

---

# SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO

Marcos Aurelio Pchek Laureano e Paulo Eduardo Sobreira Moraes  
(laureano@ppgia.pucpr.br e pauloeduardo@facinter.br)

## 1. Introdução

Este artigo tem por objetivo analisar a prática da segurança como estratégia de gestão da informação. Por meio da revisão da literatura, determina-se a relação entre estratégia e segurança no que diz respeito a dados e gestão da informação. Discute-se a segurança como atitude inerente aos processos de gestão da informação, no sentido de oferecer às organizações um maior controle sobre os dados relevantes e uma conformação maior com os mecanismos de tomada de decisão e confidencialidade dentro das instituições.

## 2. Estratégia: O que é e a que Veio

Diversos autores têm discutido sobre as origens e o significado do termo estratégia. Alguns, como Sacconi (1998), afirmam que estratégia pode ser entendida como o conhecimento necessário para a realização de desígnios hábeis que determinam uma posição privilegiada para a organização. Deste modo, oferece-se uma perspectiva apropriadamente racional para o ato estratégico, definindo-o como ato que não prescinde de cientificidade e coerência e que é caracterizado por aperfeiçoar a realização de um plano hábil (estratagema). De acordo com Sacconi, a estratégia é fruto da atividade criativa do ser humano, de sua argúcia administrativa que norteia as decisões institucionais. Por sua vez, Maslow (2001) assevera que características psicológicas particulares motivam posturas específicas nos ambientes organizacionais. Entretanto, estratégia não se limita tão somente a estratagemas, alcançando uma proporção que vai além da elaboração de um simples ardil.

A idéia do termo estratégia se ligava originalmente, em grego, a um magistrado ou comandante-chefe militar. O estrategista como comandante militar tem por responsabilidade privilegiar seus potenciais militares e forças sob seu comando a fim de maximizar as oportunidades de sucesso em conflitos. Na visão de Ferreira (1994), estratégia é a arte militar de planejar e executar movimentos e operações que visam alcançar ou manter posições relativas e potenciais bélicos favoráveis a futuras incursões de exércitos. Assim, a estratégia como atitude lógica e engenhosa cujo objetivo é privilegiar uma organização específica se origina da necessidade militar de sobrepor interesses e posições de vantagem de uma armada sobre outra. Ainda que não haja guerras no mercado além das comerciais, a estratégia é utilizada pelas corporações no mesmo sentido, procurando vantagens sobre seus concorrentes.

Pedro (1997), por sua vez, dá relevo à influência de estratégias na ascensão e desmoroamento de civilizações, reinos e impérios. Todavia, no sentido científico-

administrativo, estratégias têm por fim vantagens que não são apenas momentâneas, com vistas a um objetivo particular, mas que determinam a possibilidade de benefício direto em cada posição que a instituição assuma ao longo de sua história.

Atualmente, os gestores organizacionais, em especial os de alto escalão, têm por finalidade a promoção da instituição, seus produtos, serviços e ativos, de tal modo que estes sejam bem-sucedidos no mercado a partir de ações racionais, seguras e afinadas com os mecanismos de interação do mercado, conforme explicam Moraes, Gurek e Pieretti (2004). Por tanto, o estrategista organizacional tem necessidade de dados e informações que possibilitem tomadas de decisões fundamentadas. Assim, as decisões serão tomadas a partir de uma análise que pondere as relações internas e externas à organização. Aliás, as condições econômicas, culturais e sociais são determinadas por informações e relações de dados que emergem destes mesmos entes em um processo iterativo, em rede, complexo e multivariante. Castells (1999) corrobora tal percepção iterativa ao passo que Sveiby (1999) assinala a importância dos ativos de conhecimento e da perspicácia da organização.

A estratégia organizacional é também uma forma de inserir a cultura organizacional nas atitudes dos administradores, em especial dos de alto escalão. Castor (2000) discorre acerca da condição brasileira de mercados, governo e burocracia, revelando condicionantes culturais nas ações de administradores de empresas nacionais. Assim, as estratégias são particulares de cada instituição e são, ao mesmo tempo, uma resposta adaptativa ao meio.

Babeler (1998), vê a estratégia como resultante dos esforços racionais da organização em resposta aos desafios que o ambiente externo lhe interpõe. O mesmo pode ser dito em relação ao desenvolvimento das capacidades internas no sentido de se aperfeiçoarem para que a instituição corresponda às expectativas de seus acionistas, participantes, clientes, organizações parceiras, sociedade, etc. Assim, estratégias organizacionais podem, ao mesmo tempo, atenderem a imperativos externos e internos, independente de áreas e departamentos, de segmentos e localização de mercados e de atividades organizacionais.

