Melhores práticas envolvendo ITIL e COBIT

Willian Gabriel Ruas[1], Iwens Sene Junior[2]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Goiânia – GO – Brazil

Instituto de Informática – Universidade Federal de Goiás (UFG)
Goiânia – GO – Brazil.

willianruas.wr@gmail.com, iwensjr@gmail.com

Abstract. *With the advancement of Information Technology - IT in business, the existence of contingency plans has become increasingly aside. From a brief analysis of what are the risk management, models such as COBIT and ITIL, applies an intersection table between the best practices contained in these frameworks to mitigate risks not only in the IT field. This work is aimed at feasibility study, predict and mitigate many of the risks of a company. Case study results show a decrease in delinquency and increased sales in the studied company.*

Resumo. *Com o avanço da Tecnologia da Informação - TI nas empresas, a existência de planos de contingência tem ficado cada vez mais de lado. A partir de uma breve análise do que são a Gestão de Riscos, modelos como COBIT e ITIL, aplica-se uma tabela de intersecção entre as melhores práticas contidas nestes frameworks para mitigação de riscos não só na área de TI. Este trabalho tem como objetivo a viabilidade de estudar, prever e mitigar boa parte dos riscos de uma empresa. Resultado do estudo de caso mostra a diminuição da inadimplência e aumento das vendas na empresa estudada.*

1. Introdução

Cada vez mais as organizações se tornam dependentes das informações contidas em Sistemas de Informação, mas acabam se esquecendo de que equipamentos também estão sujeitos às falhas e deve haver um planejamento para a continuidade do negócio, com a menor perda de informação, tempo e dinheiro possível. Os riscos para o negócio dependem do contexto onde as empresas estão inseridas e de suas rotinas já definidas, envolvendo pessoas, processos e tecnologia. As melhores práticas, do ITIL e COBIT descritas neste artigo, devem ser aplicadas a todo tipo de organização e principalmente contar com o apoio das partes mais interessadas, a alta direção [3].

Para isso, utiliza-se o COBIT e ITIL, que são conjuntos de boas práticas e recomendações para a melhoria contínua dos processos já existentes nas empresas e para a criação de processos mais eficientes e eficazes. Sendo que o COBIT demonstra mais diretamente o que a empresa deve fazer e o ITIL como ela deve fazer.

O objetivo deste artigo é apresentar como o ITIL e o COBIT podem e devem trabalhar juntos, para que as melhores práticas de cada um possam ser utilizadas de forma personalizada por qualquer empresa, provendo assim uma maior organização nos

processos tanto de TI quanto nos demais processos da empresa, visando a segurança, boas práticas e fluidez nos processos.

2. Modelos das melhores práticas entre COBIT e ITIL

2.1. COBIT

O COBIT é um framework dirigido a gestão de Tecnologia da Informação e mantido pela ISACA (*Information Systems Audit and Control Association*). Sendo uma estrutura de negócios para a governança e gestão de TI corporativa, o COBIT tem como missão de pesquisar, desenvolver, publicar e promover um conjunto atualizado de padrões internacionais de boas práticas. Incorpora as últimas novidades em técnicas de governança corporativa e de gestão, fornece princípios globalmente aceitos, práticas, ferramentas e modelos analíticos para ajudar a aumentar a confiança e valor de sistemas de informação.

Estruturado em quatro domínios, que possuem 34 processos, e estes processos possuem 210 objetivos de controle: Planejar e Organizar; Adquirir e Implementar; Entregar e Suportar; Monitorar e Avaliar.

O COBIT não é uma norma como a ISO (*International Organization for Standardization*), mas sim um direcionador de esforços e recursos da TI para atender aos requisitos do negócio. A adoção do COBIT não tem como meta controlar todos os processos, mas apenas identificar quais processos da TI estão impactando, ou gerando riscos para o negócio, de modo a priorizar o gerenciamento desses processos [5].

Um fator extremamente significativo é o que o COBIT, por ser um framework de controle de alto nível, aponta o que deve ser controlado, mas não diz como fazer, encaixando-se perfeitamente com as melhores práticas para gestão de serviços de TI, descritas na ITIL, cujo foco está na recomendação das melhores práticas para serem aplicadas nos diferentes níveis de controle descritos no COBIT.

