Otimização de Práticas de Segurança da Informação – Utilização do *Balanced Scorecard Designer*

Durval Ferreira[1], Leonilde Reis[2]

1) Escola Superior de Ciências Empresariais, Setúbal, Portugal

durval.ferreira@googlemail.com

2) Escola Superior de Ciências Empresariais, Setúbal, Portugal
leonilde.reis@esce.ips.pt

Resumo

A sociedade da informação e do conhecimento, suscita às organizações a realização de uma prática de gestão estratégica contínua como forma de criar valor para os *stakeholders*, que pode ser facilitada pela utilização das Tecnologias de Informação e Comunicação (TIC) e dos Sistemas de Informação (SI). As TIC não podem ser apontadas como a resolução para todos os problemas, mas podem contribuir claramente para potenciar a melhoria do desempenho organizacional.

Na perspetiva interna da organização, a medição da *performance* consiste em criar processos que ajudem à tomada de decisão com base em factos. Com base na missão, e na descrição dos seus principais processos, na estratégia definida para a organização, e na norma ISO/IEC 27002:2005, foi iniciado um estudo para identificar problemas no domínio da segurança da informação na Mesio Serviços, Lda.

Baseado na norma ISO/IEC 27004:2009 foi possível definir um conjunto de métricas que se consideraram relevantes para o estudo. Com recurso à metodologia de avaliação do desempenho *Balanced Scorecard,* foi criada a perspetiva de trabalho para a Segurança da Informação, e consequentemente os processos e os indicadores a aplicar e monitorizar, bem como as metas pretendidas com o trabalho de avaliação.

A transposição do plano para a ferramenta de avaliação e medição da *performance Balanced Scorecard Designer* (*BSC Designer*), permitiu a avaliação em tempo real dos indicadores e das metas estipuladas para a otimização das políticas de segurança na organização, tornando-se preponderante no acompanhamento e evolução do desempenho dos controlos pela monitorização, facto que possibilita a correção dos desvios em relação ao previsto de forma a atingir as metas e os objetivos definidos.

Palavras-chave: Sistemas de Informação, *Balanced Scorecard*, Tecnologias de Informação e Comunicação, Segurança da Informação.

1. Introdução

A organização em rede deve ser capaz de preservar o objeto que lhe dá suporte e que pode contribuir de forma decisiva para o conhecimento do ambiente que a rodeia – a informação. Segundo [Mamede 2006], trata-se de um ambiente com imensas fragilidades onde qualquer organização pode ser muito facilmente atingida por variadíssimos tipos de ataques. Em consequência, os gestores demonstram um interesse crescente em obter certificações em

segurança de forma a recolher uma maior visibilidade e reconhecimento por parte dos *stakeholders*, obrigando a uma avaliação contínua das suas organizações e aumentando o seu grau de responsabilidade para com o mercado.

A segurança da informação nem sempre é considerado um processo prioritário por parte das organizações, o que as leva muitas vezes a descurar pequenos aspetos de importância vital, por vezes com um impacto incalculável no negócio, em caso de acidente ou de utilização indevida. Para [Reis 2001], é preciso dar relevo ao facto de inúmeras organizações estarem a correr riscos mal avaliados, ao não se aperceberem do valor económico da informação crítica para o negócio.

As redes globais são verdadeiros ecossistemas onde aqueles que as integram, conscientes da sua interdependência, se vêm obrigados a investir na qualidade das suas relações. "No mundo da globalização, que nos traz em simultâneo, concentração e fragmentação, assistimos a uma mudança socioeconómica e cultural muito profunda, materializada na nova sociedade da informação, cujo núcleo fundamental é uma economia baseada no conhecimento e suportada por meios digitais e por processos contínuos de inovação, produtividade e concorrência" [Leandro et al. 2000].

A avaliação das ferramentas e dos recursos existentes, os resultados obtidos, a identificação de inconformidades, permitem avaliar sobre as vulnerabilidades que a organização se encontra exposta no desenvolvimento das suas atividades, e das suas atribuições. Segundo a norma ISO/IEC 27002:2005, vulnerabilidade é a fragilidade a que está sujeito qualquer ativo ou conjunto de ativos da organização, perante uma ou várias ameaças.