O processo organizacional opera taticamente no processo dialético entre a negação de estratégias que se esgotaram e estratégias a serem implementadas no intento de satisfazerem tais imperativos. Cunha e Cunha (1999) corroboram tal percepção. Tanto o mercado como as organizações são entes dinâmicos que evoluem, ora em sentidos opostos, ora no mesmo sentido, mas que sempre buscam um discurso e prática consensual, dada à influência mútua que exercem entre si. Habermas (1989) observa que tal consenso não é necessariamente comunicativo, mas instrumental; isto é, mercado e organizações se relacionam a partir de uma concepção de disputa por privilégios.

Em especial, a gestão estratégica de informações e dados é fundamental para as organizações, uma vez que “possibilita tomadas de decisão que sustentam outros processos de gestão e outros processos estratégicos” (Gimenez, Pelisson, Krüger e Hayashi, 1999, p.69). Não por acaso Kodama (1991) destaca a necessidade de dados e informações para o estabelecimento de estratégias. Assim, passa-se a discorrer acerca da importância da informação nos processos estratégicos.

### **3. A importância da Informação nos Processos Estratégicos**

A informação, na visão de Rezende e Abreu (2000), é o dado com uma interpretação lógica ou natural agregada pelo usuário. A informação é um ativo que, como qualquer outro ativo

importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegido (NBR ISO/IEC 17799, 2003). Como salienta DIAS (2003), a informação é o principal patrimônio da empresa e está sob constante risco.

O domínio da informação sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos sistemas de informação, ganhou-se mobilidade, inteligência e real capacidade de gestão.

A informação é substrato da inteligência competitiva e deve ser administrada em seus particulares, diferenciada e salvaguardada. Ela funciona como um recurso essencial para a definição de estratégias alternativas e para a constituição de uma organização flexível, onde o aprendizado é constante.

De acordo com Rezende e Abreu (2000), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. Ela ajuda na identificação das ameaças e das oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz.

Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, uma determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente. Boran (1996), Wadlow (2000) e Abreu (2001) classificam a informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa:

- Pública. Informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital.
- Interna. O acesso livre a este tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital.
- Confidencial. Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.
- Secreta. Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Independente da relevância ou do tipo da informação, a gestão dos dados organizacionais é estratégica porque possibilita a tomada de decisões em qualquer âmbito institucional. De fato, algumas informações são centrais para a organização, e sua divulgação parcial ou total pode acarretar repercussões cuja complexidade pode ser pouco ou nada administrável pela organização. É necessário cuidado com a integridade, a precisão, a atualidade, a interpretação e o valor geral da informação.

A divulgação das informações confidenciais ou secretas pelos elementos que participam da organização constitui-se em uma falta ética e moral grave, conforme Sá (2001). De acordo com Mota e Amorim (2001), na economia do conhecimento, a divulgação de dados ou informações organizacionais pode trazer perdas econômicas ou danos.

Os conceitos que envolvem a Engenharia da Informação – que é um conjunto de disciplinas voltado ao fornecimento da informação correta para a pessoa certa no tempo exato, conforme Martin (1991) e Feliciano Neto, Furlan e Higo (1988) – já mostravam a importância da segurança da informação para as instituições. Conforme afirma Deresky (2004, p. 25), “a segurança passa a ser crítica na gestão da informação organizacional”. Assim sendo, é necessário valorizar o uso de sistemas de segurança como estratégia para a gestão da informação e dos dados organizacionais.

#### **4. Critérios para Segurança da informação**

É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam proporcionar confidencialidade, integridade e disponibilidade. Segundo Albuquerque (2002) e Krause (1999) há três princípios básicos para garantir a segurança da informação:

- **Confidencialidade.** A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.
- **Disponibilidade.** A informação deve estar disponível no momento em que a mesma for necessária.
- **Integridade.** A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

O item integridade não pode ser confundido com confiabilidade do conteúdo (significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer íntegra (não sofrer alterações por pessoas não autorizadas).

