UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE EDUCAÇÃO CONTINUADA
MBA EM GESTÃO DE NEGÓCIOS E TECNOLOGIA DA INFORMAÇÃO

THIAGO CASTRO DE OLIVEIRA

DEMONSTRANDO A ENTREGA DE VALOR DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

Um estudo de caso sobre alinhamento estratégico

São Leopoldo
2016

Thiago Castro de Oliveira

DEMONSTRANDO A ENTREGA DE VALOR DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

Um estudo de caso sobre alinhamento estratégico

Artigo apresentado como requisito parcial para obtenção do título de MBA em Gestão de Negócios e Tecnologia da Informação da Universidade do Vale do Rio dos Sinos - UNISINOS

Orientador: Prof. Ms. Leonardo Lemes Fagundes

São Leopoldo

2016

DEMONSTRANDO A ENTREGA DE VALOR DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

Um estudo de caso sobre alinhamento estratégico

Thiago Castro de Oliveira*

Leonardo Lemes Fagundes**

Resumo: Segurança da informação, embora de importância indiscutível demonstrada pelos casos críticos de prejuízos às organizações devido a sua quebra ou negligência, precisa estar alinhada aos objetivos estratégicos para que possa ser justificável os investimentos às suas necessidades de maneira consistente. O presente artigo tem como objetivo propor um meio para demonstrar o relacionamento entre os processos e objetivos de um Sistema de Gestão de Segurança da Informação (SGSI) e os objetivos estratégicos de uma organização. Realizou-se tal alinhamento, portanto, através de coleta informações da organização, busca das melhores práticas de mercado e conscientização da importância desse projeto dentre todos os envolvidos, sobretudo a alta direção da companhia. O resultado foi a criação de um *balanced scorecard* (BSC) para o sistema de gestão de segurança da informação, englobando indicadores e medidas de desempenho para acompanhamento de seus resultados e entrega de valor em relação aos objetivos da organização. Com a execução desse projeto, concluiu-se que a criação de um BSC para o SGSI provê de forma clara e coerente os relacionamentos entre os processos de segurança da informação e os objetivos de negócio da companhia. Além disso, mostrou que o engajamento de todas as áreas envolvidas é essencial para a manutenção e o atingimento dos objetivos estabelecidos.

Palavras-chave: Segurança da informação. Balanced Scorecard. Métricas. Desempenho.

1 INTRODUÇÃO

Segurança da Informação e privacidade ganharam espaço rotineiro na grande mídia. Grandes casos recentes de roubo de dados, vazamento de informações sensíveis e monitoramento de dados pessoais alertaram o grande público para a necessidade de cuidados e atenção necessária quando se lida com sistemas computacionais (KREBS, 2009; LUDLOW 2010; GELLMAN e POITRAS 2013). Contudo, mesmo havendo consenso dessa necessidade, investimento em

* Graduado em Segurança da Informação pela Universidade do Vale do Rio dos Sinos – UNISINOS em 2014, profissional com 7 anos de experiência na área. E-mail: thcastro@outlook.com.

** Mestre em Computação Aplicada (2006) e Bacharel em Informática - Habilitação em Análise de Sistemas (2002) pela Universidade do Vale do Rio dos Sinos – UNISINOS. Consultor em Segurança da Informação com as seguintes certificações: *Lead Auditor* ISO 27001 (BSI) e *Business Continuity Professional* (DRI). E-mail: llemes@unisinos.br.

segurança da informação nas grandes organizações segue sendo algo difícil de se justificar. (KPMG, 2000). A grande barreira é o fraco alinhamento dos entregáveis de segurança da informação com os objetivos estratégicos da organização, embora tenhamos demanda e imposição de mercado para alinhamento de processos internos das organizações com regulamentações, normas e boas práticas. Um exemplo dessa situação é a necessidade de organizações multinacionais estarem em conformidade com o Sarbanes-Oxley Act (SOX), o qual causa grande impacto em relatórios financeiros, auditorias, controles internos e governança corporativa (ALVES et al., 2006). Outro exemplo é a conformidade com a norma ISO/IEC 27001, vista como diferencial de mercado nos principais polos mundiais de tecnologia, mas ainda pouco disseminada em nosso país (BRENNER, 2007).

A norma ISO/IEC 27001 define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI) e possui como principal item para o planejamento de suas ações o processo de gestão de riscos e oportunidades, a fim de alcançar os objetivos definidos. (ISO/IEC, 2013). Embora seja estruturada para que se defina quando aceitar, mitigar, transferir ou evitar um risco, há uma análise subjetiva do impacto ao negócio, sendo uma tarefa difícil quantificar perdas financeiras exatas (KAPUR, 2010 e ISO/IEC, 2008). Contudo, a relação entre prejuízos ou perdas financeiras nos negócios e quebras de segurança, traz o foco para o alinhamento da gestão de riscos com os objetivos de negócio das organizações (KAPUR, 2010). O processo de gestão de riscos deve estar alinhado com as mudanças na organização e seus objetivos, para que tecnologias e processos possam estar de acordo e implementados de forma otimizada. Segurança é um processo, e como tal, não pode se basear apenas no círculo de detecção de “problemas-correção-atualização-oração” para que tudo ocorra bem (JAQUITH, 2007).

O alinhamento entre objetivos organizacionais ao longo de todos os departamentos e áreas da organização garante que cada um saiba executar seu papel de forma otimizada para com os objetivos globais. Desta forma, objetivos das áreas estarão apoiando de forma direta ou indireta os objetivos da companhia, bem como objetivos individuais, relacionados as atividades de cada colaborador. Segundo Herzog (2003), as empresas vêm criando o alinhamento entre as estratégias organizacionais por meio da elaboração do *Balanced Scorecard*, proposto por Kaplan e Norton (1997), e seu detalhamento nas áreas e processos de negócios. De acordo com Jaquith (2007), esse tipo de abordagem requer que a

organização adote processos de medição. Geralmente incluindo passos para definição e validação de métricas, coleta de dados e criação de relatórios. Ainda de acordo com os autores, um scorecard para segurança da informação necessita, a fim de se tornar legível ao nível executivo, ser completo, conciso, claro, relevante e transparente. Segue aberta, portanto, uma lacuna para pesquisa: Como alinhar os objetivos de um sistema de gestão de segurança da informação aos objetivos de negócio, mostrando de forma mais clara o valor entregue ao negócio da organização?

O presente trabalho busca de forma prática demonstrar a entrega de valor ao negócio dos processos do SGSI da empresa ADQ por meio do alinhamento aos objetivos estratégicos, utilizando a estrutura de um *balanced scorecard*.

Para alcançar desse objetivo, serão utilizadas as melhores práticas de mercado a respeito de governança e gestão estratégica alinhadas a segurança da informação. Como base de conhecimento da organização, serão coletadas informações sobre diretivas, políticas e procedimentos internos, bem como objetivos e mapa estratégico. Além de entrevistas com responsáveis e operadores do sistema de gestão. Entretanto, devido à natureza sigilosa das informações e as políticas de segurança em vigência, a organização se guardou o direito de não divulgar e/ou mascarar dados sensíveis.

Como benefícios do projeto, pode-se citar a elaboração de um painel com visão gerencial clara das metas e situação atual dos processos do SGSI da companhia, organizados a partir das perspectivas do BSC e relacionados com os objetivos estratégicos da organização. Desta forma, para cada item que não apresentar desempenho conforme esperado pelas métricas definidas pelos níveis executivos, ações poderão ser tomadas seguindo as perspectivas relacionadas. Assim, espera-se que esse alinhamento seja construtivo para os processos de segurança da informação, servindo como base para justificativa e tomada de decisão em investimentos, bem como, incorporando as demais áreas da companhia envolvidas nos processos do sistema de gestão de segurança da informação.

Ainda que seja vista como necessária a visão estratégica de segurança da informação para justificativa de investimentos e demonstração de importância junto ao nível executivo, poucos foram os projetos identificados com esse intuito. Dentre os projetos relacionados que serviram como base para o desenvolvimento deste, destaca-se Kapur (2010) e Herath et al. (2010) pelo relacionamento com as

perspectivas do BSC tradicional e o detalhamento da metodologia utilizada. Infelizmente, casos de implementações reais e resultados obtidos não foram identificados.

O restante desse trabalho está organizado da seguinte forma: No capítulo 2, o referencial teórico necessário para o entendimento dos assuntos relacionados é apresentado. No capítulo 3 será apresentada a revisão sistemática da literatura e seus critérios para busca, coleta e escolha dos trabalhos relacionados que serviram como norteadores e apoio para o desenvolvimento do presente projeto. A metodologia utilizada para o desenvolvimento do projeto é apresentada no capítulo 4. As etapas práticas da criação do BSC proposto são expostas no capítulo 5, bem como os entregáveis do projeto. Por fim, as conclusões são descritas no capítulo 6.

2 REFERENCIAL TEÓRICO

Neste capítulo serão aprofundados os assuntos relacionados ao objetivo do trabalho desenvolvido. As próximas sessões abordarão melhores práticas em gestão estratégica, segurança da informação e governança de segurança da informação (SI) e Tecnologia da informação (TI). Além disso, será descrita uma visão geral do mercado de cartões, ambiente no qual a empresa desse estudo atua.

2.1 Balanced Scorecard

De acordo com os autores Kaplan e Norton (1997), a utilização do *Balanced Scorecard* (BSC) como sistema de gestão estratégica pelas organizações tem como objetivo esclarecer e chegar ao senso comum em relação a estratégia em âmbito organizacional, focalizando iniciativas, desenvolvendo as capacidades e buscando sinergia entre as unidades de negócio. Segundo Kronmeyer (2006), o BSC busca orientar a gestão estratégica nos seguintes pontos:

- Esclarecer e obter consenso em relação à estratégia;
- Comunicar a estratégia por toda a empresa;
- Alinhar as metas departamentais e pessoais à estratégia;
- Associar os objetivos estratégicos com metas e orçamentos de longo prazo;

- Identificar e alinhar as iniciativas, programas de investimento e ação estratégicas;
- Realizar revisões periódicas e sistemáticas;
- Obter feedback para aprofundar o conhecimento da estratégia, aperfeiçoá-la, e desenvolver o aprendizado estratégico.

Esse método expõe indicadores de desempenho em quatro perspectivas: financeira, clientes, processos internos e aprendizado e crescimento (KAPLAN e NORTON, 1997). Cada perspectiva tem um conjunto específico de métricas, sendo essas desenvolvidas de acordo com as especificidades da organização. Essas métricas precisam refletir a missão e estratégia da organização (KAPLAN e NORTON, 1997).

Perspectiva financeira: Segundo Kaplan e Norton (1997) essa perspectiva define os objetivos a longo prazo para unidades de negócio, tipicamente estratégicas para obtenção de lucro. Ainda segundo os autores, os objetivos financeiros podem estar em três diferentes estágios:

- Crescimento rápido: ênfase em crescimento de vendas;
- Sustentação: retorno de capital investido, lucro operacional, e margem bruta;
- Fluxo de caixa: retorno imediato de investimento.

Perspectiva de cliente: Identificação de clientes e segmentos de mercado, os quais as unidades de negócio irão competir. São coletadas métricas genéricas de lucro para a medição da estratégica operacional implementada. Por exemplo: satisfação e retenção de clientes, aquisição de novos clientes, *market share* em determinado segmento, etc.

Perspectiva de processos internos: identificação dos processos da organização que precisam ser avaliados e melhorados constantemente. As métricas precisam ser focadas em processos que terão maior impacto na satisfação de clientes e objetivos financeiros.

Perspectiva de aprendizado e crescimento: foca nos processos e infraestrutura necessários para manutenção a longo prazo de crescimento e melhoria, buscando o aumento na capacidade das entregas de valores para clientes e acionistas (KAPLAN e NORTON, 1997). As perspectivas do modelo clássico de *Balanced Scorecard* são ilustradas na figura 1.

Segundo Prieto et al. (2006):

> Visto de maneira integrada, o *balanced scorecard* traduz o conhecimento, habilidades e sistemas que os empregados precisarão (seu aprendizado e crescimento), para inovar e construir as capacidades estratégicas certas e eficientes (processos internos) que entregarão valor específico ao mercado (clientes), os quais, eventualmente, proporcionarão o aumento do valor ao acionista (financeiro).

