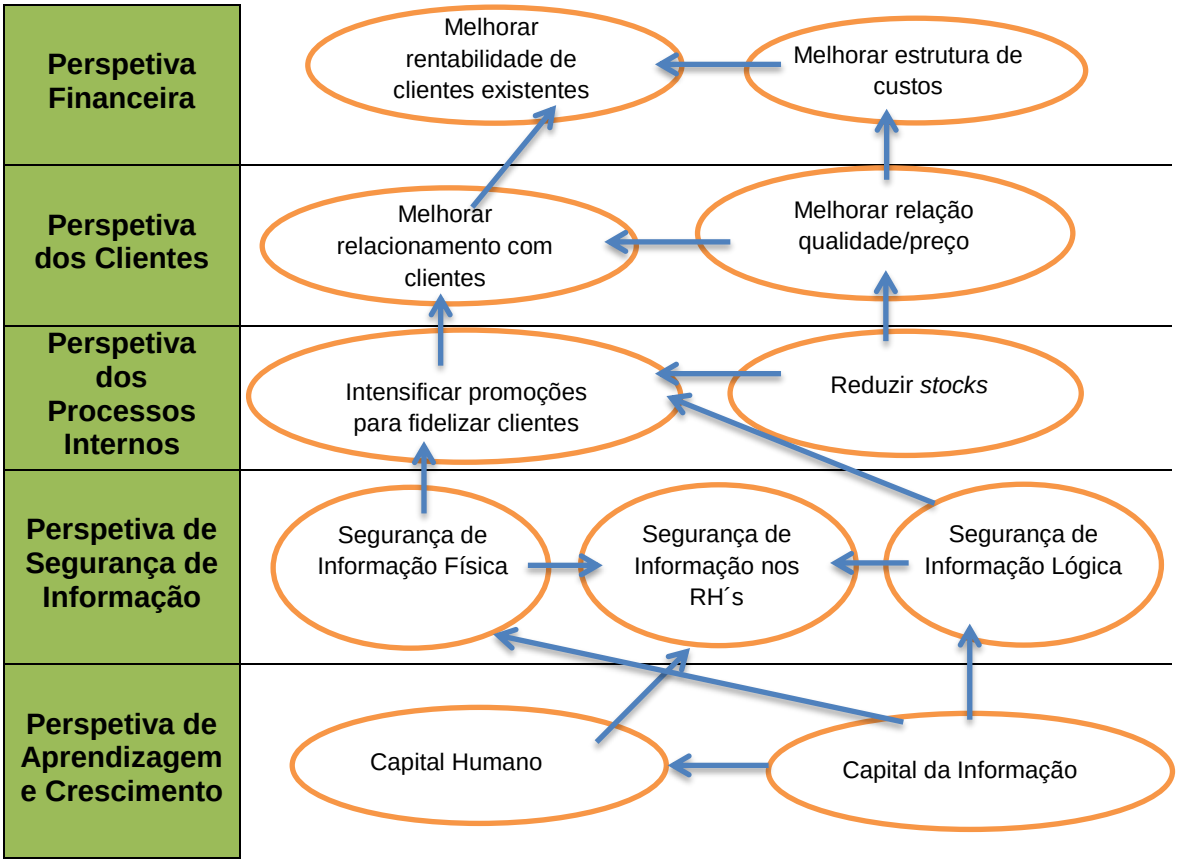

Figura 25 – Novo Mapa Estratégico da "Motor" contemplando perspetiva de Segurança de Informação

Se o objetivo final é rentabilizar os clientes existentes, então tudo o que diga respeito a campanhas e relacionamento com clientes deve ser alvo prioritário de proteção. É neste sentido que a nova perspetiva integrada no mapa estratégico vem trazer valor acrescentado.

4.4.2.7. BSC de Segurança de Informação para a Organização

É apresentado seguidamente o BSC, contemplando objetivos, indicadores, metas a atingir e respetivas ações a tomar, no caso de estas serem ou não atingidas.