O conjunto dos processos para quantificar os resultados e a sua eficiência em relação a ações decorridas, designa-se por medição da *performance*. A medição da *performance* ou do desempenho, permite tomar decisões com base em factos, portanto mais fundamentadas, ao mesmo tempo que permite executar ações de correção. O processo quantifica a eficácia e a eficiência de ações passadas na organização através da recolha, da confirmação, da categorização, ou da análise e interpretação adequada dos dados ou informações produzidas.

Nesta vertente, o artigo, apresenta um caso estudo que foi realizado na área da segurança da informação, na Mesio Serviços, Lda. Foi utilizada a metodologia de gestão estratégica e avaliação do desempenho organizacional *Balanced Scorecard*, com recurso à ferramenta de *software* para medição e monitorização da performance *Balanced Scorecard Designer*, com base nos pressupostos já referenciados. Trata-se portanto de um caso real, mas em que o nome da organização por questões de confidencialidade é fictício.

2. Problema Organizacional na Mesio Serviços, Lda.

A Mesio Serviços, Lda. é uma estrutura direta de apoio a um importante órgão de administração do estado envolvido na implementação das políticas e estratégias definidas pelo governo, para um setor importante da administração pública portuguesa. Em consequência, na primeira linha no apoio a essas políticas, a Mesio Serviços, Lda. deve estar atenta à sua envolvente, nomeadamente a novas plataformas de integração e suporte que vão de encontro às necessidades e expectativas dos seus clientes, atuais ou a incorporar, à necessidade constante de agregação de novos organismos, ou outros que recorrem com alguma frequência ao apoio da Mesio Serviços, Lda. para o cumprimento das suas próprias atribuições.

2.1. Metodologia

As vulnerabilidades existentes em segurança na organização dão origem à determinação dos controlos da norma ISO/IEC 27002:2005, e às métricas a monitorizar que permitam efetuar as correções necessárias à consolidação da estratégia da Mesio Serviços, Lda.

2.2. Estudo da Organização

A obrigatoriedade de dispor de profissionais responsáveis, com fortes e alargadas competências e capacidades, motivados, conhecedores da estratégia da organização, com formação adequada às necessidades e ao contexto organizacional, são premissas para as organizações atuais, onde naturalmente se inclui a Mesio Serviços, Lda.

O conhecimento alcançado com a informação recolhida da missão, da estratégia, dos sistemas de informação, conjugado com as atribuições da organização, e consequentes tarefas a que fica vinculada no âmbito das suas atribuições, permitiu obter um conjunto de preocupações que podem representar sérias vulnerabilidades para a organização. Salientam-se os aspetos:

- Capacidade de Armazenamento, e ciclo de vida dos equipamentos;
- *Backups* de informação;
- Organização e documentação dos Sistemas;
- Formação dos utilizadores em Segurança da Informação.

O sucesso do desempenho na realização dessas tarefas contribui de forma decisiva para consolidar a estratégia definida pela organização. O comprometimento do fornecimento dos produtos/serviços de que está incumbida no âmbito das suas atribuições aos seus clientes, é o aspeto central para a Mesio Serviços, Lda.

As vulnerabilidades dão origem à determinação dos controlos da norma ISO/IEC 27002:2005, e consequentemente às métricas a monitorizar de acordo com as especificações da norma ISO/IEC 27004:2009, e efetuar as correções necessárias à consolidação da estratégia em segurança da informação da Mesio Serviços. Com base no referencial de segurança, na Missão, e nos objetivos estratégicos definidos para a organização, o trabalho realizado identifica com clareza os aspetos condicionadores ou comprometedores do processo global de segurança da informação, considerado estratégico para o negócio da Mesio Serviços, Lda,.

Para a monitorização de todo o processo, é importante a implementação e utilização de uma ferramenta que permita gerir e otimizar os procedimentos de controlo. A medição e avaliação permanente de todos os processos de segurança da informação identificados, pretende ajudar na criação de informação para a gestão, e de um canal de divulgação dos problemas da segurança na organização que sensibilize os vários intervenientes.