**Alguns autores** defendem que para que uma informação seja considerada segura, o sistema que o administra ainda deve respeitar os seguintes critérios:

- **Autenticidade.** Garante que a informação ou o usuário da mesma é autêntico.
- **Não repúdio.** Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; não é possível negar o envio ou recepção de uma informação ou dado.
- **Legalidade.** Garante a legalidade (jurídica) da informação; a aderência de um sistema à legislação; e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação nacional ou internacional vigente.
- **Privacidade.** Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve poder ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade à informação). É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.
- **Auditoria.** Rastreabilidade dos diversos passos de um negócio ou processo, identificando os participantes, os locais e horários de cada etapa. A auditoria aumenta

a credibilidade da empresa e é responsável pela adequação da empresa às políticas legais e internas.

A todas estas ponderações acerca de critérios para a segurança da informação soma-se outra como estratégia de gestão da informação: a veracidade. Isto é, a informação deve estar calcada em acontecimentos verídicos ou argumentos lógicos compatíveis com a necessidade da organização. Nesse sentido, não basta que a informação seja autêntica, pois sua fonte pode ser desonesta. Não basta a confiabilidade, mas também deve existir veracidade.

A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem seus objetivos, pois seus sistemas de informação serão mais confiáveis. A segurança passa, assim, a ser uma estratégia de gestão da informação aplicável a toda a organização. A veracidade da informação é um critério a ser contemplado nos sistemas de segurança para que se possa fomentar uma gestão da informação estratégica para toda a instituição.

Antigamente, a atenção sobre a segurança da informação estava focada na tecnologia. Hoje, o desafio é construir uma relação de confiabilidade com clientes e parceiros. Conforme Rezende e Abreu (2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório.

Neste contexto, a segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática e viabilizando o uso de aplicações de missão crítica.

## **5. Conclusões**

O elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas), que por sua vez, é a responsável por garantir a fidelidade da informação. No planejamento estratégico da informação é vital a participação do Analista ou Gestor de Negócio, que é quem tem competência para avaliar o valor da informação.

A melhor forma de garantir a segurança da informação estratégica é atuar junto às pessoas que de alguma forma manipulam a informação (conscientizando-as através, por exemplo, de treinamentos) e utilizar termos de confidencialidade. Estes termos permitem responsabilizar juridicamente as pessoas que de alguma forma causarem um dano financeiro à empresa por vazamento de informação.

Estrategicamente, é importante que as empresas adotem as regulamentações do mercado em que atuam, como o Novo Código Civil, Sarbanes e Oxley, Publicações do Conselho Federal de Medicina, normas ABNT e ISO, entre outras. A adoção das políticas de Segurança da Informação proporciona a transparência e fornece credibilidade à empresa perante a sociedade.

Enfim, as práticas da Segurança da Informação garantem que a informação certa esteja disponível na hora certa, para que a pessoa certa possa tomar a decisão estrategicamente adequada.

**REFERÊNCIAS BIBLIOGRÁFICAS**

ABREU, Dimitri. 2001. **Melhores Práticas para Classificar as Informações**. Módulo e-Security Magazine. São Paulo, agosto. Disponível em [www.modulo.com.br](http://www.modulo.com.br). Acessado em: 17/03/2004.

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. 2002. **Segurança no Desenvolvimento de Software** – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro.

BAßELER, Ulrich. HEINRICH, Jürgen. KOCH, Walter. 1998. **Grundlagen und Probleme der Volkswirtschaft**: Lehr – und Arbeitsbuch mit lernzielorientierten Leitfragen, grundlegenden Informationen und Arbeitsaufgaben, Colônia: Wirtschaftsverlag Bachem GMBH.

BORAN, Sean. IT Security Cookbook, 1996. Disponível em <http://www.boran.com/security/>. Acesso em: 17/03/2004.

BORAN, Sean. **IT Security Cookbook**, 1996. Disponível em <http://www.boran.com/security/>. Acessado em: 17/03/2004.

CASTELLS, Manuel. 1999. **A sociedade em rede**. v. 1. São Paulo: Editora Paz e Terra.

CASTOR, Belmiro Valverde Jobim. 2000. **O Brasil não é para amadores**: estado, governo e burocracia na terra do jeitinho. Curitiba: EBEL: IBQP-PR.

COLLÉT, Gaspar Pereira e RAZZOLINE FILHO, Edelvino. 2002. Avaliação do impacto das ações de reponsabilidade social da organização, através do composto mercadológico. In: **Tecnologia & Humanismo**: órgão oficial de divulgação científica e tecnológica do Centro Federal de Educação Tecnológica do Paraná. Ano 16, número 22 e 23, 1<sup>o</sup>. e 2<sup>o</sup>. Semestres/. Páginas 111 a 119. Curitiba: CEFET-PR.

