Ano VI – Número 11 – Dezembro de 2006 – Periódicos Semestral

ADMINISTRAÇÃO DE SISTEMAS DE INFORMAÇÃO: OS DESAFIOS ÉTICOS DA TECNOLOGIA DA INFORMAÇÃO x SEGURANÇA

NAVARRO SANCHES BURGO, Rodrigo
Discente da Faculdade de Ciências Jurídicas e Gerenciais/ACEG.
E-mail: rodrigoburgo@gmail.com
YOSHIO TAMAE, Rodrigo
Docente da Faculdade de Ciências Jurídicas e Gerenciais/ACEG.
E-mail: rodrigo.tamae@uol.com.br

Informática

RESUMO

ADMINISTRAÇÃO DE SISTEMAS DE INFORMAÇÃO:
OS DESAFIOS ÉTICOS DA TECNOLOGIA DA INFORMAÇÃO x SEGURANÇA

Sistemas de informação, segurança e os desafios éticos da TI. Desenvolveram-se em razão da evolução do conhecimento humano, e tornaram-se temas muito discutidos por executivos e organizações de órgãos públicos ou privados, a preocupação com eles existe desde o século passado. Questionamentos são feitos quanto aos aspectos, necessidades, métodos, normas, políticas, controles e ética, o que motiva os gestores de segurança da informação buscarem conhecimento técnico e a aplicar mecanismos de gestão cada vez mais complexos e flexíveis, frente aos cenários dinâmicos e heterogêneos de todos os dias, com o único objetivo de proteger o bem maior, o ativo mais valoroso do século XXI, que é a informação.
Os mecanismos, recursos ou ferramentas da TI, implementados através do Plano Diretor de Segurança (PDS), trouxeram para o ambiente organizacional os desafios éticos da TI, afetando as tomadas de decisões, os negócios e os recursos humanos. O compartilhamento desse processo é feito através de treinamentos, divulgação e conscientização, iminente, a fim de flexibilizar a implementação da segurança da informação com os recursos da TI, cujo objetivo é contribuir para o melhor desempenho das organizações e dos profissionais.

Palavras-chave: métodos, normas, políticas, controles, ética, treinamentos, divulgação, conscientização.

Tema central: Segurança, Desafio Ético da TI.

ABSTRACT

ADMINISTRATION OF INFORMATION SYSTEMS:
ETHICAL TECHNOLOGY CHALLENGES OF THE INFORMATION x SECURITY

Information systems, security and the ethical challenges of IT. Developed itself because of the evolution of human knowledge, and has become a subject much discussed by executives and organizations, public agencies or private, concern exists with them since the last century. Questions are made on the issues, requirements, methods, standards, policies, controls and ethics, which motivates the managers of information security seek technical knowledge and

implement mechanisms for managing increasingly complex and flexible, Front of scenarios dynamic and heterogeneous, every day, for the sole purpose of protecting the greater good, the most active rich of century XXI, which is the information. The mechanisms, resources or tools of IT, implemented by the Director of Security Plan (PDS), brought to the environment organizational ethical challenges of IT, affecting decision-making, business and human resources. Sharing this process is done through training, dissemination and awareness, imminent, in order to easing the implementation of the information security with the resources of TI, whose goal is to contribute to the better performance of organizations and professionals.

Keywords: methods, standards, policies, controls, ethics, training, dissemination, awareness.

1. INTRODUÇÃO.

Com a revolução da informação e o crescente uso da Tecnologia da Informação nas organizações ampliaram a capacidade para adquirir, manipular e passar informações, através dos Sistemas de Informação que se tornaram extremamente importantes na estrutura organizacional, do nível estratégico até operacional.

Na realidade atual, que é dependente da informação, ativo de maior valor para as organizações, independente do segmento do negócio (seja comércio, Indústria ou financeira), a informação abre novos horizontes e mercados para a

expansão em busca de maiores lucros e perspectivas.

Existem diversos motivos para uma organização proteger suas informações, tornando-os importantes para o crescimento do negócio, assim como para os concorrentes, sabotadores, invasores, espiões, vários tipos de golpistas e/ou hackers não roubem suas informações.

2. SISTEMAS DE INFORMAÇÃO.

Sistemas de Informação é um conjunto de recursos, que coleta,

processa,armazena, analisa e dissemina as informações produzidas pelos departamentos da estrutura organizacional no apoio às decisões gerenciais e operacionais.

Os Sistemas de Informação desenvolveram-se rapidamente em razão da evolução do conhecimento humano, crescimento das organizações e a quantidade de dados no ambiente organizacional. O crescimento das organizações deve ser analisado, não apenas pelo aumento da produção, mercado e atividades, mas também pela diversificação e utilização de recursos tecnológicos mais complexos, alterando a execução dos processos, conforme o nível de complexidade e o grau de formalização das estruturas, que estão ligadas diretamente às características e ao estágio de desenvolvimento da organização.

A organização precisou organizar e estruturar seus dados, que são fatos ou descrições de eventos, atividades e transações capturadas, registradas, armazenadas e classificadas, que se desorganizadas perdem seu significado.

SI não deve ser entendido como sinônimo de TI, que é o conjunto de recursos tecnológicos facilitadores das atividades e processos organizacionais necessários para o tratamento das informações.

2.1 A ESTRUTURA DO SI.

A estrutura dos SI é fundamental, por ser essencial no ambiente organizacional para formar um conjunto dinâmico inter-relacionado utilizando os recursos e

componentes para processar dados em informações, que podem ser transmitidas como conhecimento para o nível estratégico e os usuários finais.