2.3. Avaliação de Ferramentas

Um fator de competitividade por excelência pode ser obtido graças à utilização de ferramentas de gestão integrada, como as de *Balance Scorecard* pela capacidade de análise diversificada que proporcionam. Estas ferramentas potenciam a observação dos gestores, através da execução de relatórios que agrupam informação em simultâneo acerca dos objetivos e dos resultados.

Para a medição da *performance* da segurança da informação foram avaliadas um conjunto de ferramentas de *software*. Após um trabalho intensivo de avaliação às suas potencialidades, o *BSC Designer* foi a ferramenta que mais se enquadrou nas necessidades da Mesio Serviços. A não limitação do número de relatórios, a possibilidade da sua alteração de acordo com as necessidades da gestão ou dos utilizadores, o licenciamento por utilizador, ou ainda a forma de publicação de relatórios, entre outros, tornaram-se fatores chave na decisão pelo *software* da AKS Labs. Foi utilizada no estudo uma versão experimental deste produto.

O *BSC Designer* foi criado para simplificar o processo de gestão dos *Key Performance Indicators* (KPI's). Permite estabelecer um conjunto de indicadores de desempenho, definir as relações, metas, e assinalar a importância dos indicadores. Fornece flexibilidade para calcular o desempenho com base em valores baseados nos indicadores associados, permitindo a exportação dos dados para outras ferramentas para posterior tratamento. Pode ser definido o peso relativo a

cada perspetiva, possibilitando o seu balanceamento, regulando a sua importância no mapa de BSC.

São ainda fatores positivos da ferramenta a interface de fácil utilização, com possibilidade para a criação de várias categorias, indicadores, equilibrar funções, especificar valores, ligar a outros *scorecards*, importação de dados, fácil exportação das informações, etc.

2.4. Medição da Performance

A definição dos controlos e dos objetivos dos controlos segundo a norma ISO/IEC 27002:2005 resulta do trabalho realizado com a recolha, tratamento e subsequente análise dos dados e informações, dos requisitos do negócio, obrigações contratuais da organização para com a segurança da informação, entre muitos outros aspetos.

Obedece a um trabalho de análise sustentado num conjunto de preocupações manifestadas por diversos funcionários com diferentes níveis de responsabilidades na Mesio Serviços, direta ou indiretamente ao nível dos SI, de uma análise exaustiva realizada ao nível interno à Missão organizacional, aos objetivos definidos para a organização ou ainda através do conhecimento do teatro de operações. Já no plano externo, o contributo foi dado pelo estudo dos referenciais relacionados com segurança da informação, nomeadamente a norma ISO/IEC 27002:2005, referencial de excelência em matéria de segurança da informação, pela legislação em vigor, e pela bibliografia relacionada com os temas da estratégia e da segurança da informação.

2.5. Definição de Métricas

Pela importância no suporte à Missão organizacional, a escolha dos controlos foi cuidadosamente realizada e sustentada com base em informações internas, que deram origem à escolha de quatro medidas de avaliação do desempenho da segurança da informação organizacional.

De uma forma que se pretende elucidativa são descritas as medidas e as razões que levaram à sua escolha, bem como o fim a que se destinam, por se considerar da maior importância para a Mesio Serviços, Lda. face ao crescente número e diversidade de tarefas que lhe são confiadas no âmbito das suas atribuições.

Objetivos		Indicadores		Indicador Final ou Medida Derivada	Metas
% 25	1.Formação em Segurança da Informação	Peso 100%	Índice de formações realizadas em SdI (Ações de formação realizadas em segurança da informação/Total de ações de formação realizadas) *100.	Índice de formações realizadas em SdI (Ações de formação realizadas em segurança da informação/Total de ações de formação realizadas) * 100.	20% de utilizadores com formação em segurança da informação nos próximos dois anos.
% 25	2.Procedimentos de Operações Documentados	Peso 100%	Índice de procedimentos documentados (Número de procedimentos documentados/Total de procedimentos identificados) *100	Índice de procedimentos documentados (Número de procedimentos documentados/Total de procedimentos identificados) *100	100% dos procedimentos nos próximos dois anos.
% 25	3.Gestão da Capacidade	P2)Peso %	(R2) Índice de Utilização de Espaço em Disco (Espaço Utilizado/Espaço Total)	Índice de Desempenho do Equipamento de partilha de informação: $RT = (R1 * P1) + (R2 * P2) * 100$	Manter o valor do Índice abaixo dos 80%
		P1)Peso %	(R1) Índice de Utilização de Memória do Equipamento (Memória Utilizada/Memória Total)		