2.1.1 Balanced Scorecard para Tecnologia da Informação

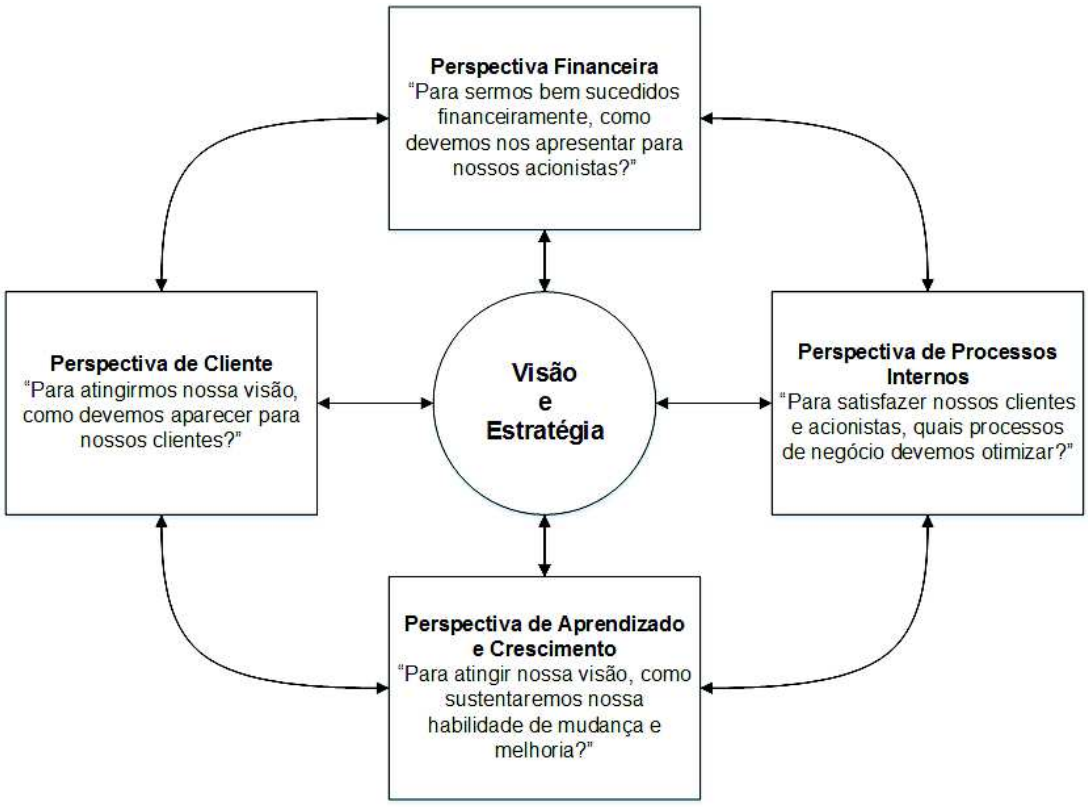
O retorno nos investimentos em segurança ou a perda sem os investimentos relativos são complicados de quantificar devido à dificuldade em definir e medir a abrangência total dos custos versus benefícios (HERATH et al., 2010). Em contrapartida, segundo Camp e Wolfram (2004), as consequências de incidentes de segurança que ameaçam a sobrevivência das organizações incluem danos a reputação que podem ter impacto negativo em clientes, fornecedores, mercado financeiro, bancos e outras relações de negócios. De acordo com Herath (2010), mecanismos de segurança agregam valor para organização de formas que não são capturadas por métodos de contabilização tradicionais. Assim, técnicas de medida de desempenho são necessárias para incorporar métricas quantitativas e medidas qualitativas mais abstratas.

Complementando e contextualizando a necessidade já descrita, o *Information Security Governance* (2006), elenca os cinco principais entregáveis de uma governança de segurança da informação, como:

- Alinhamento estratégico: alinhamento da segurança da informação com estratégica de negócio para apoiar os objetivos organizacionais;
- Gestão de Riscos: gerenciamento efetivo e mitigação de riscos de segurança implementando controles custo-efetivos e reduzindo potenciais impactos em recursos de segurança da informação a um nível aceitável;
- Gestão de recursos: gerenciamento efetivo e eficaz da infraestrutura e do conhecimento em segurança da informação;
- Gerenciamento de desempenho: medição, monitoramento e divulgação para garantir que as iniciativas de segurança da informação estão ajudando nos objetivos organizacionais; e

- Entrega de valor: otimização de investimentos em segurança para atingir objetivos organizacionais.

Figura 1 - Modelo clássico de um Balanced Scorecard



Fonte: Kaplan e Norton (1997).

Conforme Herath (2010) afirma, o modelo BSC possui como características o alinhamento e a medição de desempenho para aplicação da estratégia, e pode ser gerado para apoiar o monitoramento das metas organizacionais de gestão de riscos, gestão de recursos, entrega de valor, entre outras funções da governança de segurança da informação.

2.2 Gestão de Segurança da Informação

2.2.1 Conceitos

Informação é o dado com uma interpretação lógica ou natural dada a ele por seu utilizador (REZENDE e ABREU, 2009). Uma empresa busca, por meio da segurança de suas informações, garantir dentro do possível a continuidade de seus negócios, incrementando a estabilidade e permitindo que as pessoas e os bens estejam seguros de ameaças e perigos (SANTO, 2011). Ativo é tudo aquilo que

possui valor para a organização (ISO/IEC, 2005). Além de informações, faz-se necessário o cuidado com a segurança de todos os demais componentes dos processos da organização. De acordo com Ramos (2008), os ativos podem ser classificados nas seguintes categorias:

- Tangíveis: Informações impressas ou digitais; impressoras; Móveis.
- Intangíveis: Imagem de uma empresa; Confiabilidade de órgão federal; Marca de um produto.
- Lógicos: Dados armazenados em um servidor; Sistema ERP; Rede VoIP.
- Físicos: Estação de Trabalho; Sistema de ar-condicionado; Fábrica.
- Humanos: Empregados; Prestadores de Serviço.

2.2.1.1 Aspectos da Segurança da Informação

Em geral, os principais aspectos de segurança da informação são definidos com a tríade Confidencialidade, Integridade e Disponibilidade (HARRIS, 2010).

- Confidencialidade: garante o nível necessário de sigilo das informações ao longo do seu ciclo de vida e impede a divulgação não autorizada.
- Integridade: A integridade dá-se pela manutenção do conteúdo e confiabilidade das informações e sistemas, e qualquer modificação não autorizada é impedida.
- Disponibilidade: Garantia de acesso aos dados e recursos em tempo viável para as pessoas autorizadas.

Ao longo do ciclo de vida de uma informação, os aspectos de segurança relacionados poderão ser afetados, independentemente de sua origem ou tipo, devido a ameaças e/ou vulnerabilidades inerentes as informações. Estes e demais conceitos relacionados aos riscos que as informações sofrem são descritos, conforme as normas ISO/IEC 27002 e ISO/IEC 27005 da seguinte forma:

- Vulnerabilidade: Fragilidade de um ou mais ativos que podem ser exploradas por uma ou mais ameaças.
- Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

- Impacto: Mudança adversa ao nível dos objetivos de negócio estabelecidos.
- Risco: Potencial que uma dada ameaça possui para explorar uma vulnerabilidade em um ativo ou grupo de ativos, e causar danos à organização, como consequência.
- Controle: forma de gerenciar o risco pode ser de natureza administrativa, técnica, de gestão ou legal.

Uma vez que os ativos possuem valor para a organização, faz-se necessário o mapeamento dos riscos associados a estes, já que indisponibilidade, parada ou falha deste ativo pode causar prejuízos para a organização. Estes riscos serão provenientes da existência de vulnerabilidades passíveis de serem exploradas por ameaças. Definidos os riscos, busca-se a identificação de controles para redução do risco a um nível aceitável (DE OLIVEIRA, 2014).

2.2.2 Família ISO/IEC 27000

A família ISO/IEC 27000 é uma série de padrões de Segurança da Informação desenvolvidos e publicados pelo *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC). Estes padrões provêm um framework de boas práticas na gestão de segurança da informação (ITGI, 2013). A figura 1 mostra o relacionamento entre as normas. Destaca-se como principais normas relacionadas a este artigo, as normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27004 e ISO/IEC 27005.

A norma ISO/IEC 27001 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (ISO/IEC, 2013). Segundo Saint-Germain (2005), o padrão ISO para Segurança da Informação provê abordagem mais aprofundada para um sistema de gestão. Embora outros guias e melhores práticas possam ser seguidos, estes possuem um viés mais técnico, voltado para tecnologias. O padrão ISO possibilita que a organização que procura estar em conformidade com as boas práticas de segurança passe por um processo de auditoria externa e receba seu certificado mundialmente reconhecido. A norma ainda salienta a importância de que o sistema de gestão de segurança da informação (SGSI) seja parte de, e esteja integrado com os processos da organização e com a estrutura de administração

global da organização, sendo a segurança considerada nos projetos dos processos, sistemas de informação e controles. A norma ISO/IEC 27001 foi desenvolvida de maneira que possa ser implementada em organizações de diferentes tamanhos e necessidades. (ISO/IEC, 2013).

ISO/IEC 27002 é um código de prática o qual descreve de forma mais detalhada os controles definidos no Anexo A da norma ISO/IEC 27001, tem como base para indicação de controles para as informações, a tríade confidencialidade, integridade e disponibilidade.

O padrão ISO/IEC 27004 provê um guia e direcionamentos no desenvolvimento e uso de medidas e métricas com o objetivo de avaliar a efetividade de um SGSI, incluindo a política do SGSI e seus objetivos e controles. As medições produzidas através da aplicação desse padrão contribuem como informação de entrada para o processo de revisão dos controles existentes e determinação de quando os controles devem ser melhorados ou alterados (ISO/IEC, 2009).

A norma ISO/IEC 27005 define a abordagem para alinhamento de segurança da informação com gestão baseada em riscos, tem como objetivo possibilitar a gestão dos riscos que poderão comprometer a segurança das informações (ISO/IEC, 2008).

Outras normas foram desenvolvidas a fim de detalhar a implementação de um SGSI para nichos organizacionais específicos, como Instituições Financeiras (ISO/IEC 27015), Telecomunicações (ISO/IEC 27011) e Sistemas de Saúde (ISO/IEC 27799), entre outros.

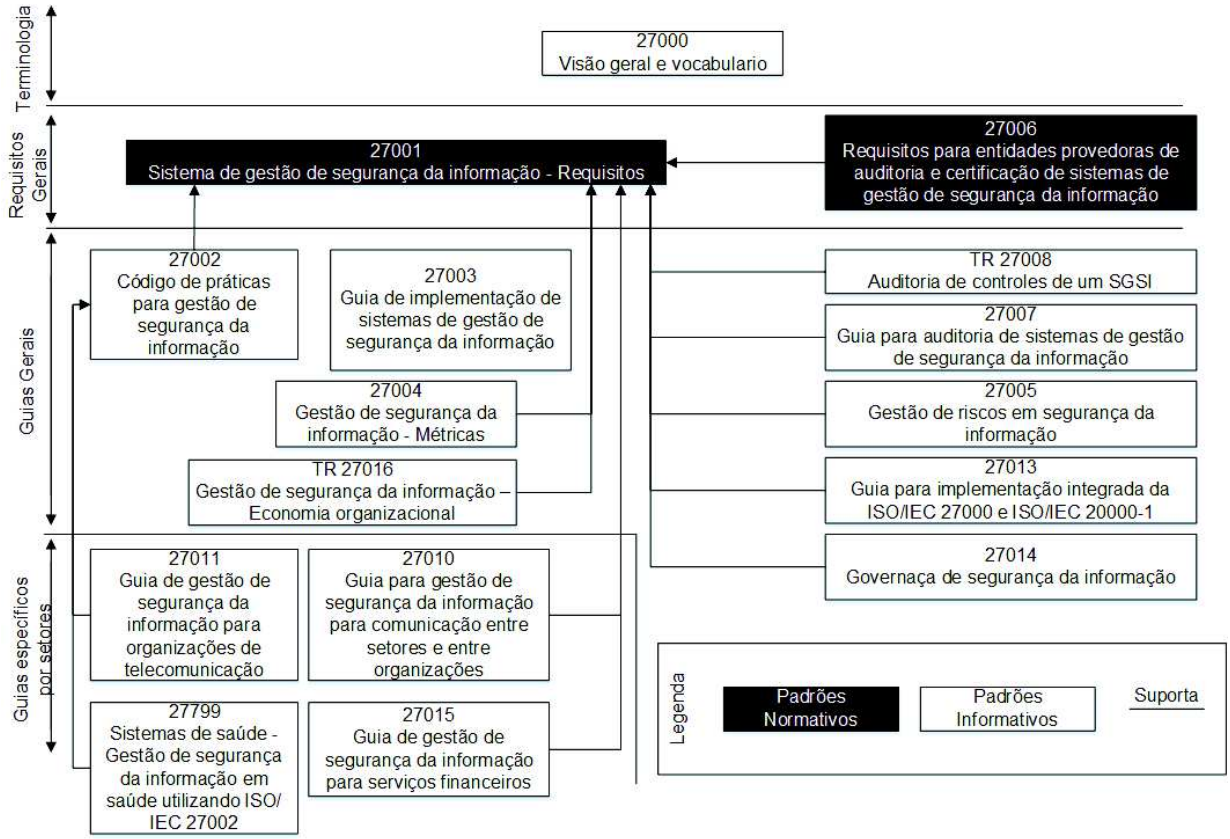
2.3 Governança de Segurança da Informação

De acordo com ITGI (2006), a governança de segurança da informação consiste em liderança, estrutura organizacional e processos para salvaguarda de informações. Sendo suas principais saídas, os seguintes itens:

- Alinhamento estratégico de segurança da informação com o negócio, apoiando os objetivos organizacionais;
- Gestão de riscos e redução de impactos a níveis aceitáveis;
- Gestão de recursos eficaz e eficiente;

- Gestão de desempenho por meio de medição, monitoramento e métricas para atingir os objetivos estabelecidos; e
- Entrega de valor pela otimização de investimentos e apoio ao negócio.

Figura 2 - Relacionamento entre a família de normas ISO/IEC 27000



Fonte: Adaptado de ISO/IEC (2014).

Segundo Von Solms et al. (2011), governança em segurança da informação se tornou uma das áreas-chave para gestão estratégica, devido a sua importância na proteção geral dos ativos da organização. O autor ainda afirma que sendo a governança de SI aplicada de forma efetiva, com o apoio da alta direção, caracterizando, portanto, um processo "*top-down*", deverá ser possível delinear as diretivas da gestão executiva do nível estratégico, através do nível tático, até o nível operacional. Corroborando a afirmação, a UCISA (2005), afirma que a governança é a fundação de um sistema de gestão de segurança da informação, pelo fato do SGSI prover frameworks tanto estratégicos como a nível operacional.

