ANÁLISE ESTRATÉGICA APLICADA A GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

STRATEGIC ANALYSIS APPLIED TO INFORMATION SECURITY GOVERNANCE

RODRIGO DE PAULA
Especialista em Gestão e Segurança em Redes de Computadores, Universidade Estadual de Goiás (UEG), Campus de Trindade
rodrigogyn@gmail.com

PAULO CÉSAR RODRIGUES DE ALMEIDA
Mestre em Ciência da Computação e docente da Universidade Estadual de Goiás (UEG) – Campus de Trindade e Universidade Salgado de Oliveira – Campus de Goiânia
paceroal@hotmail.com

Resumo: Este artigo visa à conscientização da importância de desenvolver uma visão integrada do modelo de governança nas organizações, em que a governança de segurança da informação seja parte. E mostrar que essa integração tem o objetivo de agregar valor para o corpo diretivo e as partes interessadas tornando um diferencial competitivo para as organizações, ou seja, uma visão estratégica. Os resultados apontam para que haja uma governança corporativa eficaz, a segurança da informação deve fazer parte da tomada de decisão das organizações e o corpo diretivo deve acompanhar os incidentes expressivos no ambiente organizacional.
Palavras-chave: Segurança da informação. Governança de segurança da informação. Visãoestratégica.

Abstract: This article aims to raise awareness of the importance of developing an integrated view of the governance model in organizations, where information security governance is a part. And show that this integration has the objective of adding value to the management body and the stakeholders making a competitive differential for the organizations, that is, a strategic vision. The results indicate that there is an effective corporate governance, information security should be part of the decision making of organizations and the governing body must follow the significant incidents in the organizational environment.
Keywords: Information security. Information security governance.Strategicvision.

INTRODUÇÃO

Quando discutimos governança corporativa, falamos de um conjunto de práticas que auxiliam na construção de um ambiente de confiança e transparência, necessárias para sustentar a solidez financeira e a integridade do negócio. Uns dos principais indicadores que posicionam o valor da organização é a capacidade desta organização em proteger sua informação e a qualidade destas informações.

Atualmente, devido aos ambientes cada vez mais conectados e dependentes da informação e velocidade de processamento, surgem mais ameaças e riscos para os negócios das organizações.

Para manter os bons resultados, é essencial o alinhamento das práticas de governança corporativa com os ativos de tecnologias da informação.Devido à pressão constante das organizações para alcançar resultados, a segurança da informação tornou-se uma questão-chave. As falhas nas medidas de segurança da informação de uma organização podem ter um impacto direto na sua credibilidade e imagem pública. Para evitar tais problemas, a governança da segurança da informação deve ser um mecanismo de controle que garanta ações de gerenciamento voltadas aos objetivos estratégicos das organizações.

Este artigo objetiva a conscientização da importância de se incluir a governança de segurança da informação como estratégia nas organizações. Assim como, apresentar uma orientação sobre os conceitos e princípios para a governança de segurança da informação, para que as organizações possam gerir as atividades relacionadas com a segurança da informação.

A abordagem metodológica envolveu primeiramente uma revisão da norma NBR ISO/IEC 27014:2013, e de livros e trabalhos sobre o tema proposto. A seguir, foram revisados os princípios de governança corporativa e uma analogia entre os objetivos de alguns modelos de governança.

ADMINISTRAÇÃO DA EMPRESA

Pode-se considerar a administração como o esforço que possibilita atingir objetivos pré-estabelecidos. Seus princípios gerais são compostos pelas funções administrativas (PODC): Planejamento, Organização, Direção e Controle. Junior (2012, p.1) define administração “como o ato ou processo de gerir, reger ou governar negócios públicos ou particulares”.

É no campo da administração que é definido o planejamento estratégico da empresa, que é o “processo gerencial que possibilita restabelecer o rumo a ser seguido pela empresa com vistas a obter um nível de otimização da empresa em relação a seu ambiente” (PEREIRA, 2004, p.6).O planejamento estratégico define quais são os objetivos, metas, projetos, orçamentos e planos de ações.

Os stakeholders[1] são um elemento indispensável para o planejamento estratégico dos negócios.

[1]Stakeholders, em português: parte interessada é um termo usado na administração que se refere a qualquer pessoa ou entidade que afeta ou é afetada pelas atividades da empresa.