% 25	de 4.*Backup* Informação	**Peso 100%**	Índice de Cópias de Segurança com Insucesso (Processos de *Backup* realizados com problemas / Total de Processos de Backup realizados) * 100	Índice de Eventos de Cópias de Segurança com Insucesso (Processos de *Backup* realizados com problemas / Total de Processos de Backup realizados) * 100	Manter o Índice de anomalias abaixo de 1% ao ano

Tabela 1 – Objetivos e indicadores objeto de análise do desempenho

A tabela 1 mostra de forma muito resumida os objetivos propostos para a perspetiva da segurança da informação, o seu contributo individual para o *Balanced Scorecard*, os indicadores correspondentes e o seu peso no objetivo. A descrição das medidas foi realizada com base nos controlos da norma ISO/IEC 27002:2005 e na metodologia fornecida pela norma ISO/IEC 27004:2009, atendendo à pertinência e relevância no contexto organizacional.

A cada objetivo corresponde um indicador final ou uma medida derivada consoante o número de indicadores de base utilizados, segundo a norma ISO/IEC 27004:2009. Por último, surgem as metas que são pretendidas pela definição dos objetivos.

Métrica 1 – Formação de Recursos Humanos em Segurança da Informação

A Mesio Serviços, Lda. manifesta claramente uma preocupação acrescida com a formação dos seus recursos humanos. No entanto, a formação em segurança da informação não se encontra contemplada de forma expressa nessas preocupações.

A escolha desta métrica, com base no controlo 8.2.2 da norma ISO/IEC 27002:2005 deve-se à importância para a organização de proporcionar aos seus colaboradores formação em segurança da informação, no sentido de lhes proporcionar consciencialização e competências sobre as políticas e procedimentos mais importantes ao desenvolvimento das suas responsabilidades e funções no sistema de informação da organização, na tentativa de proteger dos recursos informacionais.

A formação em segurança faculta aos utilizadores um conhecimento mais profundo das suas responsabilidades para com o sistema de informação organizacional, contribuindo para a melhoria da utilização dos recursos de processamento de informação.

A Mesio Serviços estabeleceu como meta que 20% dos seus utilizadores possuam formação em segurança da informação nos próximos dois anos.

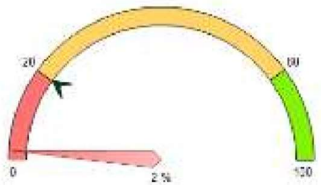

Figura 1 - Formação de Recurso Humanos em SdI

Pela figura 1 retirada da aplicação *BSC Designer*, é possível verificar a percentagem de 2% para os Recursos Humanos que têm até ao momento formação em segurança da informação, identificado pela localização do ponteiro no gráfico, de acordo com os dados recolhidos.

À medida que novos utilizadores forem sendo identificados pelas competências em segurança da informação adquiridas, e de acordo com o estabelecido na definição da medida, o carregamento dessa informação na aplicação vai introduzir alterações ao nível do gráfico, que tornará de forma fácil a visualização do valor final conseguido, e a distância à meta definida. Até que seja atingido

este valor, a zona onde se encontra o ponteiro será da cor vermelha indicando valores inferiores em relação aos pretendidos.

Métrica 2 – Documentação de Procedimentos e de Operações dos Sistemas

A opção por esta métrica, assente no controlo, 10.1.1 da norma ISO/IEC 27002:2005, baseou-se na necessidade em obter documentação sobre procedimentos de segurança implementados na organização, de forma a disponibilizá-los sempre que tal seja necessário, por qualquer utilizador habilitado. A análise realizada revela claramente a inexistência de documentados sobre procedimentos de segurança para os recursos de processamento de informação.