Segundo Sortica, Clementi e Carvalho em 2004 “O COBIT está organizado em quatro domínios para refletir um modelo para os processos de TI. Os domínios podem ser caracterizados pelos seus processos e pelas atividades executadas em cada fase de implantação da Governança Tecnológica. Os domínios do COBIT são: (a) Planejamento e Organização; (b) Aquisição e Implementação; (c) Entrega e Suporte; (d) Monitoração.

Além dos quatro domínios principais que guiam o bom uso da tecnologia da informação na organização, existe também a questão de auditoria que permite verificar, através de relatórios de avaliação, o nível de maturidade dos processos da organização. O método de auditoria segue o modelo do CMM (*Capability Maturity Model*) que estabelece os seguintes níveis: 0) Inexistente: significa que o processo de gerenciamento não foi implantado. 1) Inicial: o processo é realizado sem organização, de modo não planejado. 2) Repetível: o processo é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido. 3) Definido: o processo é realizado, documentado e comunicado na organização. 4) Gerenciado: existem métricas de desempenho das atividades, o processo é monitorado e constantemente avaliado. 5) Otimizado: as melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos. ”

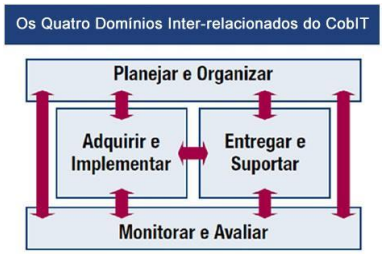

Figura 1. Domínios relacionados COBIT

2.1.1. Passos para implantação do COBIT em uma empresa:

Pontuando uma empresa de 0 até 5 conforme modelo CMM descrito anteriormente. O primeiro passo seria levantar os domínios e o grau das atividades dos processos na organização de forma satisfatória, para poder identificar qual o grau alcançado pela organização. Este trabalho de levantamento é feito com a utilização de questionários e, portanto, o investimento nestas atividades não precisa ser grande, restringindo-se apenas no tempo despendido pelas pessoas envolvidas.

Com isso percebe-se que o COBIT não necessita de novas tecnologias, podendo ser realizado em paralelo com à implementação dos sistemas corporativos de gerenciamento e administração da organização.

O resultado da auditoria aplicada a partir do COBIT é ajudar a área de TI a identificar o grau atual e como evoluir para melhorar os processos da organização.

2.2. ITIL

Assim como o COBIT, o ITIL é um conjunto de boas práticas, recomendações, a serem aplicadas na infraestrutura, operação e manutenção de serviços de TI. Busca promover a gestão com foco no cliente e na qualidade dos serviços de TI, lidando com estruturas e processos para a gestão de uma organização de TI apresentando um conjunto abrangente de processos e procedimentos gerenciais, organizados em disciplinas com os quais uma organização pode fazer sua gestão tática e operacional em vista de alcançar o alinhamento estratégico com os negócios.

Seus conceitos são aplicados nos níveis operacionais e táticos, permitindo que a área de TI estruture o ciclo de vida de seus serviços como um todo, de modo a alcançar excelência operacional.

Em 2007 foi lançada a versão 3 do ITIL, composta por 5 livros, onde a visão de processos da V2 foi organizada em ciclos de vida contendo 5 fases, sendo elas: Service Strategy, Service Design, Service Transition, Service Operation e Continual Service Improvement.

Estratégia de Serviço: Nessa fase a TI irá se integrar com o negócio, sendo o ponto de origem do ciclo de vida do serviço ITIL, é um guia sobre como tornar mais claro e priorizar investimentos sobre provimento de serviços.

Desenho de Serviço: Nessa fase tudo o que foi levantado na estratégia será usado para projetar um novo serviço, englobando todos os elementos relevantes à entrega de serviços, ao invés de focar somente no projeto da tecnologia propriamente dita.

Transição de Serviço: Depois do serviço ser desenhado, esta fase irá criar o serviço. Direcionado à entrega dos serviços necessários ao negócio no uso operacional, e geralmente englobam o projeto.

Operação de Serviço: A preocupação nesta fase é manter o serviço que foi criado na transição. Aqui serão encontrados os processos e funções que vão lidar com as atividades do dia-a-dia. Parte do ciclo de vida onde serviços e valor são entregues diretamente. Assim, monitoramento de problema e balanceamento entre disponibilidade de serviço e custo, etc, são considerados.