CUNHA, Miguel Pina e CUNHA João Vieira da. 1999. Tese, síntese, antítese: contributos para uma teoria dialéctica das organizações. In: **Revista de Administração Contemporânea**. Volume 3. Número 3, Setembro/Dezembro. Páginas 7 a 36. Curitiba: Anpad.

DeMARCO, Tom e LISTER, Timothy Peopleware. 1990. **Como gerenciar equipes e projetos tornado-os mais produtivos**. Editora McGraw-Hill. São Paulo.

DERESKY, Helen. 2004. **Administração Global**: estratégica e interpessoal. Porto Alegre: Bookman.

DIAS, Cláudia. 2000. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books.

FELICIANO NETO, Acácio; FURLAN, José Davi e HIGO, Wilson. 1988. **Engenharia da Informação** – Metodologia, Técnicas e Ferramentas. São Paulo: McGraw-Hill.

FERREIRA, Aurélio Buarque de Holanda. 1994. **Dicionário da Língua Portuguesa**, São Paulo: Nova Fronteira.

GIMENEZ, Fernando A. P. PELISSON, Cleufê. KRÜGER, Eugênio G. S. e HAYASHI Jr. Paulo. 1999. Estratégia em pequenas empresas: uma aplicação do modelo de Miles e Snow. In: **Revista de Administração contemporânea**. Volume 2; Número 3, Maio/Agosto. Páginas 53 a 74. Curitiba: Anpad.

HABERMAS, Jürgen. 1989. **Consciência moral e agir comunicativo**. Rio de Janeiro: Tempus.

KRAUSE, Micki e TIPTON, Harold F. 1999. **Handbook of Information Security Management**. Auerbach Publications.

KODAMA, Fumio. 1991. **Emerging patterns of innovation**: sources of Japan's technological edge. Boston: Harvard Business School Press.

MARTIN, James. 1991. **Engenharia da Informação – Introdução**. Editora Campus. Rio de Janeiro.

MASLOW, Abraham H. 2001. **Maslow no gerenciamento**. Reio de Janeiro: Editora Qualitymark.

**Revista Economia & Tecnologia – ISSN 1415-451X**  
**Vol. 8 – Fascículo 3 – P. 38-44 – Ano. 2005**

MORAES, Paulo Eduardo Sobreira. GUREK, Antonio Juliano de Moraes e PIERETTI, Sidinei. 2004. Resignificação de estratégia e estratégia financeira: um estudo de revisão bibliográfica. In: **Anais**. XVII Congresso Latino Americano de Estratégia. Balneário Camburiú-Itapema, 28 a 30 de Abril: Univali, no prelo.

MOTA, Antonio Gustavo da e AMORIM, Joaquim Armando Marques de. 2001. A empresa na economia do conhecimento. In: **Revista Uniandrade**, revista científica do Centro Universitário Campos de Andrade. Ano 2, Volume 2. Número 2 (12 de Junho). Páginas 59 a 74. Curitiba: Centro Universitário Campos de Andrade.

NBR ISO/IEC 17799. 2003. **Tecnologia da Informação**. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro.

PALADINI, Edson Pacheco. 2004. **Gestão da qualidade**: teoria e prática. São Paulo: Atlas.

REZENDE, Denis Alcides e ABREU, Aline França. 2000. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas.

PEDRO, Antonio. 1997. **História da civilização ocidental**: geral e Brasil, integrada. São Paulo: FTD.

SÁ, Antonio Lopes de. 2001. **Ética profissional**. São Paulo: Atlas.

SACCONI, Luiz Antonio. 1998. **Dicionário da Língua Portuguesa**, São Paulo: Atual.

SANDHU, Ravi S. e SAMARATI, Pierangela. 1994. **Authentication, Access Control, and Intrusion Detection**. IEEE Communications.

SÊMOLA, Marcos. 2003. **Gestão da Segurança da Informação – Uma visão Executiva**. Editora Campus. Rio de Janeiro.

SHIREY, R. RFC 2828. 2004. **Internet Security Glossary**. The Internet Society, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt?number=2828>. Acessado em: 08/04/.

SVEIBY, Karl Erik. 1999. **A nova riqueza das organizações**: gerenciando e avaliando patrimônios de conhecimento. São Paulo: Atlas.

WADLOW, Thomas. 2000. **Segurança de Redes**. Editora Campus. Rio de Janeiro.