Pela constante alteração ao nível dos recursos (humanos, tecnológicos, etc.) aos vários níveis da organização, torna-se indispensável a existência atualizada de documentação de suporte sobre os meios de processamento de informação e de comunicação.

A falta de informação de suporte sobre os procedimentos de segurança pode levar a que em caso de incidente possa estar comprometida a recolocação do normal funcionamento dos recursos de processamento de informação, processos ou procedimentos que podem ser críticos para a organização.

A meta definida pretende garantir que todos (100%) os procedimentos de segurança da Mesio Serviços sejam identificados e devidamente documentados, de forma a reabilitar serviços, processos, ou procedimentos em caso de necessidade, de forma rápida e eficaz, por qualquer utilizador habilitado na organização.

Figura 2 - Documentação dos Procedimentos

De um total de onze procedimentos de segurança identificados, verificou-se a existência de apenas três com documentação existente, o que aponta para uma percentagem aproximada de 30% dos procedimentos que se encontram documentados em relação ao total.

Métrica 3 – Gestão de Capacidades

Esta métrica tem por base um conjunto de preocupações sobre o desempenho de alguns serviços partilhados aos utilizadores da Mesio Serviços, Lda., em grande parte manifestada pelas pessoas que foram entrevistadas. A monitorização realizada de forma permanente ao equipamento, nomeadamente ao nível do seu desempenho e capacidade de receber informação torna-se um aspeto relevante para a garantia da prestação de serviços aos seus clientes por parte da organização.

Figura 3 - Redução de falhas nos sistemas

Considerou-se por isso ser importante a avaliação constante do equipamento mais crítico, por se pensar que pode ter impacto no desempenho da organização, o facto de existirem anomalias com a máquina que partilha a informação aos utilizadores da Mesio Serviços. A medida derivada, assenta no controlo 10.3.1 da norma ISO/IEC 27002:2005 e pretende avaliar em conjunto a capacidade de armazenamento e de desempenho da memória do equipamento.

Na figura 3 podemos verificar a *performance* conjunta do equipamento que se situa nos 20% pelas avaliações feitas de acordo com os parâmetros especificados para a medida.

A figura indica ainda o limite sobre o qual não deverá ser ultrapassado o desempenho conjunto. O desempenho conjunto e continuado de valor superior a 54%, indica que existe um dos parâmetros no limite das suas capacidades, pelo que é necessário proceder a uma avaliação profunda no sentido de por um lado identificar os problemas que estão na origem dos valores apresentados, por outro lado avaliar sobre investimentos futuros no equipamento.

Métrica 4 – Backups de Informação

Esta métrica assume grande importância no contexto funcional da Mesio Serviços, Lda. porque vai permitir avaliar a reposição com segurança das informações guardadas nos sistemas em caso de acidente. Assenta por isso no controlo 10.5.1 da norma ISO/IEC 27002:2005,

Ao existir monitorização das rotinas diárias de *backup* de informações, é possível avaliar as razões que levam ao aparecimento dos problemas, e de imediato proceder à correção dos desvios. A monitorização proporcionada pelo controlo ao *software BackupExec* serve para garantir que todo o processo (equipamentos, tapes, discos, software) implementado, corresponde às reais necessidades da organização, cumpre com os objetivos que lhe estão circunscritos, e concluir sobre investimentos ou eventuais alterações a realizar no processo.

A meta definida determina que a organização deve manter a relação existente entre os eventos de *backup* com problemas e o seu total, com valores abaixo de 1%. Caso estes valores atinjam valores superiores, deverá ser percecionado o seu tipo, e qual a origem do problema de modo a evitar a repetição.

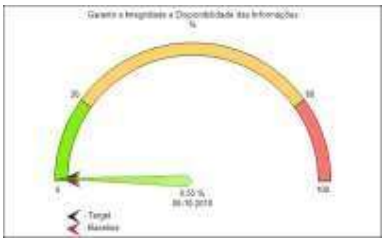

Figura 4 – *Backups de* Informação

A figura 4 apresenta o valor (0,55%) em que se encontra a relação, portanto abaixo de 1%. Não existem por isso razões para preocupações em relação à realização dos *backups*, podendo de alguma forma os responsáveis da Mesio Serviços descansar em relação à manutenção da integridade das informações guardadas ou a guardar nos suportes e unidades de *backup* da Mesio Serviços, Lda.