VISÃO ESTRATÉGICA DA EMPRESA

O termo estratégia deve ser observável sob diferentes aspectos, pois possui várias abordagens e diversas aplicações. Porter (1986 apud OLIVEIRA JUNIOR, 2008, p.19) define a estratégia como “o desempenho de atividades de forma diferente dos concorrentes”; enquanto Hamel e Prahalad (1995 apud OLIVEIRA JUNIOR, 2008, p.19) destacam que estratégia “deve se concentrar na definição das competências indispensáveis da empresa”. Esses autores, de uma forma geral, concordam que definir a estratégia de forma correta é o primeiro passo para conseguir o sucesso, depois é preciso executar o que foi planejado de forma correta, acompanhar os resultados e alterar a estratégia se for necessário.

A visão estratégica de uma empresa consiste em um conjunto de componentes que definem o que a empresa deseja ser no futuro e como atingir os objetivos através de sua cultura. Os conceitos estratégicos de uma empresa são formados pela visão, missão, valores e fatores críticos de sucesso.

A competitividade das empresas está relacionada ao valor que o corpo diretivo e a gerência executiva dão à criação das estratégias do negócio. A NBR ISO/IEC 27014 (2013, p.1) define corpo diretivo como “a pessoa ou grupo de pessoas que são responsáveis pelo desempenho e conformidade da organização”. E gerência executiva é “a pessoa ou grupo de pessoas que possuem responsabilidades delegadas pelo corpo diretivo na implementação de estratégias e políticas para alcançar o propósito da organização” (NBR ISO/IEC 27014, 2013, p.1). A visão estratégica alinha as decisões e ações organizacionais para alcançar os objetivos do negócio num panorama realista. Gerencia executiva que dá bons resultados é aquela que tem ampla visão conceitual dos negócios e alia essa característica com a capacidade de pensar estrategicamente.Nenhuma modificação importante no universo dos negócios e na estratégia das organizações pode ser implementada sem a pressuposição teórica que a sustente.

Portanto, as melhores gerências executivas de negócios e estratégias de mercado são aquelas que têm um cuidado especial no seu desenvolvimento pessoal e de seus colaboradores, e no pensamento estratégico, para analisar e interpretar informações que reflita em decisões mais eficientes.

GOVERNANÇA ORGANIZACIONAL

Segundo Manoel (2014, p.25), governança é "o conjunto de processos, tecnologia, pessoas, políticas, leis, regulamentos e agências que afetam a maneira como uma organização é dirigida, administrada ou controlada".

Existem outros modelos de governança em uma organização, como a governança corporativa da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a governança da tecnologia da informação (ISO 38500:2008). Cada um desses modelos é uma parte que completa a governança de uma organização e destaca o valor do alinhamento com os objetivos dos negócios.

A Figura 1 exemplifica a relação entre governança de segurança da informação e governança de tecnologia da informação.

Figura 1: Relação entre governanças
Fonte: Adaptada da NBR ISO/IEC 27014 (2013, p.3).

É possível e recomendável a integração das governanças de segurança da informação e tecnologia da informação com o intuito de aperfeiçoar recursos, partilhar esforços e tornar a comunicação mais fácil.

Outra razão para motivar essa integração é o fato que as medidas de segurança que protegem as informações e os serviços de TI utilizam recursos de tecnologia da informação; por exemplo; criptografia, redes virtuais privadas, backup, firewall, sistema de detecção de intrusão, etc.

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

A NBR ISO/IEC 27014 (2013, p1) descreve governança de segurança da informação (GSI) como “um sistema pelo qual as atividades de segurança da informação de uma organização são dirigidas e controladas”. Além do mais, a governança de segurança da informação promove um forte vinculo entre o corpo diretivo de uma organização, a gerência executiva e os responsáveis pela implementação e operação de um sistema de gestão de segurança da informação.

Ela proporciona uma regra indispensável para orientar as propostas de segurança da informação por toda a organização. O escopo da Governança de Segurança da Informação compreende a confidencialidade, integridade e disponibilidade da informação. Mas requer também o processo interno de divulgação, de comunicar os resultados para todos os stakeholders.

O corpo diretivo é o responsável pelas tomadas de decisões e pelo desempenho da organização e seu foco principal em relação à segurança da informação é garantir que o acompanhamento das atividades relacionadas com a segurança da informação seja eficiente e alinhado com os objetivos e estratégias de negócios. Conforme a NBR ISO/IEC 27014 (2013, p2) os objetivos da GSI são**:**

- Alinharos objetivos e a estratégia da Segurança da Informação com os objetivos e estratégia do negócio da organização (alinhamento estratégico).
- Agregarvalor para a alta direção e para as partes interessadas (entrega de valor).
- Garantir que os riscos da informação estão sendo adequadamente endereçados para as pessoas responsáveis (responsabilidade).