Objetivos	Indicadores	Ponderação	Metas	Ações a tomar
Garantir a Segurança de Informação dos RH´s	% de Contratos com Compromisso de Confidencialidade (nº de contratos com confidencialidade/nº total de contratos)*100	**15%**	**100%**	Manter
			<100%	Incluir em todos os contratos Termo de Confidencialidade
	% de pessoas que frequentaram ações de Formação e Sensibilização sobre a Segurança de Informação (nº de formações em Segurança de Informação/nº total de formações)*100	**25%**	**100%**	Manter e ministrar novas ações atualizadas sobre o tema
			<100%	Organizar ações de formação e sensibilização sobre o tema e divulgá-las a todos
Garantir a Segurança a Nível Lógico das Aplicações com Informação Crítica	Nº de funcionários sem *password* que solicita a de colegas para aceder a aplicações críticas	**15%**	**0**	Manter
			>0	Providenciar *password* com gestão de privilégios adequada
	Nº de aplicações com informação crítica que não solicita *password*	**15%**	**0**	Manter e averiguar se existem outras aplicações nesta situação
			>0	Definir adequada gestão de acessos dos utilizadores
Garantir a Segurança a Nível Físico das Instalações com Informação Crítica	% de salas com informação crítica com controlo de entradas por cartão magnético (nº de salas com controlo magnético/nº total de salas)*100	**20%**	**100%**	Manter
			<100%	Instalar sistemas adequados de controlo magnético
	% de documentação altamente confidencial que é guardada em cofres de alta segurança	**10%**	**100%**	Manter
			<100%	Providenciar este tipo de instalações ou recorrer a *outsourcing* especializado

Quadro 5 – BSC aplicado à Segurança de Informação da empresa "Motor"

A escolha diferenciada da ponderação atribuída a cada um dos indicadores pretende dar ênfase a questões que na generalidade são mais descuradas em detrimento de outras. Procede-se de seguida a uma justificação detalhada da escolha de cada controlo e respetivo indicador selecionado para medir a sua *performance*.

Objetivo: Garantir a Segurança de Informação dos RH´s
Controlo: 7.1.2 - Termos e condições dos contratos
Indicador: % de Contratos com Compromisso de Confidencialidade

É importante que no momento da contratação se verifique a preocupação em incluir termos relativos às cláusulas de confidencialidade, alertando o funcionário de que terá acesso a informação classificada e confidencial que não poderá divulgar. Esta cláusula deverá fazer

menção às leis de direitos de autor e à lei de proteção de dados e deverá igualmente incluir responsabilidades associadas ao manuseamento de tudo o que esteja associado a essa informação, nomeadamente o acesso aos seus suportes e instalações, por exemplo. O colaborador deverá também ser sensibilizado a não divulgar informação relativa a partes terceira que contratem com a entidade, nomeadamente clientes, fornecedores ou parceiros. Por fim, o funcionário deverá ser alertado das ações a tomar no caso de as regras acima descritas não serem cumpridas.

A escolha deste controlo, sendo um dos que é transversal a todas as entidades, reveste-se de maior importância neste caso já que, apesar de a empresa ser relativamente estável em termos de rotatividade, houve redução de pessoal. Talvez este facto possa futuramente ganhar maiores proporções dada a conjuntura económica presente e que perspetiva para um futuro próximo. Também o facto de as condições salariais no momento serem idênticas para os profissionais especializados ao nível da concorrência e mais exigentes para a equipa de vendedores poderá gerar futuramente alguma rotatividade.

Faria sentido, a este nível, aplicar também os controlos 8.3.1, 8.3.2 e 8.3.3 da norma ISO/IEC 27002:2008 relativos à Responsabilidade pela Rescisão, Retorno dos Ativos e Remoção dos Direitos de Acesso, respetivamente, incluídos no título de Rescisão ou Alterações de Emprego. Estes controlos não estão contemplados na nova norma no âmbito da Segurança dos Recursos Humanos.

A escolha do indicador para proceder à sua medição prende-se com o facto de monitorizar efetivamente se todos os contratos contemplam a cláusula de confidencialidade.

Objetivo: Garantir a Segurança de Informação dos RH´s
Controlo: 7.2.2 – Formação, educação e sensibilização sobre a Segurança de Informação
Indicador: % de pessoas que frequentaram ações de Formação e Sensibilização sobre a Segurança de Informação

Um programa de segurança de informação deverá contemplar formas de sensibilizar os funcionários e outras partes terceiras envolvidas na empresa no que toca às suas responsabilidades perante a segurança de informação e acerca do impacto sobre a empresa no caso de não serem observadas. Isto deverá fazer partes das políticas e procedimentos da segurança de informação e deverá ser planeado tendo e consideração as funções de cada colaborador na organização.

Como se viu na revisão bibliográfica muitos dos problemas identificados na segurança da informação deve-se a erros humanos, voluntários ou involuntários. Se os colaboradores não

estiverem sensibilizados para este tipo de questões, mais facilmente serão levados a cometer este tipo de falhas.

A escolha do indicador parece ser a mais adequada para controlar a realização de ações de formação a este nível.