3. *Performance* da Segurança da Informação

Foi adotado um critério de igualdade entre perspetivas, contribuindo cada uma com 20% para a estratégia global, apesar de reconhecida e relevante a importância do peso individual que cada perspetiva em função das características e especificidades da organização. A aplicação *BSC Designer* fornece um vasto conjunto de imagens para melhor interpretar as ações realizadas.

A figura 5 proporciona a vista da perspetiva da segurança da informação de forma particular, em relação à estratégia, e o seu contributo atual de 10,67% para o mapa estratégico no geral. O peso atribuído foi de 2 (20%) para o mapa estratégico. Este valor apresenta-se particularmente baixo pela fraca expressão demonstrada neste momento pelos objetivos que a compõem, e do seu reduzido contributo no momento. O processo de medição da *performance* estende-se no tempo, pela observação permanente e cuidada dos factos.

As restantes perspetivas, apesar de figurarem no mapa da estratégia, encontram-se com valores nulos, porque não foram avaliadas na sua *performance* por se encontrarem fora do âmbito do estudo. A medição da *performance* para as restantes perspetivas, obrigaria a uma redefinição do âmbito, pela dimensão do projeto a realizar, e pelo empo necessário para a sua execução.

Figura 5 - Perspetiva Geral da Segurança da Informação

A figura 6 descreve a perspetiva da segurança da informação de uma forma mais agregada, evitando a dispersão. Apresenta ainda o valor da *performance* e do contributo de cada indicador, indica a *baseline* de cada um, as metas pretendidas, e em que unidades de medida se representam. Depois do início da medição do desempenho organizacional da segurança da informação, e após a introdução dos valores na aplicação, as medidas que compõem a perspetiva apresentam estabilidade (seta azul na horizontal) na coluna "*value*" para a *performance*.

Na figura 7, com visualização diferenciada da anterior, é apresentado o contributo para o *Balanced Scorecard* da *performance* da perspetiva da segurança da informação, com um valor de realização de 53,36%, portanto ainda abaixo das metas definidas.

Figura 6 – Perspetiva Geral Segurança da Informação

Encontrando-se assim o valor abaixo da base, conclui-se que os contributos para a perspetiva no conjunto não são suficientes para manter um nível aceitável em relação ao previsto.

4. Evolução da Performance da Segurança da Informação

À medida que vão sendo introduzidos os novos valores na aplicação, assistimos à evolução da perspetiva pelos quadros fornecidos pelo *BSC Designer*.

Figura 7 –Perspetiva Geral da Segurança da Informação quatro dias depois

Na figura 8, a perspetiva no seu conjunto baixou o seu valor contributivo para o *Balanced Scorecard* com 49,07%, provocando uma diminuição da *performance* do BSC no seu conjunto de 5,22% (de 10,67% em 06/10, para 5,45% em 10/10).

A formação de recursos humanos em segurança da informação manteve os valores iniciais, ao contrário do que foi verificado nas restantes medidas. Foram identificados dois novos procedimentos, mas não foram acompanhados da respetiva documentação, o que fez baixar os valores percentuais da relação para 25%. A seta do campo "*value*" indica assim um decréscimo no valor, encontrando-se a sua cor alaranjada, facto com impacto negativo na perspetiva.

Com valores superiores aparece a medida que pretende garantir a integridade e disponibilidade das informações, embora abaixo do 1% definido para a meta. Apresenta 0,7% de eventos problemáticos. Embora tenha ainda alguma margem de progressão, o seu desempenho foi inferior em relação à anterior medição (0,55%). Ainda assim, ainda não são necessários cuidados especiais apesar do contributo negativo.