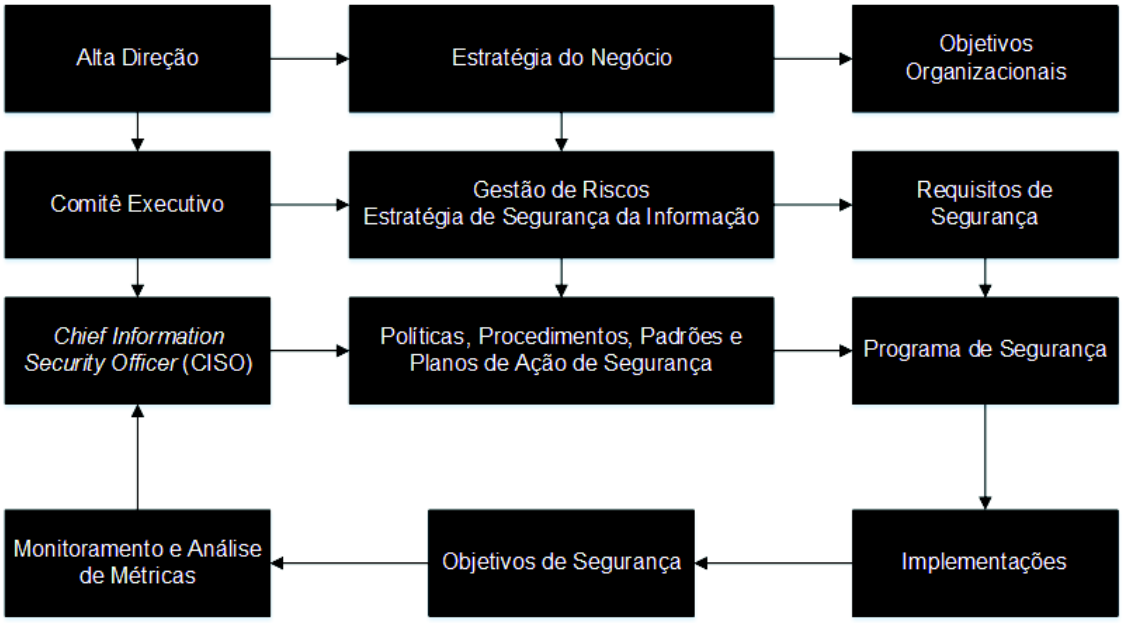
Como benefícios da governança de SI, o ITGI (2006) elenca alguns pontos:

- Aumento na confiança da relação com o cliente;
- Proteção da reputação da organização;

- Aumento na confiança entre parceiros de negócio;
- Redução no custo operacional, por meio da mitigação de fatores de risco.

A figura 3 ilustra os componentes necessários no desenvolvimento de uma governança de segurança da informação alinhada aos objetivos de negócio.

Figura 3 – Componentes da Governança de Segurança da Informação



Fonte: ITGI (2006).

Alguns padrões e normas foram desenvolvidos com o intuito de integrar elementos de segurança à estratégia organizacional, dentre eles pode-se citar o *Control Objectives for Information and related Technology* (CobIT) e as normas ISO/IEC 27001 e 27014.

2.4 Governança de Tecnologia da Informação

Segundo Gartner (2016), governança de TI é o processo que garante a efetividade e eficiência do uso da TI como facilitador na organização para alcançar seus objetivos. A ISACA (2005) corrobora a afirmação, adicionando que a governança de TI cobre a cultura organizacional, políticas e práticas que produzem uma espécie de vigilância e transparência de TI. Fazendo parte da governança corporativa, mas com seu foco específico.

IBM (2007) define que a boa governança de TI alinha as estratégias de negócio ao apoio e a evolução de uma arquitetura empresarial para que possam ser entregues valores de negócio consistentes e escaláveis.

ISACA (2005) define que a governança de TI prove gestão e controle por meio de cinco áreas:

- Alinhamento: provido pelos direcionamentos estratégicos de TI e o alinhamento de TI e negócio a respeito de serviços e projetos.
- Entrega de Valor: supervisiona a entrega de valor pela TI para o negócio, e avaliando o retorno sobre investimentos.
- Gestão de Riscos: garante que os processos estão rodando para garantir que riscos possam ser adequadamente gerenciados.
- Gestão de Recursos: provê direcionamento de alto nível para fontes e usos dos recursos de TI.
- Gestão de Desempenho: valida a conformidade estratégica, por exemplo, atingindo os objetivos estratégicos de TI. Revisa as medidas de desempenho de TI e a contribuição da TI para com o negócio.

Embora não haja um único e completo framework de governança de TI, existem alguns disponíveis publicamente e que servem como um ótimo ponto de partida para o desenvolvimento de um modelo de governança. Dentre os quais, podemos destacar os seguintes:

ISO/IEC 38500 é o padrão internacional para governança de TI. Provê guia de implementação para membros da administração de companhias para efetividade, eficiência e uso aceitável de tecnologia da informação dentro das organizações. Essa norma é aplicável para qualquer organização, incluindo companhias públicas e privadas, entidades governamentais e organizações filantrópicas.

Control Objectives for Information and Related Technology (CobIT) é um framework de governança de TI, desenvolvido em 1996, que ajuda as organizações a vencer os desafios de negócios nas áreas regulatórias, gestão de riscos e alinhamento estratégico da TI com os objetivos organizacionais (ITGI, 2016). CobIT é dividido entre 34 objetivos de controle de alto nível agrupados em 4 domínios:

- Planejar e organizar;
- Adquirir e implementar;
- Entregar e suportar;

- Monitorar e avaliar.

Para o desdobramento dos objetivos estratégicos em objetivos específicos de Tecnologia da Informação, o Cobit 5 (2012) apresenta a seguinte sequência de etapas:

Direcionadores das partes interessadas: mudanças nas estratégicas, mudanças nos negócios, regulamentações, entre outros, são aspectos possíveis de influenciar as partes interessadas;

Desdobramento das necessidades em objetivos estratégicos: relacionamento entre as necessidades e objetivos estratégicos genéricos, organizados nas perspectivas de um *balanced scorecard*. O Cobit 5 define 17 objetivos estratégicos, conforme a tabela 1 ilustra;

Tabela 1 - Objetivos corporativos do Cobit

Dimensão BSC	**Objetivo Corporativo**
Financeira	Valor dos investimentos da organização percebidos pelas partes interessadas
	Portfólio de produtos e serviços competitivos
	Gestão do risco do negócio (salvaguarda de ativos)
	Conformidade com as leis e regulamentos externos
	Transparência financeira
Cliente	Cultura de serviço orientada ao cliente
	Continuidade e disponibilidade do serviço de negócio
	Respostas rápidas para um ambiente de negócios em mudança
	Tomada de decisão estratégica com base na informação
	Otimização dos custos de prestação de serviços
Operacional	Otimização da funcionalidade do processo de negócio
	Otimização dos custos do processo de negócio
	Gestão de programas de mudanças de negócios
	Produtividade operacional e da equipe
	Conformidade com as políticas internas
Aprendizado e Crescimento	Pessoas qualificadas e motivadas
	Cultura de inovação de produtos e negócios

Fonte: ISACA (2012).

Cascata de objetivos estratégicos para objetivos de TI: o atingimento dos objetivos estratégicos depende de uma série de resultados relacionados a TI. O Cobit 5 define 17 objetivos de TI, também estruturados nas perspectivas de um BSC, conforme mostra a tabela 2.

Cascata dos objetivos de TI em metas dos habilitadores: Habilitadores incluem processos, estruturas organizacionais e informações e para cada habilitador um conjunto de metas podem ser definidos para apoiar os objetivos de TI.

Tabela 2 – Objetivos de TI do Cobit

Dimensão BSC de TI	Objetivos de TI
Financeira	Alinhamento da estratégia de negócios e de TI
	Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	Compromisso da gerência executiva com a tomada de decisões de TI
	Gestão de risco organizacional de TI
	Benefícios obtidos pelo investimento de TI e portfólio de serviços
	Transparência dos custos, benefícios e riscos de TI
Cliente	Prestação de serviços de TI em consonância com os requisitos de negócio
	Uso adequado de aplicativos, informações e soluções tecnológicas
Operacional	Agilidade de TI
	Segurança da informação, infraestrutura de processamento e aplicativos
	Otimização de ativos, recursos e capacidades de TI
	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	Conformidade de TI com as políticas internas
Aprendizado e Crescimento	Equipes de TI e de negócios motivadas e qualificadas
	Conhecimento, expertise e iniciativas para inovação dos negócios

Fonte: ISACA (2012).

Além dos itens apresentados, podemos citar ainda o modelo de maturidade de processos de TI apresentado pelo Cobit.

2.5 Mercado de Cartões

O mercado de cartões de crédito é composto por cinco entidades, são eles: a bandeira, o emissor, o portador do cartão, o adquirente e o estabelecimento comercial. As definições desses elementos, segundo Freitas (2007), são as seguintes:

- Bandeiras: são instituições que autorizam o uso de sua marca e de sua tecnologia por emissores e credenciadoras de estabelecimentos. Essas marcas aparecem nos cartões e nos estabelecimentos credenciados;
- Emissor: é o agente que se relaciona diretamente com o portador de cartão. Oferta serviços, determina limites de crédito, autoriza compras, etc.;
- Portador do cartão: principal elemento dentro do processo. É quem usa o cartão, titular ou adicional, nos estabelecimentos. Ou seja, quem de fato inicia a transação eletrônica;
- Adquirente: credencia os estabelecimentos comerciais para que possam aceitar transações eletrônicas por meio de cartões de crédito. Suas funções ainda incluem captura, transmissão, processamento e liquidação financeira de transações. O adquirente possui sua receita baseado em percentual sobre o valor de cada transação. Além de receita a partir de aluguel de *Points of Sales* e antecipação de recebíveis.
- Estabelecimento comercial: Pessoa física ou jurídica autorizada a aceitar pagamentos via cartão de crédito (OLIVEIRA, 2014).

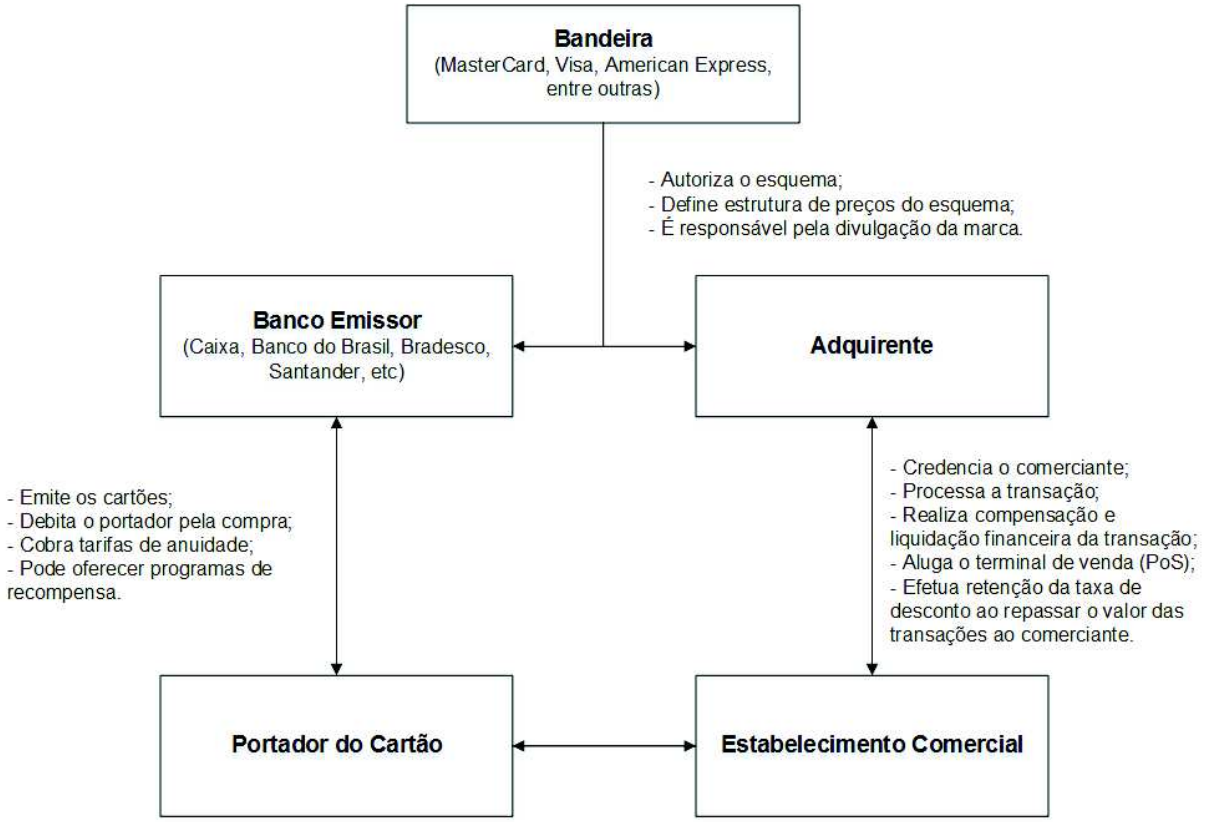
A figura 5 ilustra o relacionamento entre as entidades supracitadas.