Melhoria de Serviço Continuada (MSC): Essa fase envolve todas as outras e possui um foco na qualidade, avaliando o serviço e os processos de gerenciamento dos estágios do ciclo de vida, ajustando e reajustando os serviços de TI às mudanças contínuas do negócio através da identificação e implementação de melhorias aos serviços de TI que apoiam processos negociais.

3. A informação

Mais do que nunca, a informação é vital para o processo de tomada de decisão de Estados, empresas, órgãos públicos e afins. Cerca de 80% das informações necessárias para sustentar a tomada de decisão estão disponíveis, devido a ampliação dos meios de comunicação e democratização da informação [10].

Segundo Freitas em 2009:

"A estimativa de riscos está intimamente ligada ao que em Gestão de Riscos, de modo geral, é denominado como "apetite pelo risco"[7] o quanto de risco a alta direção está disposta a correr. As organizações *The Institute of Risk Management* – IRM, *The Association of Insurance and Risk Managers* – AIRMIC e o ALARM, um fórum nacional para Gestão de Riscos no Setor Público do Reino Unido, desenvolveram um padrão de gestão de riscos bastante interessante que é alinhado com a ISO/IEC Guide 73:2002. Neste documento o "apetite pelo risco", para fins de segurança em sistemas de informação, é melhor situado como "tolerância ao risco", que é obtido avaliando-se:

- A probabilidade de que o risco venha ocorrer
- A perda potencial ou o impacto financeiro do risco
- O valor do risco, que significa"

4. JUNÇÃO ITIL E COBIT

Em relação a compatibilidade com o ITIL, o COBIT cobre a maioria dos processos ITIL, tanto na versão 2 quanto na versão 3, entretanto o ITIL tem os processos apresentados com maior nível de detalhe. De maneira geral, enquanto o ITIL está mais direcionado ao "como", o COBIT foca no "o que". Assim, pode se dizer que o COBIT é um framework de controle que estabelece o que tem que ser feito, mas não diz como deve ser feito.

A proposta de junção fará a eleição de alguns requisitos que são definidos pela importância de uma aplicação. Sendo que para a junção, foi estudado os processos contidos tanto no ITIL quanto no COBIT, fazendo assim a compatibilização entre os dois frameworks.

4.1. ITIL

Na tabela 1, encontra-se a equivalência entre os dois frameworks, onde na primeira e quarta colunas se encontram os nomes dos domínios e estágio do ciclo de vida do COBIT e ITIL, respectivamente. E na segunda e terceira colunas, ficam os processos contidos em cada framework.

Observe que ao realizarmos a compatibilização dos processos, tanto os domínios do COBIT quanto os estágios do ITIL são incompatíveis, já que cada processo faz parte de um estágio diferente de cada framework. Contudo, ao percebermos que o COBIT trabalha com o nível mais estratégico do processo, abordando ele como um todo, o ITIL se foca nos detalhes do que cada processo deve fazer, voltado mais para o nível operacional do estágio.

Tabela 1. Equivalência entre ITIL e COBIT

Domínio do COBIT	COBIT	ITIL	Estágio do ciclo de vida do ITIL
Planejar e Organizar	Definir um Plano Estratégico de TI	Geração de Estratégia	Estratégia de Serviço
	Gerenciar Investimento em TI	Gerenciamento Financeiro	
Adquirir e Implementar	Gerenciar Mudanças	Gerenciamento de Mudanças	Transição de Serviço
	Instalar e certificar Soluções e Mudanças	Gerenciamento de Mudanças	
Entregar e Suportar	Definir Níveis de Serviço	Gerenciamento de Níveis de Serviço	Desenho de Serviço
	Gerenciar Serviços de Terceiros	Gerenciamento de Níveis de Serviço	
	Gerenciar Performance e Capacidade	Gerenciamento de Disponibilidade & Gerenciamento de Capacidade	
	Garantir a Continuidade dos Serviços	Gerenciamento de continuidade dos serviços de TI	
	Garantir a Segurança dos Sistemas	Gerenciamento da Segurança da informação	
	Identificar e Alocar custos	Gerenciamento de Finanças	Estratégia de Serviço
	Educar e treinar usuários	Gerenciamento de Mudança	Transição de Serviço
	Gerenciar Dados	Gestão do conhecimento	
	Gerenciar Service Desk e Incidentes	Service Desk	Operação do Serviço