Objetivo: Garantir a Segurança a Nível Lógico das Aplicações com Informação Crítica
Controlo: 9.3.1. Uso das *passwords*
Indicador: Nº de funcionários sem *password* que solicita a de colegas para aceder a aplicações críticas

Todos os utilizadores deverão ser advertidos para o facto de que a sua autenticação para aceder a aplicações com informação confidencial deverá permanecer secreta, não devendo ser revelada nem a outras pessoas ou autoridades. A *password* também não deverá anotada em papéis, a menos que estes possam ser guardados num local onde mais ninguém tenha acesso. Esta *password* deverá ser modificada frequentemente e não deverá ser a mesma que se utiliza para fins pessoais. Deverá ser fácil de memorizar, porém complexa e que não faça menção a datas ou particularidades do utilizador fáceis de descobrir.

No caso do estudo faz sentido a escolha deste controlo porque a informação constante deste tipo de aplicações deverá estar altamente protegida a nível lógico, incentivando a que cada um dos utilizadores faça uso da sua autenticação privada.

A escolha do indicador prende-se com o facto de ser comum nas organizações em geral, colegas que não tê acesso a determinada aplicação, solicitarem a *password* de outros, muitas vezes quando estão a substituí-los ou com o intuito de os auxiliarem. Porém, o utilizador que divulga a sua *password* descura o facto de ficar exposto e não salvaguardado no caso de ocorrer algum erro na utilização do colega.

Objetivo: Garantir a Segurança a Nível Lógico das Aplicações com Informação Crítica
Controlo: 9.4.1. Restrições de acessos às Aplicações
Indicador: Nº de aplicações com informação crítica que não solicita *password*

Deverão existir restrições no que se relaciona ao acesso à aplicações de forma individual adaptadas às particularidades de cada uma, de acordo com o que está definido na política de controlo de acessos. Neste aspeto será fulcral definir perfis de acesso a informação dentro de cada uma das aplicações, bem como que autorizações tem cada um dos perfis, nomeadamente, se poderá só consultar ou também editar ou copiar essa informação.

A escolha deste controlo justifica-se mais uma vez porque a informação constante deste tipo de aplicações deverá estar altamente protegida a nível lógico, e muitas vezes nas entidades há determinadas aplicações ou bases de dados em Excel com propostas de clientes, por exemplo, que estão desprovidas de qualquer tipo de *password* de acesso.

A seleção do indicador vai de encontro à escolha do controlo e considera-se ser a melhor medida para averiguar a existência de aplicações que, aparentemente poderão não ter informação significativa, mas revestem-se de suma importância para o negócio. Pelo que deverão estar adequadamente protegidas.

Objetivo: Garantir a Segurança a Nível Físico das Instalações com Informação Crítica
Controlo: 11.1.2. Controlo físico das entradas
Indicador: % de salas com informação crítica com controlo de entradas por cartão magnético

As áreas seguras deverão estar protegidas com barreiras de acesso adequadas, por exemplo, através da conjugação de dois fatores como cartão de acesso e PIN. É recomendado que a entrada de visitantes seja registada e devidamente autorizada. É recomendado pela norma inclusivamente que os trabalhadores usem vestuário que os caracterize enquanto trabalhadores da empresa para identificar este processo.

A escolha do controlo justifica-se porque muitas vezes as salas dos servidores e dos arquivos não estão convenientemente protegidas e qualquer funcionário lhes pode ter acesso. Isto pode causar incidentes involuntários ou ações de má fé na procura de informação sigilosa.

O indicador escolhido pretende estreitar este tipo de acesso, usando pelo menos o controlo de entradas através de cartão magnético.

Objetivo: Garantir a Segurança a Nível Físico das Instalações com Informação Crítica
Controlo: 11.1.3. Segurança de escritórios, salas e outras instalações
Indicador: % de documentação altamente confidencial que é guardada em cofres de alta segurança

Salas ou escritórios com informação crítica deverão, antes de mais, estar completamente isoladas de forma a evitar o acesso ao público. Quando se justifique, edifícios onde conste informação confidencial deverão inclusivamente localizar-se em endereços completamente desconhecidos e sem identificação alusiva à empresa.

A aplicação deste controlo faz todo o sentido quando há informação sigilosa, como propostas de clientes empresariais ou contatos de fornecedores que queremos manter exclusivos perante a concorrência.