PRINCÍPIOS E PROCESSOS

A seguir serão apresentados os princípios e processos de acordo com a Norma NBR ISO/IEC 27014. “A governança de segurança da informação é formada pela junção dos princípios e processos” (NBR ISO/IEC 27014, 2013, p.3).

Princípios

Princípios de governança de segurança da informação são regras aceitas para a ação ou conduta de governança que atuam como um guia para a implementação de GSI. A descrição de cada princípio é um referencial ao que convém a ser realizado, mas não indica com precisão como, quando, nem por quem os princípios seriam implementados, pois estas

características são subordinadas á natureza da organização que vai levar a prática os princípios.

Para atingir o objetivo da GSI em alinhar com rigor a segurança da informação com os objetivos do negócio e entregar valor aos stakeholders, estabelece seis princípios.

- Princípio 1: Estabelecer a segurança da informação em toda a empresa. A GSI deve garantir que as atividades de segurança da informação devem ser entendidas, integradas e levadas em consideração nas tomadas de decisões do negócio.

- Princípio 2: Adotar uma abordagem baseada em riscos.

A GSI deve ser fundamentada em decisões nos riscos. Deve ser adotada uma gestão de riscos da informação que seja apropriada para a organização e seja integrada à gestão de riscos da organização. Os recursos para a implementação da gestão de riscos da informação devem ser alocados pelo corpo diretivo.

- Princípio 3: Estabelecer a direção de decisões de investimento.

Deve estabelecer uma estratégia de investimento em segurança da informação baseado nos resultados nos negócios. O corpo diretivo deve assegurar a integração com os processos de investimentos e despesas da organização.

- Princípio 4: Assegurar conformidade com os requisitos internos e externos. A GSI deve garantir que as políticas e as práticas de segurança da informação respeitem a legislação, regulamentos, contratos e outros requisitos externos ou internos. O corpo diretivo deve certificar que as atividades de segurança da informação estejam em conformidade e estejam sendo executadas conforme os requisitos internos e externos.

- Princípio 5: Promover um ambiente positivo de segurança.

Para instituir uma cultura positiva de segurança da informação, o corpo diretivo deve exigir promover e apoiar a coordenação das atividades dos stakeholders para atingir um direcionamento coerente para a segurança da informação. Isto ajudará na implantação de programas de educação, treinamento e conscientização em segurança.

- Princípio 6: Analisar criticamente o desempenho em relação aos resultados de negócios.

A GSI deve garantir que a abordagem utilizada para proteger as informações esteja adequada ao seu objetivo de apoio à organização. Para analisar o desempenho de segurança da informação, a partir de um panorama da governança, o corpo diretivo deve avaliar o desempenho da segurança da informação em relação ao seu impacto no negócio.

Processos

O processo descreve uma série de rotinas que torna viável a SGI e suas relações mútuas, e relata o relacionamento entre governança e gestão da segurança da informação. Para governar a segurança da informação, o corpo diretivo executa os processos de avaliação, direção, monitoração e comunicação. E ainda o processo de garantia apresenta um parecer independente e objetivo em relação à governança da segurança da informação e do nível atingido.

A Figura 2 mostra o modelo de implantação de GSI.

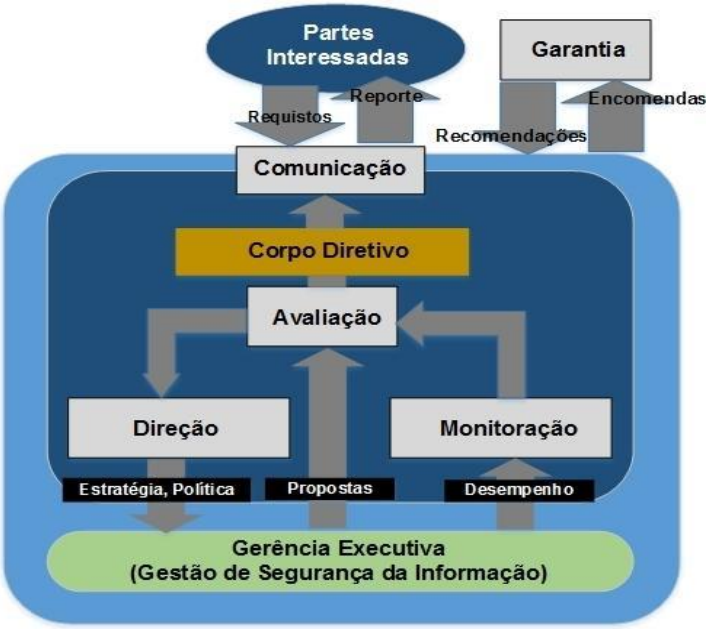

Figura 2: Modelo de implantação de SGI
Fonte: Adaptada da NBR ISO/IEC 27014 (2013, p.6).