2.5.1 Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI-DSS)

O PCI-DSS é um conjunto de requisitos elaborados por um conselho composto pelas principais empresas da indústria de cartões de pagamento com o objetivo de garantir que as companhias que processam, armazenam ou transmitam dados de cartão mantenham seu ambiente seguro (PCI-SSC, 2006). O *Payment Card Industry Security Standards Council* (PCI-SSC) foi criado em 2006 para administração da evolução da indústria de cartões de pagamento. O PCI-DSS é gerenciado por esse conselho, o qual é composto pelas principais bandeiras de cartões do mercado – Visa, MasterCard, American Express, Discover e JCB. O PCI-DSS encontra-se em sua versão 3.1 (2015), composta por 12 requisitos e 240 controles. A tabela 3 descreve de maneira geral esses requisitos. Os comerciantes que aceitam cartões de crédito ou débito como meio de pagamento de seus clientes,

devem seguir os requisitos definidos pelo PCI-DSS. Os níveis de conformidade requeridos pelo PCI-DSS variam de acordo com cada bandeira e o volume de transações realizadas.

Figura 4 - Relacionamento das principais entidades no mercado de cartões



Fonte: Adaptado de PCI-SSC (2015).

Tabela 3 – Requisitos PCI-DSS

Categoria	Requisito
Construir e manter os sistemas e a rede segura	1. Instalar e manter um firewall para proteger dados de cartão de crédito.
	2. Não utilizar senhas padrão ou outras configurações de segurança dos softwares utilizados.
Proteger as Informações dos portadores de cartão	3. Proteger dados de cartões de crédito armazenados.
	4. Utilizar criptografia na transmissão de dados de cartões de crédito, manter um programa de Gerenciamento de Vulnerabilidades.
Manter um programa de gestão de vulnerabilidades	5. Utilizar regularmente programas anti-vírus.
	6. Desenvolver e manter sistemas e aplicações seguras, implementar um forte controle de acesso.
Implementar medidas rigorosas de controle de acesso	7. Restringir acesso a dados de cartões de crédito por negócio e por pessoas que realmente precisam acessá-los.
	8. Designar um único identificador para cada usuário da rede e sistemas.
	9. Restringir acesso físico aos dados de cartão de crédito, testar e monitorar a rede regularmente.
Monitorar e testar as redes regularmente	10. Rastrear e monitorar todos os acessos à rede e dados de cartões de crédito.
	11. Testar a segurança de sistemas e processos regularmente, manter um programa de Gerenciamento de Vulnerabilidades.
Manter uma política de segurança da informação	12. Manter uma política que enderece informações de segurança.

Fonte: Adaptado de PCI-SSC (2015).

3 REVISÃO SISTEMÁTICA DA LITERATURA

Para maior assertividade na revisão sistemática da literatura, foi utilizada a metodologia proposta por Dresch et al. (2015), a qual é composta pelas etapas que seguem.

3.1 Definição da Questão

Revisão agregativa, ou seja, teste de teoria a partir de observações empíricas buscando aplicações teóricas ou práticas de artefatos que se apresentem como solução para a obtenção de alinhamento entre a estratégia da organização e a segurança das informações.

3.2 Escolha da Equipe de Trabalho

Devido a participação ativa do autor do projeto junto aos processos analisados, não será necessária a criação de uma equipe para coleta de

informações. Assim como, para a pesquisa e revisão da literatura a respeito dos assuntos envolvidos. Dessa forma, a equipe de trabalho será formada pelo autor e o orientador desse artigo.

3.3 Estratégia de Busca

Os seguintes itens caracterizam a busca realizada para os modelos e trabalhos relacionados a pesquisa do presente artigo.

3.3.1 Termos de Busca

- Segurança da informação; métricas; balanced scorecard; BSC; information security; metrics; governança; governance.
- (Segurança da Informação OR Information Security) OR (BSC OR Balanced Scorecard)
- (Segurança da Informação OR Information Security) AND (Métricas OR Metrics OR KPI)
- (Segurança da Informação OR Information Security) AND (Desempenho OR Performance)
- (Segurança da Informação OR Information Security) AND (BSC OR Balanced Scorecard)
- (Governança OR Governance) AND (BSC OR Balanced Scorecard)
- (Governança OR Governance) AND (Métricas OR Metrics OR KPI)

3.3.2 Fontes para Busca

- Base de dados eletrônicas: Google Acadêmico, Research Gate, IEEE Xplore Digital Library, ScienceDirect, ACM Digital Library, Emerald Insight.
- Busca manual: Livros, revistas, sites.

3.3.3 Critério de Inclusão e Exclusão

- Inclusão: Boas práticas de mercado; Padrões internacionais; aplicação prática; estudo de caso; ano de publicação (15 anos ou menos).
- Exclusão: Idioma não português/inglês; aplicação fora de segurança da informação ou governança de TI; artefatos sem proposta prática.

3.4 Busca, Elegibilidade e Codificação

A listagem dos estudos encontrados a partir da estratégia de busca pode ser observada na tabela 4.

Tabela 4 – Consolidação da coleta de estudos relacionados.

Estudos Encontrados	Estudos Incluídos	Estudos Excluídos
KONG, Hee-Kyung; KIM, Tae-Sung; KIM, Jungduk. **An analysis on effects of information security investments: a BSC perspective**. Em: Journal of Intelligent Manufacturing, v. 23, n. 4, p. 941-953, 2012.	X	-
Information Systems Audit and Control Association (ISACA), **An Introduction to the Business Model for Information Security.** EUA, 2009	-	X
Information Systems Audit and Control Association (ISACA), **From Here to Maturity Management - The Information Security Life Cycle.** Em: *ISACA Journal,* v. 6, 2014	-	X
VOLCHKOV, Andrej. **How to Measure Security From a Governance Perspective**. Information Systems Control Journal, v. 5, p. 44-351, 2013.	-	X
HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. **Balanced scorecard implementation of security strategies: a framework for IT security performance management**. Information Systems Management, v. 27, n. 1, p. 72-81, 2010.	X	-
HUANG, Shi-Ming; LEE, Chia-Ling; KAO, Ai-Chin. **Balancing performance measures for information security management: A balanced scorecard framework**. Em: Industrial Management & Data Systems, v. 106, n. 2, p. 242-255, 2006.	X	-
SANGKYUN, K. I. M.; KO, Franz IS. **BSC-based Evaluation on Security Risks of IT Infrastructure**. Em: Journal of Convergence Information Technology, v. 7, n. 15, 2012.	X	-
SUER, Myles. **COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement**. COBIT Focus, v.1, p.5, 2013	X	-

Estudos Encontrados	Estudos Incluídos	Estudos Excluídos
GOLDMAN, James E.; AHUJA, Suchit. **Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework**. **ICT Ethics and Security in the 21st Century: New Developments and Applications**, p. 277-309, 2011.	X	-
VAN GREMBERGEN, Wim; SAULL, Ronald; DE HAES, Steven. **Linking the IT balanced scorecard to the business objectives at a major Canadian financial group**. **Journal of Information Technology Case and Application Research**, v. 5, n. 1, p. 23-50, 2003.	X	-
VAN GREMBERGEN, Wim; DE HAES, Steven. **Measuring and improving IT governance through the balanced scorecard**. Em: Information Systems Control Journal, v. 2, n. 1, p. 35-42, 2005.	X	-
SILVA, Rozelito Felix da. **Proposta de adaptação do modelo Balanced Scorecard: BSC para a gestão de segurança da informação em órgãos da administração pública**. 2010. 82 f. Dissertação (Mestrado em Engenharia Elétrica), Universidade de Brasília, Brasília, 2010.	X	-
MARCELINO, Carmen Lúcia Nunes. **Segurança de Informação na Estratégia Empresarial - BSC**: Estudo de caso. Setúbal, 2014. 73 f. Dissertação (Mestrado em Sistemas de Informação Organizacionais) - Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Setúbal, 2014.	X	-
VAN GREMBERGEN, Wim. **The balanced scorecard and IT governance**. IRMA Conference**,** p. 1123-1124, 2000.	X	-
KAPUR, Rajesh. **Use of the Balanced Scorecard for IT Risk Management**. ISACA Journal, v.5, p.45, 2010.	X	-
GARTNER. **Toolkit: Developing a Balanced Scorecard for Security**. Maio de 2014. Disponível em: <https://www.gartner.com/doc/2740419/toolkit-developing-balanced-scorecard-security>. Acesso em: 15 dez. 2015.	-	X

Fonte: Elaborado pelo autor.

3.5 Avaliação de Qualidade

Para análise de qualidade dos estudos escolhidos, foram utilizados os critérios e classificações descritos na tabela 5.

Tabela 5 – Critérios para classificação dos estudos

Nível	Qualidade na execução do estudo	Adequação à questão de revisão	Adequação ao foco da revisão
Alto	O método proposto atende aos padrões exigidos para o tema em estudo, o estudo seguiu o método proposto.	O estudo aborda exatamente o assunto alvo da revisão sistemática.	O estudo foi realizado em um contexto idêntico ao definido para a revisão.
Médio	O método proposto possui algumas lacunas relacionadas ao tema ou o estudo não demonstra ter seguido o método proposto em sua totalidade, ou os resultados não se apoiam integralmente em fatos.	O estudo aborda parcialmente o assunto alvo da revisão sistemática.	O estudo foi realizado em um contexto semelhante ao definido para a revisão.
Baixo	O método proposto não está de acordo com os aplicáveis ao tema ou os estudos não seguiram os métodos propostos ou os resultados não se baseiam em fatos.	O estudo apenas tangencia o assunto alvo da revisão sistemática.	O estudo foi realizado em um contexto diverso ao definido para a revisão.

Fonte: adaptado de Dresch et al. (2015).

Os resultados da avaliação dos estudos seguiram a matriz representada na tabela 6. Todos os estudos que tiveram classificação “Baixa” foram desconsiderados. A tabela 7 ilustra a classificação dos trabalhos escolhidos para análise.

Tabela 6 – Matriz de classificação

Análise			**Classificação**
Alta	Alta	Alta	**Alta**
Alta	Alta	Média	**Média**
Alta	Média	Média	**Média**
Média	Média	Média	**Média**
Alta	Alta	Baixa	**Baixa**
Alta	Média	Baixa	**Baixa**
Média	Média	Baixa	**Baixa**
Média	Baixa	Baixa	**Baixa**
Baixa	Baixa	Baixa	**Baixa**

Fonte: Dresch et al. (2015).

Tabela 7 – Consolidação da avaliação dos estudos relacionados.

Estudo	Qualidade na execução do estudo	Adequação à questão de revisão	Adequação ao foco da revisão	Avaliação do Estudo
KONG, Hee-Kyung; KIM, Tae-Sung; KIM, Jungduk. **An analysis on effects of information security investments** (2012)	Alta	Média	Alta	Média
HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. **Balanced scorecard implementation of security strategies** (2010)	Alta	Média	Média	Média
HUANG, Shi-Ming; LEE, Chia-Ling; KAO, Ai-Chin. **Balancing performance measures for information security management** (2006)	Alta	Alta	Alta	Alta
SANGKYUN, K. I. M.; KO, Franz IS. **BSC-based Evaluation on Security Risks of IT Infrastructure** (2012)	Alta	Baixa	Baixa	Baixa
SUER, Myles. **COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement**. (2013)	Média	Média	Baixa	Baixa
GOLDMAN, James E.; AHUJA, Suchit. **Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework** (2011)	Média	Baixa	Baixa	Baixa
VAN GREMBERGEN, Wim; SAULL, Ronald; DE HAES, Steven. **Linking the IT balanced scorecard to the business objectives at a major Canadian financial group**. (2003)	Alta	Média	Alta	Alta
VAN GREMBERGEN, Wim; DE HAES, Steven. **Measuring and improving IT governance through the balanced scorecard**. (2005)	Alta	Média	Média	Média
SILVA, Rozelito Felix da. **Proposta de adaptação do modelo Balanced Scorecard** (2010)	Alta	Média	Média	Média
MARCELINO, Carmen Lúcia Nunes. **Segurança de Informação na Estratégia Empresarial - BSC: Estudo de caso**. (2014)	Alta	Alta	Alta	Alta

Estudo	Qualidade na execução do estudo	Adequação à questão de revisão	Adequação ao foco da revisão	Avaliação do Estudo
VAN GREMBERGEN, Wim. **The balanced scorecard and IT governance**. (2000)	Média	Baixa	Baixa	Baixa
KAPUR, Rajesh. **Use of the Balanced Scorecard for IT Risk Management**. (2010)	Alta	Média	Média	Média

Fonte: Elaborado pelo autor.

3.6 Síntese dos Resultados

A tabela 8 apresenta a síntese da etapa de revisão sistemática da literatura. Sendo o resultado “positivo” para aqueles estudos que foram selecionados para compor o presente artigo, e “negativo” os artigos descartados devido ao resultado da avaliação pelos critérios já apresentados.

Tabela 8 – Resultado da revisão sistemática.