O indicador escolhido pretende avaliar se a empresa segue as boas práticas que vão de encontro às novas tendências no mercado, no que toca a proteger informação sensível. Há empresas especializadas que fornecem este tipo de serviço, como a EAD e a Urbanos, que são entidades cujo *cuore business* é armazenar arquivo, em qualquer formato, seja corrente ou morto. Estas entidades criaram salas cofre completamente impenetráveis e com acesso altamente condicionado de forma a proteger este tipo de informação. Inclusivamente no caso da Urbanos, o cofre situa-se em morada completamente desconhecida para a maior dos trabalhadores da própria entidade.

4.4.3. Análise dos Resultados da Segurança de Informação na Estratégia Organizacional

A análise de resultados privilegiará uma abordagem qualitativa pelos motivos anteriormente explicados no subcapítulo da metodologia.

Considerando os indicadores selecionados de acordo com as boas práticas de segurança de informação constantes na norma ISO/IEC 27005:2013, após recolher informação com base em *checklists* elaboradas para o efeito, foi possível tirar as ilações resumidas no quadro seguinte.

Objetivos	Indicadores	Metas	Ponderação	Resultados	Ações a tomar
Garantir a Segurança de Informação dos RH´s	% de Contratos com Compromisso de Confidencialidade ⬇ (nº de contratos com confidencialidade/nº total de contratos)*100	**100%**	**15%**	**100%**	Manter
	% de pessoas que frequentaram ações de Formação e Sensibilização sobre a Segurança de Informação ⬇ (nº de formações em Segurança de Informação/nº total de formações)*100	**100%**	**25%**	**0%**	Organizar ações de formação e sensibilização sobre o tema e divulgá-las a todos
Garantir a Segurança a Nível Lógico das Aplicações com Informação Crítica	Nº de funcionários sem *password* que solicita a de colegas para aceder a aplicações críticas	**0**	**15%**	**0**	Manter
	Nº de aplicações com informação crítica que não solicita *password*	**0**	**15%**	**0**	Manter e averiguar se existem outras aplicações nesta situação

Garantir a Segurança a Nível Físico das Instalações com Informação Crítica	% de salas com informação crítica com controlo de entradas por cartão magnético (nº de salas com controlo magnético/nº total de salas)*100	**100%**	**20%**	**0%**	Instalar sistemas adequados de controlo magnético
	% de documentação altamente confidencial que é guardada em cofres de alta segurança (nº de documentos altamente confidenciais guardados em cofre/nº total de documentos altamente confidenciais)*100	**100%**	**10%**	**0%**	Providenciar este tipo de instalações ou recorrer a *outsourcing* especializado

Quadro 6 – BSC aplicado à Segurança de Informação da empresa "Motor" (Resultados)

Apesar de não se ter conseguido coletar informação que confirme a existência de um SGSI, pode-se quase decerto afirmar que a empresa tem definidas e aplica políticas de segurança de informação, uma vez que garante o cumprimento de metade das boas práticas sugeridas. Em valor alcança apenas 45% das recomendações propostas, o que reflete a ponderação atribuída a cada um dos indicadores.

No que se relaciona com o primeiro indicador, que tem como intuito incluir cláusulas de confidencialidade nos contratos, a empresa cumpre na íntegra a percentagem que se pretende alcançar, ou seja, 100%.

Relativamente ao segundo indicador, que objetiva ministrar ações de formação/sensibilização acerca da segurança de informação aos funcionários em geral, verificou-se que estes apenas têm formações de segurança no âmbito de higiene e segurança no trabalho, que elucidam como agir em caso de incêndio ou outra catástrofe natural. Assim, a par do programa de formação excelente que a entidade proporciona todos os anos a todos os funcionários acerca de requisitos da marca e outras questões relacionadas com o *cuore business*, seria crucial ministrar formação também na área de segurança de informação. Esta deverá ser atualizada conforme assim se justifique ano após ano.

Relativamente ao objetivo de aumentar a segurança de informação nos RH´s, tendo em consideração os indicadores alvo de medição, a empresa cumpre um deles apenas, tornando-se fulcral aumentar a sensibilização neste âmbito que é o que desencadeia a maior parte das falhas a nível de segurança.

No que respeita ao terceiro indicador, que perspetiva medir o desempenho a nível lógico no uso de *passwords,* pode-se afirmar que a empresa segue todas boas práticas recomendadas a este nível, já que cada um dos funcionários dispõe das *passwords* que necessita para aceder às aplicações por si usadas diariamente. Inclusivamente, as aplicações solicitam automaticamente a

alteração das *passwords* de acesso a cada dois meses e só aceitam no mínimo oito caracteres, dos quais deverão fazer parte letras e números. As sessões nos computadores são também bloqueadas automaticamente ao fim de alguns segundos de inutilização.