	Gerenciar Problemas	Gerenciamento de Problemas	
	Gerenciar Operações	Operação	
Monitorar e Avaliar	Monitorar e Avaliar a Performance da TI	Melhoria Continua de Serviço	
	Monitorar e Avaliar Controle Interno		
	Assegurar Conformidade Regulatória		

Pode-se ver que ambos os frameworks têm suas partes em comum, tendo várias de suas boas práticas presentes um no outro. Ao se fazer a implantação destes processos citados acima, resolveremos a parte principal da implantação integral de um dos métodos.

Há também uma maior facilidade na implantação destes processos, pois pode-se consultar ambos os frameworks, adequando a implantação com as necessidades da empresa. Fazendo com que a empresa esteja sempre à frente dos acontecimentos, isso garante uma certa confiabilidade e segurança para cada processo a ser implantado.

5. Estudo de caso

Esta pesquisa utilizou uma abordagem exploratória de estudo de caso da EMPRESA X, uma fábrica de blocos e artefatos de concreto. Detalhando o processo do Departamento Financeiro como um todo e em seguida aplicando a tabela para melhoria do processo.

5.1. O Processo

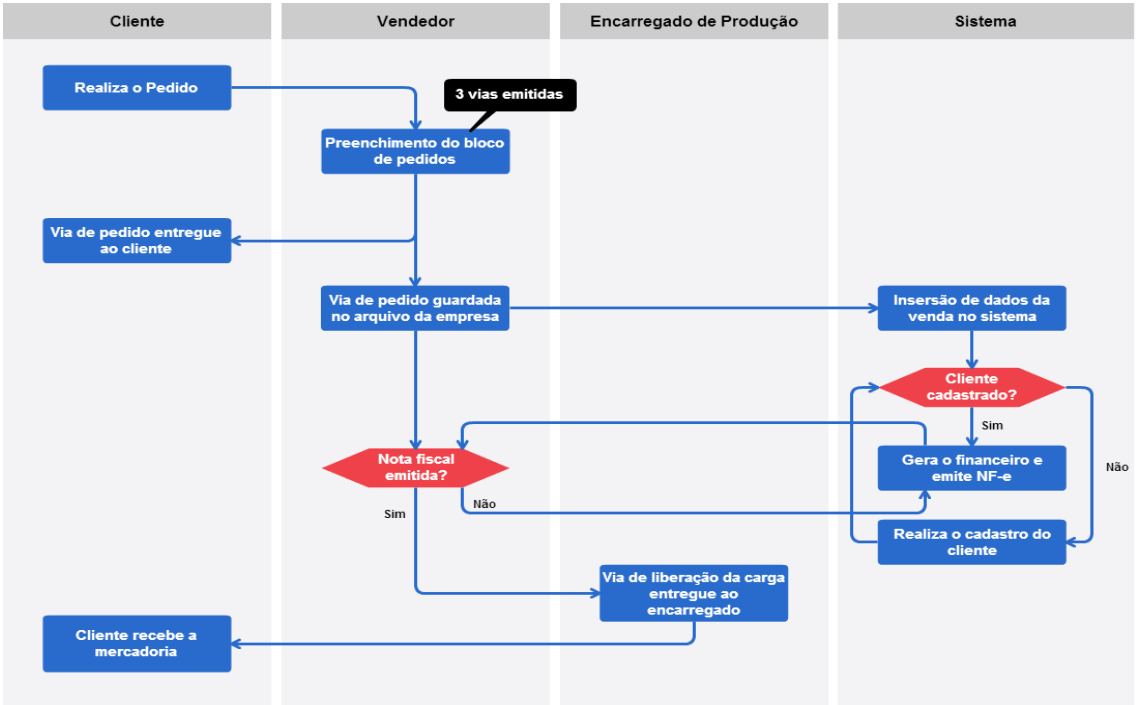

Figura 2. Representação do processo financeiro da empresa