Estudo Primário	Problema	Artefato	Fatores Internos	Fatores Externos	Resultado
KONG, Hee-Kyung; KIM, Tae-Sung; KIM, Jungduk. **An analysis on effects of information security investments** (2012)	Falha em eficácia e desempenho de investimento em SI	BSC	Identificação de objetivos estratégicos organizacionais; Objetivos estratégicos de SI;	Sem delimitações	Positivo
HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. **Balanced scorecard implementation of security strategies** (2010)	Avaliação adequada para investimentos em segurança tecnológica	BSC	Identificação de objetivos estratégicos organizacionais; Objetivos estratégicos de SI; Definições de investimentos	Sem delimitações	Positivo

Estudo Primário	Problema	Artefato	Fatores Internos	Fatores Externos	Resultado
			estratégicos e em segurança tecnológica.		
HUANG, Shi-Ming; LEE, Chia-Ling; KAO, Ai-Chin. **Balancing performance measures for information security management** (2006)	Boas práticas para guiar a relação entre estratégia organizacional e indicadores de desempenho para projetos em segurança da informação	KPI	Identificação de objetivos estratégicos organizacionais; Objetivos estratégicos de SI; Definições de investimentos estratégicos e em segurança da informação; Definições sobre ROI.	Empresas de manufatura de Taiwan	Positivo
SANGKYUN, K. I. M.; KO, Franz IS. **BSC-based Evaluation on Security Risks of IT Infrastructure** (2012)	Avaliação adequada de riscos e investimentos em segurança da informação	BSC	Definições de objetivos estratégicos baseados nas perspectivas do balanced scorecard; Medidas de desempenho.	Sem delimitações	Negativo
SUER, Myles. **COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement**. (2013)	Modelo de medição de desempenho em segurança da informação utilizando o alinhamento entre CobIT 5 e BSC	BSC	Artigo conceitual e genérico	Sem delimitações	Negativo

Estudo Primário	Problema	Artefato	Fatores Internos	Fatores Externos	Resultado
GOLDMAN, James E.; AHUJA, Suchit. **Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework** (2011)	Desalinhamento entre o CobIT e o modelo de Balanced Scorecard	ISM Framework	Revisão da literatura, sem limitações internas	Sem delimitações	Negativo
VAN GREMBERGEN, Wim; SAULL, Ronald; DE HAES, Steven. **Linking the IT balanced scorecard to the business objectives at a major Canadian financial group**. (2003)	Análise crítica do Balanced Scorecard de Tecnologia da Informação de uma organização canadense	BSC	Análise dos processos organizacionais, indicadores de desempenho e suas integrações	Grupo financeiro canadense	Positivo
VAN GREMBERGEN, Wim; DE HAES, Steven. **Measuring and improving IT governance through the balanced scorecard**. (2005)	Como avaliar o nível da implementação de uma governança de TI?	BSC	Indicadores de desempenho e mapeamento de processos para as perspectivas do BSC	Sem delimitações	Positivo
SILVA, Rozelito Felix da. **Proposta de adaptação do modelo Balanced Scorecard** (2010)	Análise crítica da situação atual da gestão estratégica da segurança da informação no Departamento de Segurança da Informação e Comunicações (DSIC)	BSC	Identificação dos objetivos estratégicos, metas, indicadores e ações, referentes às perspectivas do BSC	Departamento de Segurança da Informação e Comunicações (DSIC) do governo brasileiro	Positivo
MARCELINO, Carmen Lúcia Nunes. **Segurança de Informação na Estratégia Empresarial – BSC: Estudo de caso**. (2014)	Alinhamento entre objetivos estratégicos e de SI	BSC	Identificação de missão, visão, valores, objetivos estratégicos, atividades críticas, riscos e indicadores de desempenho	Estudo de caso específico para a organização em questão.	Positivo

Estudo Primário	Problema	Artefato	Fatores Internos	Fatores Externos	Resultado
VAN GREMBERGEN, Wim. **The balanced scorecard and IT governance**. (2000)	Como o IT BSC pode ser relacionado ao BSC organizacional?	BSC	Artigo conceitual e genérico	Sem delimitações	Negativo
KAPUR, Rajesh. **Use of the Balanced Scorecard for IT Risk Management**. (2010)	Alinhamento entre riscos de TI e estratégia organizacional	BSC	Identificação dos objetivos estratégicos, metas, indicadores e ações, referentes às perspectivas do BSC	Sem delimitações	Positivo

Fonte: Elaborado pelo autor.

4 METODOLOGIA

4.1 Definições sobre a Metodologia

Com o objetivo de buscar o alinhamento dos processos do SGSI estabelecido com seus objetivos estratégicos da organização, definiu-se em conjunto com a coordenação do SGSI e os responsáveis pela elaboração e manutenção do mapa estratégico da companhia, a reorganização dos objetivos e processos do SGSI nas mesmas perspectivas já utilizadas pelo mapa da companhia.

Para isso, as ações necessárias foram organizadas como mostra a figura 6.

A tabela 9 correlaciona as atividades definidas na metodologia do projeto com os capítulos e sessões desse documento.

5 DESENVOLVIMENTO

Este capítulo descreverá as atividades realizadas durante as diferentes etapas de criação do *balanced scorecard* de segurança da informação, definidas a partir da metodologia de pesquisa ilustrada na figura 6.

5.1 Atividades iniciais

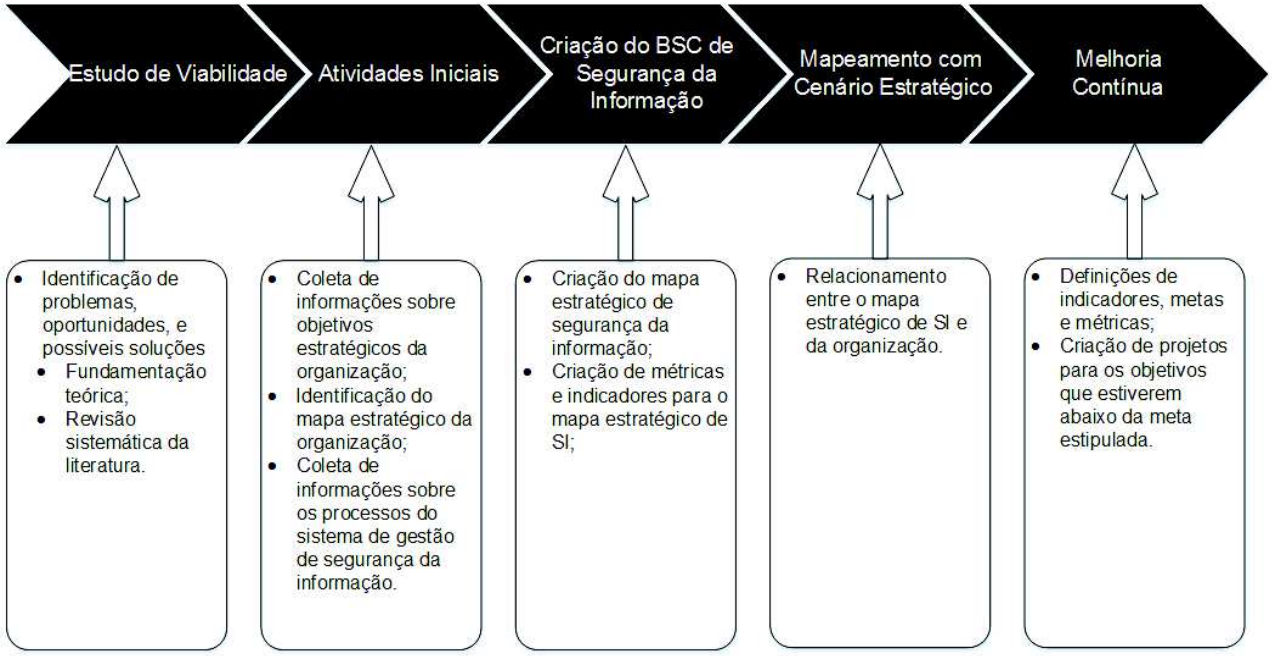
5.1.1 Coleta de informações sobre objetivos estratégicos da organização

Como primeira etapa para identificação das informações críticas a nível estratégico da organização, foram coletadas:

5.1.1.1 Visão geral da organização e contextualização

A empresa alvo desse estudo de caso atua no setor financeiro brasileiro, mais especificamente como adquirente transacional multibandeira, ou seja, possibilitando a realização de captura, transmissão e liquidação financeira de transações com cartões de crédito e débito para seus estabelecimentos comerciais clientes. Vem se consolidando como parceira de seus clientes, estabelecida entre os grandes players desse mercado, com crescimento consistente.

Figura 5 - Desenho da Pesquisa



Fonte: Elaborado pelo autor.

A segurança da informação é crítica para o negócio da organização. Roubo, vazamento ou divulgação indevida de dados de portadores de cartões de crédito acarretariam em fortes sansões por parte das bandeiras, incluindo a revogação do direito de transacionar as principais bandeiras do mercado para casos mais graves, o que poderia levar a empresa a falência. Por esse motivo, as principais bandeiras do mercado exigem que as empresas que queiram transacionar seus cartões sigam controles específicos de segurança contidos no conjunto de boas práticas PCI-DSS - *Payment Card Industry - Data Security Standard*. Tais controles são auditados por entidades credenciadas, sendo sua certificação validada anualmente.

De forma complementar aos controles exigidos pelo PCI-DSS, a organização decidiu se adequar também as exigências da norma ISO/IEC 27001, submetendo-se a mais esse processo de certificação para garantir aos seus clientes um nível superior de confiança em suas transações.

5.1.1.2 Missão

Ser referência e liderança em soluções tecnológicas para transações eletrônicas.

Tabela 9 – Relacionamento entre a metodologia e os capítulos do projeto

Etapas da Metodologia		Capítulo/Sessão
Estudo de Viabilidade	Identificação de problemas, oportunidades e possíveis soluções;	1. Introdução
	Fundamentação teórica;	2. Referencial Teórico
	Revisão Sistemática da Literatura	3. Revisão Sistemática da Literatura
Atividades Iniciais	Coleta de informações sobre objetivos estratégicos da organização;	5.1 Atividades Iniciais
	Identificação do mapa estratégico da organização;	
	Coleta de informações sobre os processos do SGSI;	
Criação do BSC de SI	Criação do mapa estratégico de segurança da informação;	5.2 Criação do BSC de Segurança da Informação
	Criação de métricas e indicadores para o mapa de SI;	
Mapeamento com o Cenário Estratégico	Relacionamento entre o mapa estratégico de SI e da organização;	5.3. Mapeamento com o cenário estratégico
Melhoria Contínua	Definição de indicadores, metas e métricas;	5.4. Melhoria contínua
	Criação de projetos para os objetivos que estiverem abaixo da meta estipulada.	

Fonte: Elaborado pelo autor.

5.1.1.3 Visão

Prosperar de maneira sólida e sustentável junto aos nossos clientes.

5.1.1.4 Objetivos estratégicos

- Aumento do lucro e receita líquida;
- Crescimento sustentável da base ativa de clientes;
- Aumento do *market share*.

5.1.2 Identificação do mapa estratégico

O mapa estratégico da organização já utilizava o modelo de Business Scorecard, com suas quatro perspectivas. Iniciativas por áreas, utilizando as perspectivas do mapa estratégico para elaboração e priorização de projetos que poderiam ser utilizadas como modelo para esse projeto foram identificadas. Contudo, não foram disponibilizadas durante a fase de coleta de informações. A figura 7 ilustra o mapa estratégico da organização.

Figura 6 - Mapa estratégico da organização

Fonte: Elaborado pelo autor.

5.1.3 Coleta de informações sobre o SGSI

5.1.3.1 Escopo e processos do SGSI

O escopo do Sistema de Gestão de Segurança da Informação da companhia, de acordo com o certificado ISO/IEC 27001 de sua certificação, contempla as seguintes áreas da empresa:

- Alta direção
- Segurança da informação
- Infraestrutura e sustentação
- Recursos Humanos
- Governança de TI
- Jurídico
- Controles internos
- Riscos operacionais

A organização possui o Comitê de Segurança da Informação, composto pelas áreas supracitadas, o qual se reúne mensalmente para deliberação de assuntos

relacionado aos processos do SGSI. Nesse comitê são tomadas as decisões por meio de votação de maioria simples a respeito das ações, correções e melhorias nos processos e áreas relacionadas. Dessa forma, a organização visa mitigar possíveis impactos nos negócios, compartilhando conhecimento entre as áreas. Outro ganho percebido por meio desse comitê é o acompanhamento das atividades, sendo essa uma pauta fixa nas reuniões. As atas dessas reuniões são reportadas para o Comitê Executivo da organização.

Dentre as áreas que compõem o SGSI, foram identificados os seguintes processos documentados:

- Recrutamento e Seleção: descrição das ações realizadas no momento da escolha de candidatos a funcionário da organização;
- Rescisão de Contrato: processo de rescisão contratual, garantindo o retorno de bens da organização, revogação de acessos e validação do termo de confidencialidade no momento do desligamento;
- Gestão de Mudanças: procedimento que descreve as necessidades para solicitação de qualquer mudança dentro do ambiente da organização, a validação por meio de comitê responsável envolvendo todos as partes interessadas, e o reporte do resultado final da execução da atividade;
- Gestão de Continuidade de Negócio: procedimento que detalha o acionamento das ações em caso de desastre envolvendo a infraestrutura da organização;
- Acesso Físico ao Data Center: atividades relacionada a entrada de colaboradores, terceiros e visitantes ao ambiente do data center;
- Solicitação e Testes de Rotina de Backup: descrição de como solicitar e quais as opções possíveis de restauração de dados;
- Descarte Seguro de Mídias: procedimento sobre descarte de mídias que não serão mais reutilizadas pela organização. Descreve as ações para remoção dos dados contidos nas mídias;
- Gestão de Riscos em Segurança da Informação: procedimento que detalha a coleta de informações, critérios e níveis de risco, reporte para as partes interessadas e prazos para correção de riscos de acordo com seu nível e complexidade;

- Gestão de Vulnerabilidades Técnicas: detalhamento das etapas de identificação, encaminhamento, reporte e correção das vulnerabilidades no ambiente tecnológico da organização;
- Gestão de Incidentes de Segurança da Informação: identificação, investigação, classificação, reporte e ações acerca de incidentes de segurança da informação;
- Gestão de Perfis e Controle de Acessos: descrição das atividades de solicitação, concessão, revisão, re-certificação e revogação de acessos;
- Aceitação de Riscos de Segurança da Informação: ações necessárias para registro de riscos os quais não serão mitigados, reduzidos ou transferidos no primeiro momento;
- Ação Corretiva e Melhorias: procedimento para registro e acompanhamento dos planos de tratamento para os riscos, não conformidades ou melhorias identificadas nos processos organizacionais;
- Análise Crítica do SGSI pela Alta Direção: detalhamento das ações necessárias e registros das lacunas identificadas nos processos a partir da análise anual pela alta direção dos processos do SGSI;
- Auditoria do SGSI: descrição das ações anuais de auditoria interna no sistema de gestão de segurança da informação realizadas pelos colaboradores capacitados para a atividade requerida pela norma ISO/IEC 27001.