O quarto indicador, que perspetiva mais uma vez medir o desempenho a nível lógico desta vez relativamente ao bloqueio no acesso a aplicações, também é atingido na íntegra, já que todas as aplicações, críticas a nível estratégico ou não, solicitam *password* de acesso. Existe inclusivamente uma *password* específica só para clientes, no caso destes pretenderem consultar alguma informação no computador do *stand* que está disponível para o efeito. No que concerne à criação de perfis, estes estão muito bem definidos com autorizações adequadas.

Podemos concluir que a nível lógico, tendo em conta os critérios alvo de análise, a empresa está completamente alinhada a nível estratégico.

No que respeita ao quinto indicador, este analisa a segurança a nível físico e pretende medir a percentagem de salas que armazena informação crítica de negócio tanto em arquivo ótico como em papel, que está protegida com controlo de acessos magnético. Este é um aspeto a melhorar, já que a sala dos servidores está sempre trancada, mas a chave encontra-se à responsabilidade da administrativa do departamento da área comercial e qualquer funcionário a pode solicitar para entrar. Este procedimento pode pôr em causa não só o controlo de acesso a informação crítica como também a integridade dessa mesma informação, já que os *backups* são efetuados de uma vez por dia no final do expediente. Já as duas salas nas quais constam o arquivo de clientes, tanto de oficina que se localiza na cave, como de vendas, que se encontra no primeiro andar ao lado da sala de servidores, têm acesso livre a qualquer funcionário da empresa. Inclusivamente esta última é uma sala de utilização comum. Os arquivos estão protegidos em estantes, no entanto esta barreira considera-se insuficiente, dada a pertinência da informação nelas contida.

O derradeiro indicador pretende aferir uma boa prática a nível físico também considerada muito importante, ou seja, a percentagem de documentação altamente confidencial que é guardada em cofres de alta segurança. A empresa dispõe de um cofre onde possivelmente é guardada alguma informação sensível (não se conseguiu recolher informação conclusiva a este nível). No entanto, este cofre está situado na sala de servidores, que apresenta a barreira física à entrada anteriormente referida, pelo que não se pode considerar um cofre de alta segurança. Sabe-se que a empresa tem por política destruir alguma informação sensível em formato papel, no entanto não se considera suficiente. Seria prudente seguir as últimas práticas do mercado no sentido de proteger a informação de negócio e recorrer às *Safe Boxes*, por exemplo. Já no que respeita por exemplo ao posicionamento dos écrans e localização das salas com informação pertinente longe do acesso ao público, a empresa segue o recomendado. Cumpre referir também que a entidade está protegida por sistema de alarme e tem contrato com a uma empresa externa de segurança que faz rondas noturnas.

Podemos concluir que a nível físico, tendo em conta os critérios alvo de análise, a empresa necessita proceder a alguns ajustes para se considerar completamente alinhada a nível estratégico.

De acordo com os resultados obtidos podemos concluir que a Motor reconhece a importância da Informação enquanto recurso intangível de elevada importância, e assim sendo do seu sigilo e segurança, tendo apenas que alinhar alguns critérios.

5. Conclusões e Perspetivas de Trabalho Futuro

Neste capítulo apresenta-se uma reflexão relativamente ao estudo desenvolvido e à respetiva análise de resultados. Pretende-se também deixar em aberto perspetivas de trabalho ou temas a analisar futuramente.

5.1. Conclusões

Com este estudo de caso pôde-se concluir que a empresa "Motor" reconhece a importância da Informação enquanto recurso intangível de suma importância na prossecução dos seus objetivos estratégicos. O valor da Segurança é também reconhecido, já que grande parte dos controlos considerados pertinentes é aplicada. No entanto, possivelmente a empresa foca o dispêndio dos seus recursos noutras áreas consideradas prioritárias.

No que respeita ao uso do BSC, que se deduz que seja aplicado num grupo de tamanha dimensão já que não se conseguiu averiguar a sua utilização, é identificada a sua relevância e o respetivo uso de indicadores e métricas, uma vez que permitem avaliar o desempenho da organização não somente no que concerne à análise Financeira, contemplado também na ótica de Processos Internos, Clientes e Aprendizagem e Crescimento, o que permite obter um alinhamento estratégico bastante abrangente.

Considera-se que com esta análise mais alargada e criação de indicadores se obtém um plano que auxilia na tomada de decisão no processo de gestão da empresa e na melhoria de todo o seu desempenho. É benéfico implementar uma política de análise dos indicadores constantes para fazer ajustamentos e otimizações aos mesmos.