O indicador conjunto para medir a Redução de Falhas nos Sistemas apresenta um desempenho também ele negativo. Na origem está a maior utilização do espaço em disco, em resultado da incrementação de novos volumes de informações por parte dos utilizadores da Mesio Serviços, devido à necessidade ocorrida de digitalização para a rede de vários documentos.

Em suma, a figura proporciona uma visualização integrada da perspetiva da segurança da informação, e uma avaliação rápida sobre a sua evolução, bem como dos elementos que a compõem, e percecionar onde se encontram os desvios, facto que possibilita de uma forma célere

agir na sua correção. Da mesma forma possibilita monitorizar a evolução e estimar sobre o seu contributo para a estratégia, podendo os valores ser transportados para o mapa estratégico.

5. Conclusão

A definição de uma política de segurança conduz ao respeito dos tópicos abordados por parte de funcionários, parceiros ou prestadores de serviços na organização, trazendo-os para o centro do problema, melhorando os seus comportamentos, embora por vezes tal imposição de medidas possa criar incompreensão por parte dos intervenientes.

A norma 27002:2005 estabelece as linhas de orientação para iniciar, implementar, manter e melhorar a gestão da segurança da informação nas organizações. Os seus objetivos, provenientes das grandes linhas de orientação gerais, deveriam ser amplamente aceites para gerir a segurança, e permitir desenvolver os procedimentos de segurança da informação bem como as eficientes práticas de gestão, e contribuir para a confiança das atividades entre organizações. A política de segurança deverá contribuir para a estratégia organizacional através da definição de objetivos, que auxiliem a Mesio Serviços, Lda. a manter-se como uma organização de referência junto da tutela e dos seus clientes.

O *BSC Designer* como *software* utilizado para medir o desempenho da perspetiva da segurança da informação, utilizando os resultados observados no tempo, revelou-se de estrema importância na monitorização das métricas, possibilitando a sua correção, a consequente disseminação dos resultados obtidos por toda a organização.

Apesar da complexidade, considera-se ser da maior importância a adoção do modelo de forma alargada na Mesio Serviços, Lda., pela sua flexibilidade e facilidade de interação com outras técnicas e métodos que contribuem para consolidar a estratégia organizacional. A avaliação das métricas estabelecidas de acordo com a Missão e com os objetivos estratégicos reforçam assim o papel cada vez mais importante da segurança da informação na Organização, como a forma mais acertada de proteger o ativo informação.

6. Referências

Calder, A., Watkins S., "*IT Governance – A Manager's Guide to Data Security and ISO 27001/ISO 27002*", Kogan Page Limited, 4th Edition, London-Philadelphia, 2008, ISBN: 9780749452711.

ISO (2005), ISO/IEC 27001 – "*Information Technology – Security Techniques – Information Security Management Systems – Requirements*", International Organization for Standardization.

ISO (2005), ISO/IEC 27002 – "*Information Technology – Security Techniques – Code of Practice for Information Security Management*", International Organization for Standardization.

ISO (2009), ISO/IEC 27004 – "*Information Technology – Security Techniques - Information Security Management - Measurement*", International Organization for Standardization.

Kaplan, R., Norton, D., "*Strategy Maps. Converting Intangible Assets into Tangible Outcomes*", Boston: Harvard Business School Publishing Corporation, 2004.

Leandro, G., Carrapatoso, A., Azevedo, B., Rodrigues, C., Ficuciello, A., Almeida, B., Couto, S., Rodrigues, L, Magalhães, J., "A Gestão da Informação e a Tomada de Decisão", Edições Atena, Lda., São Pedro do Estoril, 2000, ISBN: 9728435401.

Mamede, H., (2006), "Segurança Informática nas Organizações", FCA - Editora Informática, Lisboa, ISBN: 9789727224418

Pinto, F., "*Balanced Scorecard*", Edições Sílabo, Lda., Lisboa, 2007, ISBN: 9789726184591.

Reis, L., "Planeamento de Sistemas de Informação e da Contingência e Recuperação", Tese de Doutoramento, Universidade do Minho, Braga, 2001.

Silva, P., Carvalho H., Torres, C., "Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial", Centro Atlântico, Lda., 1ª edição, Lisboa, 2003, ISBN: 9728426666.