5.1.3.2 Plano diretor de segurança da informação

A organização possui o Plano Diretor de Segurança da Informação (PDSI), documento elaborado ao final de cada ano com intuito de guiar as ações do próximo ano de acordo com os resultados e evoluções durante o ano anterior. São entradas para a elaboração do PDSI:

- Gestão de Riscos de Segurança da Informação;
- Resultado da Auditoria Interna do SGSI;
- Resultado da Auditoria Certificadora do SGSI;

- Gestão de Vulnerabilidades Técnicas;
- Status dos Riscos Operacionais;
- Calendário de Atividades do SGSI.

Também são definidos objetivos de segurança da informação para o próximo período, com o objetivo de focalizar as ações. Cada objetivo possui projetos e ações relacionadas, as quais serão executadas ao longo do período. Para o ano de 2016, os objetivos foram sinalizados conforme a tabela 10.

5.2. Criação do BSC de Segurança da Informação

5.2.1 Mapa estratégico de Segurança da Informação

Tomando como base as informações coletadas na etapa anterior, foi desenvolvido junto ao coordenador do sistema de gestão de segurança da informação, buscando reorganização para alinhamento com as estratégias da organização e os objetivos relacionados ao SGSI já definidos no PDSI, os objetivos do SGSI pelas quatro perspectivas de um BSC. A tabela 12 ilustra essa subdivisão. Tomou-se como base para organização dos dados o modelo sugerido pelo Gartner (2010) para *balanced scorecard* de segurança da informação.

5.2.2 Métricas e Indicadores para o SGSI

Para cada objetivo em sua respectiva perspectiva, foram criadas medidas para acompanhamento de seu desempenho. Cada medida possui suas ações rotineiras já definidas dentro de seus processos que compõem o SGSI. Por exemplo: para o objetivo financeiro de "Gerenciamento de fornecedores de forma eficiente", as seguintes informações foram coletadas de seu processo: a) porcentagem de fornecedores com nota de avaliação superior a 8 (oito) e b) porcentagem de contratos com requisitos de segurança da informação definidos.

Para cada objetivo em sua respectiva perspectiva, foram criadas medidas para acompanhamento de seu desempenho. Cada medida possui suas ações rotineiras já definidas dentro de seus processos que compõem o SGSI. Por exemplo: para o objetivo financeiro de "Eficiência na gestão da segurança", definiu-se como medida de desempenho a "taxa de gastos anuais em proporção ao budget orçado".

Como forma de medição, foram definidos um objetivo percentual e um índice relacionado a perspectiva, além de um dado variável que representa o resultado da coleta ao longo do período. Por exemplo: a perspectiva financeira possui 4 (quatro) objetivos. "Eficiência na gestão de segurança" tem o peso de 25% do total da perspectiva financeira. A medida "Taxa de gastos anuais em proporção ao budget orçado" relacionada a esse objetivo tem como objetivo 100%. Ou seja, quanto mais próximo forem os gastos em relação ao budget previamente definido, melhor será o indicador. O resultado coletado no último período é de 115%. Representando 85% de desempenho em relação ao objetivo dessa medida. E 21,3% de desempenho relacionado ao total da perspectiva financeira.

De acordo com os critérios definidos para essa medida de desempenho, detalhados na tabela 11, o resultado tem indicador "M", ou seja, Médio.

Cada perspectiva possui uma meta e seu resultado, bem como um indicador de resultado da perspectiva. Sendo “Bom” (B) igual ou maior que a meta estabelecida, “Ruim” (R), abaixo de 80% da meta e “Médio” (M) entre 81% da meta até o atingimento da mesma.

As tabelas 12 mostra um sumário dos objetivos e suas respectivas medidas de desempenho. As tabelas 13, 14, 15 e 16 descrevem todos os indicadores elaborados para as perspectivas financeira, de cliente, operacional e de aprendizado e crescimento, respectivamente.

Tabela 10 - Objetivos do SGSI para 2016

Objetivos do SGSI
Otimização de gastos
Assertividade, eficácia e otimização de investimentos
Gestão de riscos em todas as áreas da organização
Redução ao máximo a probabilidade de casos de vazamento de dados
Melhoria contínua na eficácia dos controles de segurança
Reduzir a ocorrência de indisponibilidades não previstas no ambiente da companhia
Aumento da conscientização dos colaboradores

Fonte: Elaborado pelo autor.

5.2.2.1 Critérios para peso relativo das medidas de desempenho

Como forma de representação mais assertiva na representação dos resultados das medidas de desempenho em cada objetivo dentro das perspectivas do BSC, elaborou-se critérios para definição do peso percentual do resultado da medida. Segundo Andersen et al. (2008), adicionar peso aos indicadores de desempenho dá importância às medidas que são críticas para a organização, com a criticidade refletida nos resultados que aparecem no *scorecard*. Assim, em reunião com os responsáveis pelo SGSI, definiu-se o seguinte rito para definição dos pesos: cada medida de desempenho terá seu peso definido quando da inclusão ou alteração da mesma em reunião do comitê do SGSI, o qual contará com a aprovação de todos os membros dos processos envolvidos na medida, bem como a análise crítica da alta direção para validação do peso relativo em relação aos objetivos gerais do SGSI.

5.3 Mapeamento com o cenário estratégico

Criado o mapa estratégico do SGSI, foi possível realizar a correlação entre os objetivos estratégicos dentro do escopo de processos do SGSI e os mesmos a nível organizacional. Dessa forma, pode-se ilustrar de forma clara de que maneira e através de quais entregáveis de processos a segurança da informação agrega valor, de forma direta ou indireta, ao negócio da companhia, suportando de forma consistente e segura os processos de negócio, sem impeditivos ou burocratizações desnecessárias, visto que os objetivos finais ficam, por meio dessa correlação, alinhados. A figura 8 ilustra e correlaciona por meio de cores os dois níveis de mapas estratégicos.

Tabela 11 - Exemplo de acompanhamento de uma medida de desempenho

Ref.	Objetivo	Medida de Desempenho	Peso	Objetivo		Valor	Desempenho Relativo	Desempenho Absoluto	Tolerância	Regra de Tolerância	Observações
F2	Eficiência na gestão da segurança								M		
(i)		Taxa de gastos anuais em proporção ao budget orçado	25,0%	=	100%	115%	85%	21,3%	M	B >= 95%; R < 80%	Proporção de gastos em relação ao orçado. Valor próximo de 100% é o ideal.

Fonte: Adaptado de Gartner (2010).

Tabela 12 - Objetivos do SGSI por perspectivas do BSC

Balanced Scorecard de Segurança da Informação

InfoSec Balanced Scorecard — Sumário

Perspectiva Financeira	81%	M
F1 Segurança como auxílio para o crescimento do negócio		R
F2 Eficiência na gestão da segurança		M
F3 Execução de projetos de acordo com planejado		B
F4 Gerenciamento de fornecedores de forma eficiente		M

Perspectiva Operacional	78%	M
O1 Ferramentas adequadas às nossas necessidades		B
O2 Mudanças no ambiente de forma eficiente e confiável		B
O3 Melhoria contínua em nossos processos		M
O4 Manutenção de nosso risco operacional dentro do apetite definido		M

Perspectiva de Cliente	99%	B
C1 Provimento de disponibilidade e continuidade de nossos serviços		B
C2 Clientes com confiança em nossos serviços e instalações		B
C3 Cumprimento das regulamentações aplicáveis		M
C4 Acessos adequados às pessoas e funções - não mais, não menos		M

Perspectiva de Aprendizado e Crescimento	83%	M
AC1 Pessoas engajadas		B
AC2 Pessoas preparadas		B
AC3 Investimento em pessoas e desenvolvimento de suas especialidades		R
AC4 Proteção de nosso conhecimento como vantagem competitiva		R

Fonte: Adaptado de Gartner (2010).

Tabela 13 – Perspectiva financeira do BSC de Segurança da Informação

Perspectiva Financeira											
Ref.	Objetivo	Medida de Desempenho	Peso (constante)		Objetivo (constante)	Valor (variável)	Desempenho Relativo (calculado)	Desempenho Absoluto (calculado)	Tolerância Baseado no desempenho relativo	Regra de Tolerância	Observações
F1	Segurança como auxílio para o crescimento do negócio								R		
(i)		Investimentos em Segurança	12,5%	>=	75%	63%	84%	10,5%	M	B = 100%; R <= 80%	Objetivo é 75% ou mais de gastos para investimentos, e 25% ou menos para gastos em operações.
(ii)		Taxa de quebra de estimativas em projeto	12,5%	>=	5,00	0,00	17%	2,1%	R	B >= 80%; R <= 60%	Para cada projeto é definido um escore de gastos de -1 ("vermelho", significando que o gasto do projeto foi < 60% do budget ou > 140% do budget), 0 ("amarelo", gastos < 80% ou > 120% do budget) ou 1 ("verde", gastos entre 80% e 120% do budget orçado).
F2	Eficiência na gestão da segurança								M		
(i)		Taxa de gastos anuais em proporção ao budget orçado	25,0%	=	100%	115%	85%	21,3%	M	B >= 95%; R < 80%	Proporção de gastos em relação ao orçado. Valor próximo de 100% é o ideal.
F3	Execução de projetos de acordo com planejado								B		
(ii)		Taxa média de alocação de recursos em projetos (horas por semana)	12,5%	=	38	40	95%	11,8%	B	B >= 85%; R < 65%	Tempo de recursos da equipe de segurança da informação alocados para projetos (horas/semana).
F4	Gerenciamento de fornecedores de forma eficiente								M		
(i)		Porcentagem de fornecedores com nota de avaliação superior a 8	12,5%	>=	90%	94%	100%	12,5%	B	B = 100%; R < 90%	Avaliação realizada semestralmente pelos gestores de fornecedores.
(ii)		Porcentagem de Contratos com requisitos de Segurança da Informação	12,5%	=	100%	92%	92%	11,5%	M	B = 100%; R < 90%	Revisão anual dos contratos junto ao jurídico pela área de segurança da informação.
									Indicador da perspectiva		
		Peso Financeiro	100,0%		Meta	90%	Resultado	81,2%	M		

Fonte: Adaptado de Gartner (2010).

Tabela 14 – Perspectiva de cliente do BSC de Segurança da Informação

Perspectiva de Cliente											
Ref.	Objetivo	Medida de Desempenho	Peso	Objetivo		Valor	Desempenho Relativo	Desempenho Absoluto	Tolerância	Regra de Tolerância	Observações
			(constante	(constante)		(variável)	(calculado)	(calculado)	Baseado no desempenho relativo		
C1	**Provimento de disponibilidade e continuidade de nossos serviços**								B		
(i)		Falhas em sistemas externos sem notificação	12,5%	=	0	0	100%	12,5%	B	B = 100%; R = 0%	Número de minutos no último mês que os clientes não puderam acessar nossos serviços sem que tivéssemos sido alertados.
(ii)		Porcentagem de mudanças planejadas e pré-aprovadas	12,5%	<=	30	10	100%	12,5%	B	B = 100%; R = 0%	Relação de mudanças abertas no ambiente de forma planejada em relação ao total.
C2	**Clientes com confiança em nossos serviços e instalações**								B		
(i)		Testes de Segurança conforme agendamentos	12,5%	>=	95%	96%	100%	12,5%	B	B = 100%; R <= 90%	Execução dos testes de segurança no ambiente no último mês conforme calendário definido.
(ii)		Todos os pontos de auditorias externas estão no prazo	12,5%	>=	90%	90%	100%	12,5%	B	B = 100%; R <= 95%	Status dos planos de correção para tratamento dos pontos de auditoria
C3	**Cumprimento das regulamentações aplicáveis**								M		
(i)		Status de conformidade com ISO 27001	8,3%	=	100%	97%	97%	8,1%	M	B = 100%; R <= 85%	Status dos planos de correção relacionados a auditoria externa da ISO 27001.
(ii)		Status de conformidade com políticas e normas internas	8,3%	=	100%	97%	97%	8,1%	M	B = 100%; R <= 85%	Status dos planos de ação corretiva ou melhoria oriundos da auditoria interna da ISO 27001.
(iii)		Status de conformidade com PCI-DSS	8,3%	=	100%	98%	98%	8,2%	B	B >= 80%; R < 50%	Status dos planos de correção relacionados a auditoria externa do PCI DSS
C4	**Acessos adequados às pessoas e funções - não mais, não menos**								M		
(i)		Usuários com acesso recertificado no último período	12,5%	>=	98%	95%	97%	12,1%	M	B = 100%; R <= 90%	Proporção dos usuários com acessos revalidados pelos seus gestores no último trimestre.
(ii)		Incidentes de vazamento de dados de clientes	12,5%	=	0	0	100%	12,5%	B	B = 100%; R < 99%	Incidentes relacionados a dados de clientes no último mês.