Conclui-se assim que a Informação representa cada vez mais um recurso estratégico a ser preservado, apesar de ser um ativo intangível. É crucial que as empresas em geral passem a direcionar alguns dos seus recursos no sentido de lhe darem a devida importância como tal. Como diz o provérbio "o segredo é a alma do negócio", pelo que é de extrema relevância desenvolver políticas de Segurança de Informação, no sentido de garantir a confidencialidade deste recurso estratégico tão importante.

Pode-se afirmar que um Programa de Segurança de Informação supervisiona a iniciativa das organizações no que respeita à proteção da Informação crítica de negócio de uma empresa. Foi útil recorrer à norma ISO 27002:2013, que é um guia que sugere o que deve ser feito com base nas melhores práticas reconhecidas internacionalmente e portanto, servindo como uma excelente base para definir as regras de um SGSI. Deverá ser usada em organizações com o intuito de preservar e garantir a segurança das suas informações, já que esta é uma norma certificada e com provas dadas de confiança.

É necessário ter muito cuidado com a aplicação de medidas de segurança nas organizações, mesmo que já sejam acreditadas, pois podem criar uma falsa sensação de segurança na informação, uma vez que estas poderão equacionar que a simples posse das políticas de "segurança" é tudo o que é necessário. Deve haver o cuidado de aplicar de forma abrangente todas as boas práticas recomendadas, principalmente as que se adequam à estratégia de negócio da empresa.

Com este Estudo de Caso conseguiu-se verificar no terreno a forma como é encarada a Segurança de Informação no tecido empresarial, tendo sido bastante prazeroso o seu desenvolvimento, apesar de todas as dificuldades com que a autora se deparou.

Apesar de a intenção da autora ao realizar um trabalho desta dimensão sempre se ter direcionado para investigar algo completamente inovador que fosse indiscutivelmente útil a outros leitores, relacionando estratégia e redes sociais, a recetividade da entidade sobre a qual inicialmente se debruçou o estudo e que acabou por se demonstrar indisponível depois, terminou por condicionar a escolha do tema. Este facto a dada altura gerou alguma desmotivação, tanto pelo desejo de investigar algo diferente, como pela dificuldade em arranjar outra entidade para investigar. No entanto, todo este trabalho de pesquisa e a temática nele envolvida acabaram por se revelar muito interessantes, principalmente na parte estratégica, já que está mais relacionada com a formação base da autora. O facto de a autora não trabalhar na entidade, nem na área do estudo de caso também acabou por complicar a sua execução, situação que ganhou maior dimensão porque decidiu elaborar a dissertação dois anos após ter concluído a parte curricular, ou seja, sem o acompanhamento dos colegas com quem mais facilmente poderia trocar ideias e com alguns dos conceitos esquecidos ou obsoletos na área de SI.

Pelo supra referido, todo este trabalho académico foi desenvolvido com sacrifício, tendo que lutar, por vezes, contra alguma desmotivação conjugada com excesso de trabalho profissional. Espera-se que toda a investigação e considerações acima tecidas sejam úteis a outros leitores nas suas decisões e na aplicação nos seus estudos de caso.

5.2. Perspetivas de Trabalho Futuro

No que concerne a perspetivas de trabalho futuro, seria interessante, solicitar autorização ao grupo em questão para desenvolver outro estudo de caso, com o intuito de ter acesso a pormenores relacionados com a Segurança de Informação. Isto permitiria alargar a pesquisa a outras áreas temática.

Conferir se a empresa faz uso da ferramenta estratégica do BSC também seria interessante, assim como ter acesso ao mapa estratégico da entidade, de forma a conseguir comparar com o novo mapa evidenciando a perspetiva da Segurança de Informação e retirar ilações mais concretas relativamente ao seu peso na Estratégia.

Proceder à cartografia dos processos, através de fluxogramas, mapas e outras ferramentas tipicamente utilizadas para o efeito, após acesso a informação mais detalhada, traria valor acrescentado no sentido de que seria mais fácil detetar aspetos comprometedores do SGSI relativamente à estratégia a seguir.

Estabelecer tabelas detalhadas de causa-efeito, de forma a confrontar os efeitos indesejáveis com os objetivos estratégicos já estabelecidos, recorrendo a indicadores e metas para o demonstrar seria muito útil.

Proceder a uma completa análise de risco, com base na norma ISO/IEC 27005 com o intuito de revelar de forma aprofundada ameaças e vulnerabilidades a que a informação de negócio está exposta e determinar o grau de risco exato permitiria trata-lo de forma adequada.