O processo do departamento financeiro tem início na chegada do cliente, onde a venda ocorre. Após a venda, faz-se o preenchimento do bloco de pedidos (físico), sendo uma via para o cliente, outra via para a empresa e outra via para liberação da carga. Após isso, insere-se a venda no sistema, com o devido cadastro do cliente, preenchendo o produto vendido, a quantidade de cada produto, o valor de cada produto e a forma de pagamento. Se a forma de pagamento for a vista, guarda-se o dinheiro no caixa para depósito posterior. Se o pagamento for em cheque a prazo, faz-se a custódia no banco. Se o pagamento for em boleto, emite-se o boleto para ser entregue junto com a mercadoria e a nota fiscal. Após a emissão da NF-e, a carga é liberada e entregue para o cliente, sendo o próximo passo a cobrança do mesmo. A cobrança consiste em executar o cheque ou receber o boleto. Em caso de inadimplência, entra-se em contato com o cliente para esclarecimento. Caso o pagamento não seja realizado em um número x de dias, a duplicata é enviada para protesto no cartório, como demonstrado na figura 2.

5.2. Aplicação da tabela 1 no processo financeiro

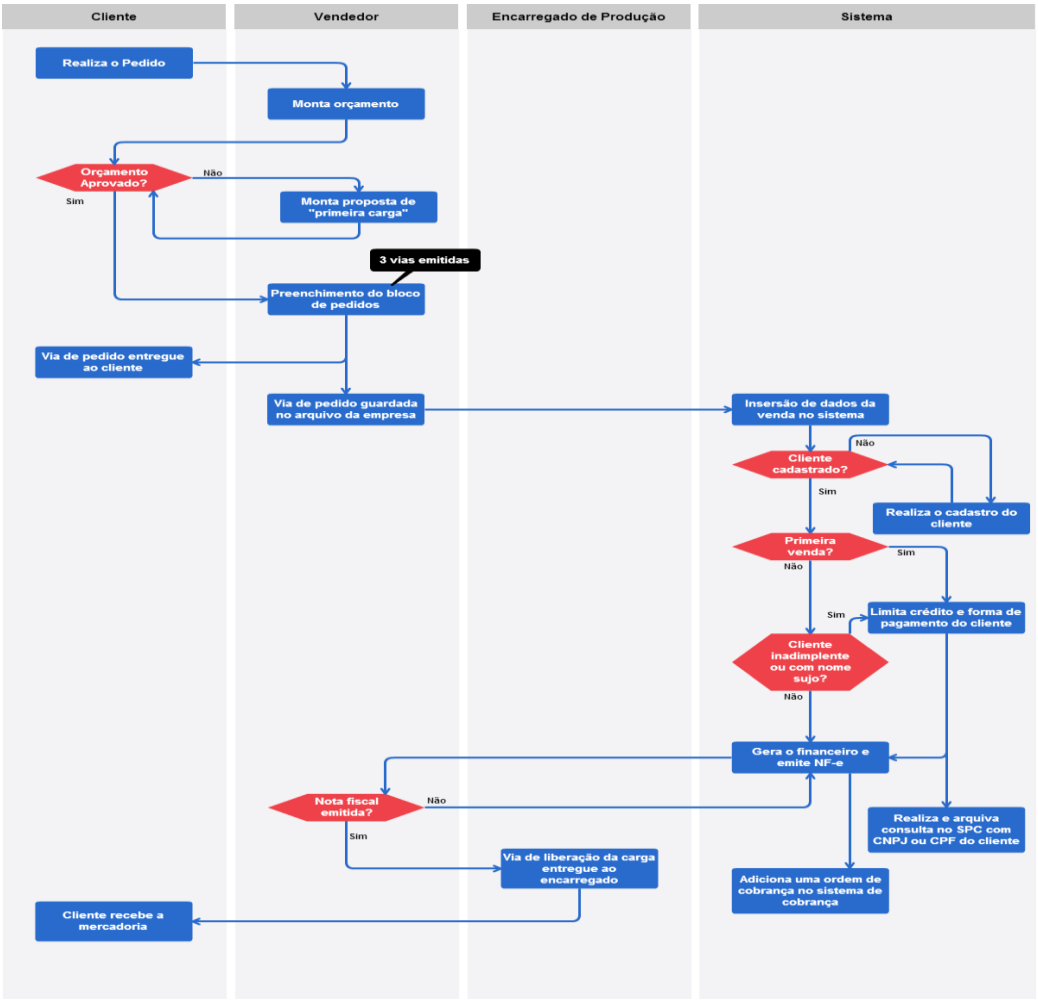

Figura 3. Representação do processo financeiro da empresa após aplicação da tabela 1

Para exemplificar o uso da tabela 1 aplica-se no departamento financeiro os seguintes estágios do ITIL e COBIT: Gerenciamento de Finanças e Identificar e alocar custos, já que o processo citado no caso de uso remete ao departamento financeiro.