				Indicador da perspectiva	
Peso de Cliente	**100,0%**	**Meta**	**90,0%**	**Resultado**	**99,0%**	B

Fonte: Adaptado de Gartner (2010).

Tabela 15 – Perspectiva Operacional do BSC de Segurança da Informação

Perspectiva Operacional											
Ref.	Objetivo	Medida de Desempenho	Peso		Objetivo	Valor	Desempenho Relativo	Desempenho Absoluto	Tolerância	Regra de Tolerância	Observações
			(constante)		(constante)	(variável)	(calculado)	(calculado)	Baseado no desempenho relativo		
O1	**Ferramentas adequadas às nossas necessidades**								B		
(i)		Porcentagem do monitoramento de capacidade	12,5%	>	97,5%	99%	100%	12,5%	B	B > 90%; R < 80%	Porcentagem de servidores sob monitoramento de capacidade
O2	**Mudanças no ambiente de forma eficiente e confiável**								B		
(i)		Porcentagem de Mudanças Imediatas	12,5%	=	10%	0%	100%	12,5%	B	B = 100%; R = 0%	Porcentagem de mudanças imediatas (sem planejamento) em relação ao total de mudanças abertas no último mês.
O3	**Melhoria contínua em nossos processos**								M		
(i)		Porcentagem de Incidentes que geraram Ações Corretivas	8,3%	=	100%	83%	83%	6,9%	M	B = 100%; R <= 80%	Incidentes abertos no último mês que originaram uma ação corretiva ou de melhoria.
(ii)		Recorrência de incidentes após Ações Corretivas	8,3%	=	0	0	100%	8,3%	B	B = 100%; R = 0%	Incidentes recorrentes nos últimos 6 meses.
(iii)		Porcentagem de Ações Corretivas dentro do prazo	8,3%	=	100%	95%	95%	7,9%	M	B = 100%; R <= 80%	Status das Ações Corretivas em aberto.
O4	**Manutenção de nosso risco operacional dentro do apetite definido**								M		
(i)		Tempo médio de correção para vulnerabilidades de risco alto	25,0%	<=	60	80	33%	8,3%	M	B = 100%; R = 0%	Tempo até a correção de vulnerabilidades de risco alto a partir de sua identificação.
(ii)		Porcentagem de Planos de tratamento de riscos dentro do prazo	25,0%	=	99%	85%	86%	21,5%	M	B = 100%; R < 80%	Status das correções de riscos de segurança da informação em aberto.
									Indicador da perspectiva		
		Peso Operacional	**100,0%**		**Meta**	**90%**	**Resultado**	**78,0%**	M		

Fonte: Adaptado de Gartner (2010).

Tabela 16 – Perspectiva de aprendizado e crescimento do BSC de Segurança da Informação

Perspectiva de Aprendizado e Crescimento											
Ref.	Objetivo	Medida de Desempenho	Peso (constante)	Objetivo (constante)		Valor (variável)	Desempenho Relativo (calculado)	Desempenho Absoluto (calculado)	Tolerância	Regra de Tolerância (Baseado no desempenho relativo)	Observações
AC1	Pessoas engajadas								B		
(i)		Média de nota curso EAD segurança	8,3%	>=	4,80	4,82	100%	8,3%	B	B = 100%; R <= 90%	Média do teste pós curso de conscientização realizado por todos os colaboradores anualmente.
(ii)		Turnover das áreas que compõem o SGSI	8,3%	<=	5%	3,8%	100%	8,3%	B	B = 100%; R = 0%	Porcentagem de saída de funcionários.
(iii)		Nível de satisfação da equipe - pesquisa de clima	8,3%	>=	95%	96%	100%	8,3%	B	B = 100%; R < 90%	Resultado da pesquisa de clima realizada anualmente.
AC2	Pessoas preparadas								B		
(i)		Índice de treinamento em Segurança da Informação	12,5%	>=	95%	96%	100%	12,5%	B	B = 100%; R < 90%	Porcentagem de colaboradores que realizaram treinamento em SI nos últimos 2 anos.
(ii)		Equipe de Segurança com Qualificação adequada (cursos x descrição de cargo)	12,5%	=	100%	100%	100%	12,5%	B	B = 100%; R < 90%	Relação entre qualificação e as necessidades para cada função.
AC3	Investimento em pessoas e desenvolvimento de suas especialidades								R		
(i)		Porcentagem de áreas com *job rotation*	12,5%	>	75%	15,0%	20%	2,5%	R	B > 90%; R <= 75%	Compartilhamento de conhecimento entre colaboradores dentro das áreas.
(ii)		Plano de desenvolvimento individual definidos e em dia	12,5%	>=	95%	81%	85%	10,7%	M	B = 100%; R < 85%	Status dos Planos de Desenvolvimento Individual
AC4	Proteção de nosso conhecimento como vantagem competitiva								R		
(i)		Porcentagem de áreas mapeadas pelo sistema de prevenção de vazamento de dados	8,3%	=	100%	45%	55%	4,6%	R	B = 100%; R < 75%	Áreas com suas informações já mapeadas pelo sistema de prevenção a vazamento de dados.
(ii)		Dados organizacionais sensíveis mapeados pelo sistema de prevenção de vazamento de dados	8,3%	=	100%	94%	94%	7,8%	M	B = 100%; R < 90%	Dados com regras para proteção contra vazamento já aplicadas em produção.
(iii)		Incidentes envolvendo dados internos (excluí-se dados de clientes)	8,3%	=	0%	9%	91%	7,6%	R	B = 100%; R < 95%	Porcentagem de incidentes no último mês relacionados a vazamento de dados de clientes.
									Indicador da perspectiva		
		Peso de A&C	100,0%			Meta	90%	Resultado 83,2%	M		

Fonte: Adaptado de Gartner (2010).

5.4 Melhoria Contínua

Como forma de acompanhamento das ações, objetivos e metas, o BSC do SGSI será populado e atualizado mensalmente pelos responsáveis pelos processos relacionados a cada medida de desempenho. Esses resultados serão apresentados nas reuniões mensais do Comitê de Segurança da Informação e, havendo necessidade, ou seja, caso os objetivos das medidas de desempenho e/ou as metas das perspectivas não estejam sendo atingidas, ações serão reformuladas ou replanejadas. O Comitê também terá a responsabilidade de inserir novas medidas de desempenho ou objetivos, bem como alteração das metas, conforme resultados forem obtidos e uma análise crítica pelo menos anual de todo o BSC. Um relatório executivo será gerado sumarizando os resultados do SGSI por perspectiva do BSC e submetido ao Conselho Executivo da organização, deixando claro o atendimento e suporte aos objetivos estratégicos da organização por meio dos processos do SGSI. Tais resultados também serão divulgados internamente na organização por meio de boletins trimestrais.

5.5 Análise crítica

Embora a organização já possuísse um SGSI estabelecido e um dos requisitos da ISO/IEC 27001 trate de monitoramento, medição, análise e avaliação, tais aspectos não eram diretamente relacionados aos objetivos de negócio, tornando o acompanhamento de desempenho por vezes pontual e executado apenas pela equipe responsável pelo SGSI. Ou seja, não havia engajamento das outras áreas pela aparência de que a responsabilidade pelo bom desempenho da segurança das informações da companhia era exclusivamente da equipe de SI.

A busca por maior alinhamento do SGSI com as áreas de negócio e a Alta Direção deu o apoio necessário para que a disseminação de responsabilidades e o engajamento das outras áreas se fizessem presentes. Esse foi um ganho logo percebido ao início do processo.

Notou-se que os objetivos definidos para o SGSI, embora estivessem contemplando as atividades de segurança das informações, não refletiam a busca da organização pelos objetivos estratégicos. A coordenação do SGSI se mostrou

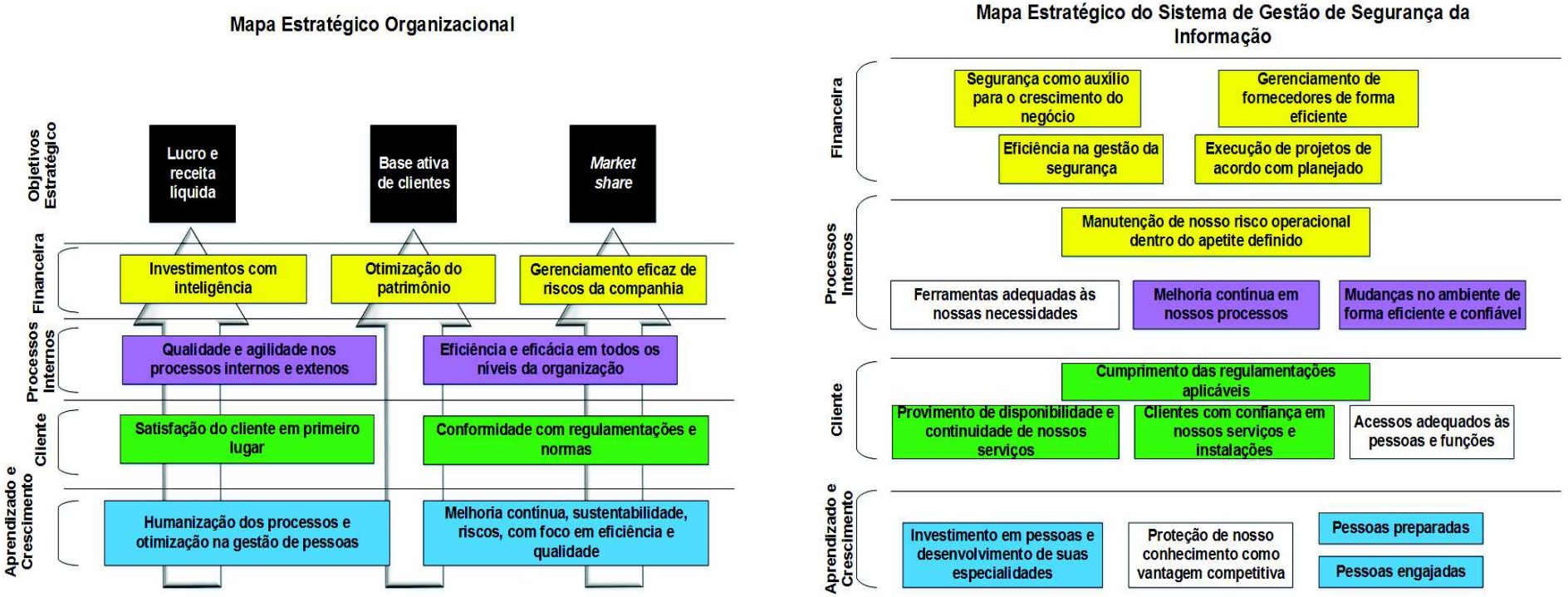
solícita nessa adequação e percebeu, nas perspectivas do BSC já utilizadas pela companhia, um ótimo meio de organizar os objetivos do SGSI.

Conforme as reuniões para definição de medidas de desempenho foram ocorrendo, ficou claro entre as demais áreas da companhia suas responsabilidades dentro do SGSI. Uma percepção geral foi de que processos não precisariam ser criados para estar de acordo com o SGSI, apenas algumas adequações pontuais seriam necessárias. Contudo, o levantamento de informações para medição gerou alguns conflitos. Uma vez que alguns indicadores não eram medidos ou sequer existiam viu-se que, com essa mudança, processos demonstrariam estar com desempenho abaixo do esperado. O que inicialmente causou resistência em algumas áreas. Graças ao engajamento e apoio da Alta Direção esses impasses foram superados.

Com os resultados atuais coletados, notou-se necessidade de melhoria imediata em alguns processos, como metodologia de projetos, conscientização dos colaboradores e classificação e proteção das informações contra vazamento. No primeiro momento, como tal levantamento foi realizado durante o ano vigente, não foi possível a realocação de recursos para aquisição de tecnologias ou consultorias. Dessa forma, uma revisão processual foi planejada. A partir do acompanhamento do desempenho desses indicadores, espera-se investimento mais assertivo para o próximo ano e o reflexo dessas melhorias no BSC do SGSI.

Ficou definido em política que a revisão dos objetivos e indicadores será anual, a partir da análise crítica realizada pela Alta Direção e representantes de todas as áreas do SGSI.

Figura 7 - Correlação entre os diferentes níveis dos mapas estratégicos



Fonte: Elaborado pelo autor.

6 CONCLUSÃO

Mesmo com frequência assustadora de casos de quebra de segurança da informação para diversas empresas em diferentes setores causando prejuízos não só às organizações, mas também a seus clientes e usuários, segue sendo um desafio para os gestores e equipes de segurança da informação justificarem investimentos. Seja em tecnologias cada vez mais específicas e igualmente caras ou melhorias de processos como um todo. Identificou-se, portanto, uma vertente relevante para aprofundamento de pesquisa: como prover alinhamento entre os objetivos da gestão de segurança da informação e os objetivos de negócio da organização? A criação de indicadores alinhados ao mapa estratégico da organização se mostrou uma abordagem precisa para essa questão.

Por meio da aproximação da segurança da informação e as áreas de negócio da organização, juntamente com o fundamental apoio da Alta Direção, foi possível alcançar o engajamento necessário para a criação do BSC do SGSI da companhia, que atingiu o resultado esperado: relacionar os processos e objetivos do SGSI com os objetivos de negócio da organização.