Seria igualmente bastante aliciante proceder a análises periódicas de gestão de segurança de informação e de gestão de risco, recorrendo a auditorias de entidades certificadas ou até mesmo de forma interna, para averiguar se estão a ser corretamente aplicadas as normas do SGSI e se estas estão adaptadas à estratégia da empresa.

Por fim, concretizando a vontade inicial da autora, seria muito cativante conjugar o estudo da informação enquanto recurso estratégico e a sua segurança com a forma como é partilhada tão rapidamente nas redes sociais, incidindo particularmente na rede profissional do Linkedin. A escolha desta rede social em particular deve-se ao facto de expor com bastante facilidade a rede de contatos de empresas e dos seus trabalhadores, nomeadamente no que toca a clientes, fornecedores e parceiros de negócio. Este facto concede a potenciais novos competidores informação acerca de processos e relações, que muitas vezes levaram anos a ser descobertos e mantidos, em questão de minutos. E numa conjuntura económica debilitada e cada vez mais competitiva, isto poderá conduzir ao colapso rápido de certas entidades, principalmente pequenas, pois é uma fonte excelente e inesgotável de Benchmarking concorrencial. Não deixando de considerar obviamente que a recíproca é verdadeira. No entanto, há que comparar e ponderar acerca das vantagens e condicionante da sua utilização.

Neste tipo de estudo talvez fosse interessante escolher mais do que uma entidade, principalmente das que façam uso intensivo deste tipo de meio para divulgar os seus produtos aos clientes de forma excessivamente detalhada, o que não seria difícil, já que nos dias de hoje é a ferramenta de marketing de excelência utilizada pela maior parte do tecido empresarial.

Seria interessante analisar qual o nível de volume de negócios que tem origem nessa divulgação, análise que muitas empresas fazem, porém, sem comparar com o eventual prejuízo que têm em divulgar processos e informação confidencial da empresa no que toca a valores, por exemplo. É importante evidenciar transparência ao cliente, contudo sem dar armas de arremesso aos competidores.

Referências

ANECRA (2013). Análise Sintética da Situação do Setor Automóvel em Portugal 2012-2013;

Carneiro, A. (2001). *Auditoria de Sistemas de Informação*. Lousã: FCA;

Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação*. Lisboa: FCA;

Coelho, J. et al (2005). *Sistemas de Informação Organizacionais.* Lisboa: Edições Sílabo;

Cruz, C. (2006). *Balanced Scorecard – Concentrar uma Organização no que é Essencial*. Porto: Editora Vida Económica;

Farreca, E. (2006). *Estratégia: Da Formulação à Ação Aplicando o Balanced Scorecard.* Mangualde: Edições Pedago;

Freire, A. (1995). *Estratégia – Sucesso em Portugal.* Lisboa: Editorial Verbo;

Ferreira, D. (2010). *Segurança da Informação – Importância do BSC Designer na Definição Estratégica – Estudo de Caso*. Dissertação de Mestrado. Setúbal: Escola Superior de Ciências Empresariais;

Gaivéo, J. (2008). *As Pessoas nos Sistemas de Gestão da Segurança da Informação*. Tese de Doutoramento. Lisboa: Universidade Aberta;

Gaivéo, J. (2009). *Segurança da Informação - Sebenta* (versão 1.2). Setúbal: Escola Superior de Ciências Empresariais;

Grilo, R. (2008). *Investigação em Sistemas de Informação Organizacionais – Teses e Dissertações em Portugal*. Vila Real : Universidade de Trás-os-Montes e Alto Douro;

Herrmann, D. (2002). *Security Engineering and Information Assurance*. USA: Auerbach Publications;

Gummesson, E. (1991). *Qualitative Methods in Management Research*. California: Sage Publications, Inc.;

Hill, M. e Hill, A. (2005). *Investigação por questionário*, Lisboa: Edições Sílabo;

ISO (2008). ISO/IEC 27002 – *Information Technology – Security Techniques – Code of Practise for Information Security Management, International Organization for Standardization*;

ISO (2013). ISO/IEC 27002 – *Information Technology – Security Techniques – Code of Practise for Information Security Management, International Organization for Standardization*;

ISO (2008). ISO/IEC 27005 – *Information Technology – Security Techniques – Information Security Risk Management, International Organization for Standardization*;

Trad. de J. Freitas e Silva (2000). *Strategor Política Global da Empresa.* Lisboa: Dom Quixote;