Segundo o Gerenciamento de Finanças “Representa oportunidades para provedores de serviço entregarem valor para o negócio do cliente, através de um ou mais serviços”. Com isso, amplia-se o escopo do processo de venda, adicionando o processo de “primeira venda” e “consulta do cliente”, onde clientes novos só pagam a vista, ou no cartão, para logo em seguida realizar a consulta nos órgãos de proteção de crédito. Garantindo assim uma maior segurança para empresa e grande redução na inadimplência causada por clientes novos com nome sujo no mercado. Implementa-se também o processo de “primeira carga”, onde o cliente traz o preço orçado por outra empresa e a primeira carga é feita naquele preço, mostrando assim a qualidade do produto oferecido, como demonstrado na figura 3.

Como resultados, obtemos o aumento de vendas com o método de “primeira carga”, sem afetar a lucratividade da empresa e a diminuição na inadimplência com a implantação da “primeira venda”, já que a consulta da situação cadastral do crédito do cliente assegurou a viabilidade da venda.

6. Conclusão

Ignorar riscos não os faz deixar de existir, mas sim, ter uma bomba relógio que explodirá quando menos esperar e sempre muito importante se prevenir, segundo a maioria dos autores de segurança da informação os ataques acontecerá na pior hora, da pior forma e de modo que cause o maior dano possível.

Um foco nas pessoas deve ser dado na tentativa de conscientizar acerca de suas importâncias na segurança do sistema e do valor dos dados resguardados. Devem saber que um sistema seguro depende bem mais que apenas do setor de segurança da informação, mas de todos da instituição. Afinal, falhas humanas tornam vulneráveis tecnologias ou processos implementados na segurança da instituição.

Uma Política de Segurança da informação é percebida como fundamental na implementação de um projeto de segurança. Fazendo-se necessária uma correta valorização quanto a existência de uma política associada aos procedimentos de sua utilização, para a defesa do bem mais importante de uma empresa, a informação.

Como foi apresentado, o COBIT é aplicado a um nível estratégico e o ITIL a um nível tático e operacional. O primeira mostra “do que fazer”, o outro de “como fazer”, e apesar deles terem focos e objetivos diferentes, e público-alvo distintos, eles têm estruturas complementares podendo ser combinadas, o que pode trazer uma valiosa contribuição para a empresa.

7. Referências

BRASIL, ABNT. NBR ISO/IEC 27001:2006. Rio de Janeiro: ABNT, 2006

Laureano, M. A, P.; Moraes, P. E. S. Segurança como Estratégia de Gestão da Informação. Artigo de Revista Economia & Tecnologia, v. 8, pp. 38-44. 2005.

Freitas, Antônio Mello. Gestão de Riscos Aplicada a Sistemas de Informação: Segurança Estratégica da Informação. Universidade Candido Mendes. 2009.

https://cobitonline.isaca.org/about - 27/10/2014

http://www.devmedia.com.br/cobit-4-1-entendendo-seus-principais-fundamentos/28793 - 27/10/2014

Fundação Nacional Da Qualidade. Gestão de Risco. 2014.

Sortica, Eduardo Almansa; Clementi, Sérgio; Carvalho, Tereza Cristina M. B. Governança de TI: comparativo entre COBIT e ITIL. EPUSP-LARC. 2004.

Casrtlidge, Alison. An Introductory Overview of ITIL V3. 1. ed. [S.l.]: The UK Chapter of the itSMF, 2007.

Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender, Ed. ACM Press Frontier Series. ACM, New York, NY, 19-33. DOI= http://doi.acm.org/10.1145/90417.90738.

Andreuzza, Mário. O valor da informação. Sagres.