Segue abaixo a descrição desses processos:

- Avaliação: Este processo avalia os resultados atuais e previsto dos objetivos de segurança baseado nas atividades atuais e nas alterações planejadas e determina os ajustes para atingir os objetivos estratégicos.
- Direção: Nesta etapa o corpo diretivo informa o direcionamento, os objetivos e estratégia da segurança da informação que serão implementados.
- Monitoração: Permite ao corpo diretivo avaliar se os objetivos estratégicos foram alcançados.
- Comunicação: É realizada a troca de informações entre o corpo diretivo e as partes interessadas sobre a segurança da informação e suas necessidades especificas.

- Garantia: O copo diretivo permite auditorias e analises críticas que irão identificar e validar os objetivos e atividades relacionadas com a governança para alcançar o nível desejado de segurança da informação.

IMPLANTAÇÃO DA GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Neste tópico, abordaremos os conceitos da implantação da governança de segurança da informação fundamentados na referência de Manoel (2014) por tratar-se de um modelo que pode adaptar-se com facilidade ao modelo de governança já implantado na organização. O plano Estratégico de Segurança da Informação (PESI) é "um processo utilizado para desenvolver e elaborar atividades com o objetivo de saber o que deve ser executado, de qual maneira deve ser executado, comunicar e implantar a estratégia que a organização optou" (MANOEL, 2014, p.70). Esse plano é indispensável para a governança da segurança da informação e um fator essencial para o êxito da segurança da informação na organização.

Para sustentar a exigências de segurança da informação devido ao surgimento de novas ameaças e vulnerabilidades, o PESI deve ser flexível e seu principal objetivo é instituir ações em concordância com os objetivos estratégicos da organização, a fim de tornar efetiva a GSI. As principais vantagens do PESI são:

- Diminuir custos de projetos dispensáveis.
- Melhorar a orientação dos esforços através do direcionamento das ações de segurança da informação.
- Evidenciar as ações de segurança da informação nas exigências do negócio.
- Levantamento do nível de segurança da informação através de diagnósticos de segurança e identificar os riscos.
- Adesão às práticas melhores de segurança da informação.

METODOLOGIA DE ELABORAÇÃO DO PESI

A primeira ação para preparar gradualmente o PESI é a entrevista com a alta direção e um estudo dos objetivos estratégicos da organização. E a principal indagação que deve ser realizada é: como a segurança da informação pode colaborar com os objetivos estratégicos da sua organização? Na segunda, verifica-se a conformidade com leis e regulamentos que a organização tem o dever de cumprir.

Na terceira ação, é realizado o mapeamento das áreas e dos processos da organização, com a finalidade de identificar o setor mais crítico e essencial para a organização, que deve ter mais cuidado na implantação da governança de segurança da informação. A seguir, são realizados os diagnósticos de segurança da informação e da gestão e por fim deve ser realizada uma análise SWOP[2], que é uma ferramenta estrutural da administração e tem o objetivo de avaliar os ambientes internos e externos, e desenvolver estratégias de negócios a fim de melhorar o desempenho dos negócios.

OBJETIVOS ESTRATÉGICOS DE SEGURANÇA DA INFORMAÇÃO

Realizados os diagnósticos, devem-se descrever os objetivos estratégicos de segurança da informação alinhados com os princípios de governança. È essencial elaborar uma missão e visão para orientar a segurança da informação de acordo com os objetivos estratégicos da organização.

MATRIZ DOS OBJETIVOS ESTRATÉGICOS E OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

Os objetivos estratégicos da organização relacionados aos objetivos da segurança da informação devem estar apresentados em uma tabela, para mostrar uma estimativa da colaboração dos objetivos da segurança da informação em beneficio dos objetivos estratégicos da organização. Exemplos de objetivos estratégicos de uma organização:

- Proteger as informações contra roubo e vazamento.
- Melhorar os processos de suporte aos funcionários.
- Reduzir a vulnerabilidade da organização em relação aos concorrentes.