Para a criação do *balance scorecard* para o SGSI foram coletados dados gerais sobre a organização e informações sobre os objetivos estratégicos, bem como dados já existentes sobre o mapa estratégico em uso. Como forma de prover o alinhamento mais estreito entre os processos do SGSI e os objetivos de negócio, os objetivos do SGSI foram reorganizados nas perspectivas do BSC e medidas de desempenho para acompanhamento e conjunto com os gestores e responsáveis das áreas envolvidas. Por fim, metas para cada medida de desempenho e resultado geral das perspectivas foram definidas de acordo com os dados obtidos nos últimos períodos.

Diversos obstáculos foram enfrentados ao longo do processo. Falta de informação ou informações sem definições a respeito de responsabilidades para gerá-las; burocracia e excesso de aprovações necessárias para coletar dados; ausência de agenda para entrevistas e má interpretação dos objetivos; resistência na coleta de dados que poderiam gerar indicadores negativos às áreas. Foram necessárias redefinições e esclarecimentos mais detalhados sobre as necessidades e um apoio próximo por parte da Alta Direção para superá-los.

Contudo, por meio de conscientização das demais áreas sobre a importância dessas definições para indicação de entrega de valor dos processos ao negócio, foram elaborados objetivos e indicadores que melhor refletem os atuais processos e sua participação nos objetivos estratégicos da companhia.

Como limitações do projeto podemos sinalizar que, embora o escopo do SGSI da organização seja abrangente em relação aos principais processos de negócio, não engloba todas as áreas da empresa, ficando em aberto essa melhoria. Além disso, não foi escopo do projeto a crítica em relação aos objetivos estratégicos já definidos pela organização, bem como seu mapeamento em uso.

Uma vez que se tenha um acompanhamento constante dos resultados obtidos pelos processos de segurança da informação na organização em relação aos seus objetivos e estes estejam relacionados direta ou indiretamente aos objetivos de negócio da organização, faz-se possível e mais simples indicar quais são os pontos fortes e fracos SGSI, bem como a justificativa para investimentos nos pontos os quais não estejam alcançando as metas definidas. Por se tratar de um estudo de caso pontual, no entregável do projeto não consta o acompanhamento ao longo de um período extenso. Porém, o arcabouço necessário para que os investimentos sejam justificáveis está definido e alinhado entre todas as áreas envolvidas e o negócio da organização para com o mercado e seus acionistas.

Adicionalmente como resultado do projeto, pode-se destacar a importância da conscientização sobre o funcionamento e escopo de processos do SGSI para com as demais áreas da organização. Sem isso, não há engajamento, tampouco a visão da Alta Direção sobre a importância que, de fato, há na gestão de segurança da informação e sua entrega de valor para a companhia. Não havendo o alinhamento entre os processos de um SGSI e os objetivos estratégicos, a segurança da informação acaba como responsável por processos os quais não executa, sem ter apoio efetivo das áreas em questão. Pode-se afirmar, portanto, que a melhoria contínua de um sistema de gestão de segurança da informação está diretamente relacionada a como tal sistema é visto em relação a sua entrega de valor ao negócio, o que reflete diretamente no engajamento de toda a companhia.

Por fim, espera-se que com o seguimento do processo estabelecido, as decisões futuras para os processos envolvidos no SGSI sejam, de fato, baseadas nos indicadores em uso. O que proporcionará investimentos mais precisos e mais relevantes ao negócio da organização. Por se tratar de um sistema de gestão

baseado em norma, espera-se que mais empresas adotem os passos aqui apresentados para adequação e alinhamento estratégico de seus processos de segurança da informação.

REFERÊNCIAS

ALVES, G.; CARMO, L. e ALMEIDA, C. (2006). Enterprise Security Governance - A practical guide to implement and control Information Security Governance (ISG). Em: **Business-Driven IT Management**, pages 71-80. IEEE.

ANDERSEN, Elaine; AZIZA, Bruno; FITTS, Joey; HOBERECHT, Steve e KASHANI, Tim. **Microsoft Office PerformancePoint Server 2007**. Wiley Publishing, Indianapolis, EUA, 2008.

BASSETTE, Fernanda. **Estado de São Paulo cria prontuário digital para o SUS**. 2012. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/estado-de-sao-paulo-cria-prontuario-digital-para-o-sus>. Acessado em: 9 ago. 2015.

BKF. **Cartão de crédito: como funciona o mercado?** 2013. Disponível em: <https://www.bankfacil.com.br/blog/artigos/cartoes/cartao-de-credito-como-funciona-o-mercado>. Acessado em: 20 fev. 2016.

BRENNER, Joel. **ISO 27001: Risk management and compliance**. Risk management, v. 54, n. 1, p. 24, 2007.

CAMP, Jean; e WOLFRAM, Catherine. **Pricing Security: Vulnerabilities as Externalities**. Em: The Economics of Information Security. v. 12. Kluwer Academic Publishers, EUA. 2004.

CONDE, Diogo Matheus Rubio. - A relação entre *business intelligence* e o processo de inovação no mercado de cartões de crédito brasileiro: um estudo de caso. 2011. FGV. São Paulo.

DAVIS, R. (1978). **The Data Encryption Standard in Perspective**. In: *Communications Society Magazine*, pages 5-9. IEEE.

DE OLIVEIRA, Thiago Castro. **Uma proposta de ontologia para área de segurança da informação em instituições de saúde**, 2014. Artigo (Graduação em Segurança da Informação) – Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2014.

DRESCH, Aline; LACERDA, Daniel Pacheco; e JÚNIOR, José Antonio Valle Antunes. **Design Science Research**: Método de Pesquisa Para Avanço da Ciência e Tecnologia. Porto Alegre, Bookman. 1 ed. 2015.

GARTNER. **IT Governance (ITG).** Disponível em: <http://www.gartner.com/it-glossary/it-governance>. Acessado em: 8 mar. 2016.

GARTNER. **Toolkit: Developing a Balanced Scorecard for Security**. Maio de 2014. Disponível em: <https://www.gartner.com/doc/2740419/toolkit-developing-balanced-scorecard-security>. Acesso em: 15 dez. 2015.

GELLMAN, Barton; e POITRAS, Laura. **U.S.; British intelligence mining data from nine U.S. Internet companies in broad secret program**. 2016. Disponível em: <http://www.washingtonpost.com/www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. Acessado em: 8 ago. 2015.

GOLDMAN, James; e AHUJA, Suchit. **Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework**. **ICT Ethics and Security in the 21st Century: New Developments and Applications**, p. 277-309, 2011.

HARRIS, Shon. **CISSP All-in-One Exam Guide**, McGraw Hill Professional, 5 ed. 2010.

HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. **Balanced scorecard implementation of security strategies: a framework for IT security performance management**. Em: Information Systems Management, v. 27, n. 1, p. 72-81, 2010.

HERZOG, Ana Luiza. Pensar, planejar e fazer. Como o Unibanco está disseminando entre seus 28000 funcionários o balanced scorecard, sistema que promete tirar a estratégia da gaveta. **Exame Fórum**. Editora Abril. Edição 787. Ano 37. n.5. 12 de março de 2003.

HUANG, Shi-Ming; LEE, Chia-Ling; KAO, Ai-Chin. **Balancing performance measures for information security management: A balanced scorecard framework**. Industrial Management & Data Systems, v. 106, n. 2, p. 242-255, 2006.

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION (ISACA). **An Introduction to the Business Model for Information Security.** EUA, 2009

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION (ISACA). **From Here to Maturity Management - The Information Security Life Cycle.** *ISACA Journal,* v. 6, 2014

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27000:2014**: Information technology - Security techniques - Information security management systems - Overview and vocabulary, Suíça, 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27001:2013**: Information technology - Security techniques - Information security management systems – Requirements, Suíça, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27002:2013**: Information technology - Security techniques - Code of practice for information security management, Suíça, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2011**: Information technology - Security techniques - Information security risk management, Suíça, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 38500:2015** Information technology - Governance of IT for the organization", Suíça, 2015.

IT GOVERNANCE INSTITUTE (ITGI). **Resource Center**. 2013. Disponível em: <http://www.itgi.org/Resource-Center.html>. Acessado em: 22 out. 2015.

IT GOVERNANCE INSTITUTE (ITGI). **Information Security Governance: Guidance for Boards of Directors and Executive Management**. 2 ed. EUA

JAQUITH, Andy. **Security metrics**. 1. Ed. Pearson Education, 2007.

KAPLAN, Robert e NORTON, David. **A Estratégia em Ação. Balanced Scorecard**. Rio de Janeiro; Campus, 1997.

KAPUR, Rajesh. **Use of the Balanced Scorecard for IT Risk Management**. In: ISACA Journal, pages 1-5. v.5. 2010. ISACA.

KONG, Hee-Kyung; KIM, Tae-Sung; KIM, Jungduk. **An analysis on effects of information security investments: a BSC perspective**. Em: Journal of Intelligent Manufacturing, v. 23, n. 4, p. 941-953, 2012.

KPMG. **Information Security Survey 2000**. 2000. Disponível em: <http://www.kpmg.co.uk/services/audit/pubs/>. Acessado em: 8 dez 2015.

KREBS, Brian. **Data Theft Common By Departing Employees**. 2009. Disponível em: <http://articles.washingtonpost.com/2009-02-26/news/36791861_1_data-theft-employer-job>. Acessado em: 22 out. 2015.

KRONMEYER, Oscar Rudy. **Pilotagem de Empresas - Uma nova abordagem no desdobramento, implementação e monitoramento da estratégia**. Brasil. 2006. Tese (Pós-graduação em Engenharia de Produção) - Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal do Rio Grande do Sul UFRGS. Porto Alegre, 2006.

LUDLOW, Peter. **WikiLeaks and Hacktivist Culture**. 2010. Disponível em: <http://www.arifyildirim.com/ilt510/peter.ludlow.pdf>. Acessado em: 20 fev. 2016.

MARCELINO, Carmen Lúcia Nunes. **Segurança de Informação na Estratégia Empresarial - BSC**: Estudo de caso. Setúbal, 2014. 73 f. Dissertação (Mestrado em Sistemas de Informação Organizacionais) - Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Setúbal, 2014.

MASTERCARD. **Site Data Protection and PCI**. 2016. Disponível em: <https://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html>. Acessado em: 20 fev. 2016.

NATIONAL COMPUTING CENTRE. **IT Governance - Developing a Successful Governance Strategy.** Oxford House, Manchester, Inglaterra, 2005.

OLIVEIRA, Rodrigo Eduardo de Mello. **O mercado de cartões de crédito: taxa de intercâmbio e interoperabilidade no mercado brasileiro**. 2014. Dissertação (Mestrado em Economia do Setor Público) - Universidade de Brasília, Brasília, 2014.

PCI-SSC. **Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures**. 2015. Disponível em: <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf>. Acessado em 20 fev. 2016.

PRIETO, Vanderli; PEREIRA, Fábio; CARVALHO, Marly e LAURINDO, Fernando. **Fatores críticos na implementação do Balanced Scorecard**. Em: Gestão & Produção. v. 13, n. 1., p. 81-92, jan-abr 2006.

RAMOS, Anderson. **Guia Oficial para Formação de Gestores em Segurança da Informação**. 2 ed. Zouk, 2008.

REZENDE, Denis Alcides. e ABREU, Aline França de. (2009), **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**, Atlas, 6 ed. 2003

SANGKYUN, Kim. KO, Franz. **BSC-based Evaluation on Security Risks of IT Infrastructure**. Journal of Convergence Information Technology, v. 7, n. 15, 2012.

SANTO, Adrielle. **Segurança da Informação. Instituto Cuiabano de Educação.** 2011. Disponível em: <http://www.ice.edu.br/TNX/storage/webdisco/2011/03/11/outros/2bc3b892c73868cf712dcf084ed96b8a.pdf>. Acessado em: 10 out. 2015.

SILVA, Rozelito Felix da. **Proposta de adaptação do modelo Balanced Scorecard: BSC para a gestão de segurança da informação em órgãos da administração pública**. 2010. 82 f. Dissertação (Mestrado em Engenharia Elétrica), Universidade de Brasília, Brasília, 2010.

SUER, Myles. **COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement**. COBIT Focus, v.1, p.5, 2013

SYMONS, Craig. **IT governance framework- structures, processes, and communication.** Forrester Research, EUA, 2005.

UNIVERSITIES AND COLLEGES INFORMATION SUSTEMS ASSOCIATION (UCISA). **UCISA Information Security Toolkit**. Disponível em: <http://www.ucisa.ac.uk/istoolkit>. Acessado em: 3 mar. 2016.

VAN GREMBERGEN, Wim. **The balanced scorecard and IT governance**. IRMA Conference**,** p. 1123-1124, 2000.

VAN GREMBERGEN, Wim; DE HAES, Steven. **Measuring and improving IT governance through the balanced scorecard**. Em: Information Systems Control Journal, v. 2, n. 1, p. 35-42, 2005.

VAN GREMBERGEN, Wim; SAULL, Ronald; DE HAES, Steven. **Linking the IT balanced scorecard to the business objectives at a major Canadian financial group**. Em: Journal of Information Technology Case and Application Research, v. 5, n. 1, p. 23-50, 2003.

VOLCHKOV, Andrej. **How to Measure Security From a Governance Perspective**. Information Systems Control Journal, v. 5, p. 44-351, 2013.

VON SOLMS, Russouw; THOMSOM, Kerry-Lynn; e MANINJWA, Mvikeli. **Information Security Governance control through comprehensive policy architectures**. Em: Information Security for South Africa. IEEE. 17 ago. 2011, Johannesburg