Kaplan, R. e Norton, D. (1997). *A estratégia em ação: Balanced Scorecard (8ª ed.)*. Rio de Janeiro: Editora Campus;

Kaplan, R. e Norton, D. (2004). *Mapas Estratégicos – convertendo os ativos intangíveis em resultados tangíveis*. São Paulo: Editora Campus;

Kaplan, R. e Norton, D. (2006). *Alignment: Using the Balanced Scorecard to Create Corporate Synergies.* Boston: Harvard Business School Press;

Kiyan, F. (2001). *Proposta de Desenvolvimento de Indicadores de Desempenho como* Suporte Estratégico – Dissertação de Mestrado em Engenharia de Produção. São Paulo: USP;

LeVeque, V. (2006). *Information Security: A Strategic Approach*. New Jersey: IEEE Computer Society;

Lopes, F., Morais, M. & Carvalho, M. (2005). *Desenvolvimento de Sistemas de Informação: Métodos e Técnicas.* Lisboa: FCA;

Mamede, H. (2006). *Segurança Informática nas Organizações*. Lisboa: FCA;

Martins, J. (2008). *Framework de Segurança de um Sistema de Informação.* Lisboa: Universidade do Minho e Academia Militar;

Müller-Stewens G. e Lechner C. (2005). *Strategisches Management*. Stuttgart: Schäffer-Poeschel;

Norreklit, H. (2000), *The Balance on the Balanced Scorecard – a Critical Analisys of some of its Assumptions*, Management Accounting Research, nº 11;

Oliveira, W. (2001). *Segurança da Informação – Técnicas e Soluções*. Lisboa: Centro Atlântico;

Peltier,T.R. (2005). *Information Security Risk Analysis*, (2nd edition), USA: Auerbach Publications;

Porter, M. (1999). *Competição: Estratégias Competitivas Essenciais.* Rio de Janeiro: Elsevier Editora;

Rascão, J. (2000). *Análise Estratégica – Sistemas de Informação para a Tomada de Decisão Estratégica*. Lisboa: Edições Sílabo;

Rascão, J. (2004). *Sistemas de informação para as organizações: a informação chave para a tomada de decisão*. Lisboa: Edições Sílabo;

Rascão, J. (2006). *Da Gestão Estratégica à Gestão Estratégica da Informação*. Rio de Janeiro: E-Pappers;

Rascão, J. (2008). *Novos Desafios da Gestão da Informação.* Lisboa: Edições Sílabo;

Rascão, J. (2012). *Novas Realidades na Gestão e na Gestão da Informação.* Lisboa: Edições Sílabo;

Santos, A. (2008). *Gestão Estratégica – Conceitos, Modelos e Instrumentos*. Lisboa: Escolar Editora;

Selig, G. (2008). *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*. Amersfoort: Van Haren Publishing;

Schein, E. (1992). *Organizational Culture and Leadership*. San Francisco: Jossey-Bass;

Tzu, S. (2009). *A Arte da Guerra.* Lisboa: Bertrand Editora;

Whitman e Mattford (2004). *Management of Information Security*. USA: Thomson Course Technology;

Whitman e Mattford (2005). *Principles of Information Security*. USA: Thomson Course Technology;

Wilson, D. (2002). *Managing Information: IT for Business Processes*. Oxford: Butterworth-Heinemann

Yin, R. (2009). *Case Study Research – Design and Methods* (volume 5, fourth ed). California: Sage Inc..

Referências Digitais

Strategy Train (2009). *Porquê usar uma Análise de Grupo Estratégico em vez das Cinco Forças de Porter?* Disponível em 11, Abril, 2014 em http://www.strategy-train.eu/index.php?id=104&L=5;

Social Entrepreneuship Strategy Planning (2013). *Porquê Utilizar o benchmarking?* Disponível em 11, Abril, 2014 em http://cms.sesp-project.eu/index.php?id=321&L=5;

Deco Proteste (2014). *Peugeot 308: já testámos o carro do ano.* Disponível em 30, Abril, 2014 em http://www.deco.proteste.pt/motor/automoveis/noticia/peugeot-308-ja-testamos-o-carro-do-ano

Peugeot (2014). Disponível em 11, Maio, 2014 em http://www.peugeot.pt/automoveis/

http://www.safetykleeneurope.com/index2.php?len=pt

http://www.urbanos.com/

http://www.ead.pt/ead/pt/

Site do grupo ao qual pertence a empresa, que por questões de confidencialidade não será aqui mencionado

Site da empresa, que por questões de confidencialidade não será aqui mencionado