Exemplos de objetivos da segurança da informação:

1 - Implantar a GSI.

2 - Proteção à organização contra ataques virtuais.

3 - Garantir a continuidade do negocio.

4 - Conscientização, educação e treinamento aos colaboradores.

A Tabela 1 exemplifica o alinhamento dos objetivos estratégicos com os objetivos de segurança da informação:

[2] "É um acrônimo das palavras *strengths*, *weaknesses*, *opportunities* e *threats* que significam respectivamente: forças, fraquezas, oportunidades e ameaças" (BASTOS, 2014, p.1).

Tabela 1: Alinhamento dos objetivos estratégicos com os objetivos de SI

Objetivos Estratégicos	Objetivos da Segurança da Informação			
Proteger as informações contra roubo e vazamento	1	2	3	4
Melhorar os processos de suporte aos funcionários	1	4		
Reduzir a vulnerabilidade da organização em relação aos concorrentes.	1	2	3	4

Fonte: Adaptada de Manoel (2014 p75).

PLANO DE AÇÃO

O plano de ação de segurança da informação tem o objetivo de reunir as ações estratégicas que ajudam a atingir os objetivos estabelecidos para a segurança da informação. È essencial a criação de métricas e indicadores para medir a eficiência das atividades de segurança da informação implantadas na organização. Estes indicadores devem está inseridos no plano de ação.

CONSIDERAÇÕES FINAIS

Este artigo apresentou uma proposta de integração de governança de segurança da informação e governança corporativa como vantagem competitiva. A definição de governança corporativa não é recente, porém a sua integração com as características de governança de segurança da informação é um desafio para os gestores que buscam um modelo ideal para suas atividades de segurança da informação.

Os conceitos de estratégia e governança são indispensáveis para uma organização que deseja manter-se competitiva. E ao integrar seus processos de governança, cria-se um ciclo de benefícios que levam ao aumento na integridade do negócio e a confiança de acionistas e partes interessadas, melhorando sua competitividade, garantindo investimentos e estabilidade financeira.

A governança de segurança da informação deve ser ajustada a qualquer organização, mesmo as que não possuem governança corporativa implementada. Esta tarefa pode ser facilitada pela adoção de normas, práticas já adotadas e modelos de documentação, como da família ISO/IEC 27001.

Entre os resultados desejados a partir da implementação eficiente da governança de segurança da informação, estão: a visibilidade do corpo diretivo sobre a situação da segurança da informação, a tomada de decisão mais rápida sobre os riscos da informação, investimentos mais eficientes em segurança da informação e a conformidade com requisitos legais e contratuais.

A segurança da informação deve ser vista como estratégia e ser um diferencial competitivo nas organizações, pois agrega valor ao negócio e à imagem da empresa. Este processo não é simples e traz consigo uma mudança de cultura administrativa.

Como sugestão para novos estudos destaca-se a gestão do planejamento estratégico da organização e da governança de segurança da informação através da ferramenta Geplanes[3].

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014:2013 Tecnologia da informação – Técnicas de Segurança – Governança de segurança da informação**. Rio de Janeiro, 2013.

BASTOS. Marcelo. **Análise SWOT (Matriz) – Conceito e Aplicação.** [2014]. Disponível em: <http://www.portal-administracao.com/2014/01/analise-swot-conceito-e-aplicacao.html>. Acesso em: 06 nov.2016.

JUNIOR. Nivaldo dos Santos Pereira. **Administração Geral.** [2012]. Disponível em: <https://www.portaleducacao.com.br/administracao/artigos/11608/administracao-geral.html>. Acesso em: 31 out.2016.

MANOEL, Sergio da Silva. **Governança de Segurança da Informação:** como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014

OLIVEIRA JUNIOR. Nilson José. **Um diagnóstico da Gestão Estratégica baseada no *BalancedScoread:*** um estudo de caso. 2008. 148 f. Dissertação (Mestrado de Estudo Sociais) – Universidade Federal do Amazonas, Manaus, 2008.

PEREIRA. Heitor José Pereira. **Estratégias de Negócios:** conceitos básicos de Planejamento e Estratégia. MBA Executivo em Gestão Empresarial Estratégica – EDUCON, São Paulo, 2004.

[3] Disponível em: https://softwarepublico.gov.br.