2.2 A IMPORTANCIA DOS SI NA ESTRUTURA ORGANIZACIONAL.

Os papéis vitais dos SI na estrutura organizacional proporcionam a essência do planejamento, a vantagem competitiva e o controle na tomada de decisões, nos níveis estratégico, tático e operacional, se o conteúdo for adequado e confiável. Portanto, quando os SI desenvolvem os principais papéis realizam conquistas de vantagens estratégicas, gerenciais e operacionais, mas isso requer inovação, dinamismo e investimentos, para conquistar vantagem competitiva no mercado e principalmente apoio do ambiente empresarial. Investimentos e inovação nos SI com recursos de TI requerem mais empenho dos recursos utilizados nos SI.

Sistemas mal administrados e mal aplicados têm mais chances de seguir para o fracasso do que para o sucesso tecnológico e comercial do próprio negócio. Identificar os objetivos e as razões seja de sucesso ou de fracasso é fundamental para o desenvolvimento dos SI que representam uma área funcional importante para o sucesso, assim como o marketing, a produção, as vendas e os recursos humanos.

2.3 OS TRÊS PRINCIPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO.

Hoje em dia é muito fácil atacar sistemas informatizados, visto que os SI estão conectados através das redes. Portanto, pode acontecer a perda de confidencialidade, quando informações caírem nas mãos da concorrência,

perda de integridade, quando as informações forem corrompidas ou apagadas, e perda de disponibilidade quando não puderem ser acessadas para o fechamento de um grande negócio. Isso caracteriza a segurança da informação pela preservação de:

Confidencialidade – garantia de que toda informação deve ser protegida, com certo grau de sigilo, acessível somente a pessoas autorizadas.

Integridade – visa proteger toda informação contra alterações indevidas, intencionais ou acidentais.

Disponibilidade – garantia de que toda informação e ativos estarão disponíveis e somente serão acessados por usuários autorizados no momento em que delas necessitem para qualquer finalidade.

2.4 PLANO DIRETOR DE SEGURANÇA.

O PDS é o planejamento e a elaboração de diretrizes, normas e procedimentos para controlar acessos aos dados e informações no ambiente organizacional.

O planejamento para implementar e manter a segurança nos SI deve ser enfatizado com importância e esforço para o seu desenvolvimento, algo que parece ser uma tarefa fácil ou desnecessária, para muitas organizações. No entanto, esse processo depende de toda organização da diretoria aos usuários finais, com os mesmos objetivos focados na melhoria constante dos SI. A efetiva gestão de segurança precisa ser permanente, cíclica, interativa e baseada em processo técnicos e organizacionais consistentes. Portanto, adotar um modelo corporativo de gestão permite à organização equacionar os desafios de proteção, levando em conta todos os aspectos essenciais para a

segurança: componentes dos ambientes físico e lógico, pessoas e processos. Na adoção do modelo de gestão, um método conhecido como PDCA (de plan, do, check, act) utilizado em processo de gestão da qualidade e outros níveis de gestão, é útil para fornecer uma visualização global das etapas que devem compor a gestão da segurança da informação.

O PDCA é basicamente:

P = Plan, de planejar: estabelecer objetivos,

metas e meios de alcançá-los.

D = Do, de executar.

C = Check, de verificar, avaliar (comparação

do executado com o planejado).

A = Act, de agir corretivamente (caso sejam

detectados desvios ou falhas a serem

corrigidos).

A elaboração de um modelo de gestão de segurança deve levar em consideração, em primeiro plano, os desafios do negócio como um todo, abrangendo todos os conceitos de segurança: confidencialidade, integridade, disponibilidade e os aspectos de autenticidade e legalidade.

3. CONSIDERAÇÕES FINAIS.

A evolução da informação, o desenvolvimento e a implementação de SI e dos recursos da TI proporcionam às organizações, profissionais, usuários e a sociedade maior capacidade para ampliar, adquirir, manipular e comunicar informações referentes aos negócios, vida profissional e pessoal de todos.

Os SI tornaram-se importantes nas estruturas organizacionais, contribuindo com o gerenciamento e a classificação das informações úteis nas tomadas de decisões estratégicas, táticas e operacionais no desenvolvimento dos negócios. Esse contexto motivou as organizações a divulgarem e compartilharem informações e resultados do processamento dos dados coletados importantes ao segmento do negócio.

Um dos desafios das organizações foi adotar e programar métodos para garantir a segurança da informação que é um conjunto de diretrizes, normas e procedimentos aplicados em todos os movimentos do ciclo de vida da informação de acordo com o negócio desenvolvido. Esse desafio exigiu melhor planejamento dos gestores de toda estrutura organizacional e a elaboração do PDS, que estabelece os tipos de controles a serem implementados no SI e as PSI a serem seguidas no processamento dos dados e gerenciamento da informação.

No entanto a simples criação de normas ou implantação de ferramentas de segurança não é suficiente para minimizar os riscos de incidentes de segurança (ataques, vazamento de informação, infestação por vírus, etc.), e sim a adoção de um completo processo de gestão da segurança, dinâmico e participativo que inclui a definição de responsabilidades de todos os elementos envolvidos no processo da informação com base na política de segurança.

As metodologias de segurança da informação devem ser adotadas considerando as normas, processos e características técnicas e não técnicas

da segurança dos sistemas para seu manuseio e proteção. Porém, muitas organizações têm ignorado o valor de suas informações, a necessidade de manter a metodologia de segurança e até mesmo de investimento, por considerarem estas despesas que não trarão retorno sobre investimento, visão que não contribui com eficácia para a gestão da informação, maior ativo das organizações.

A falta de critérios, planejamento e investimentos nos recursos dos SI, na admissão, treinamentos e sensibilização dos profissionais e usuários finais, têm

causado grandes prejuízos às organizações de diferentes segmentos no mercado.

Essa necessidade também tem criado desafios éticos para as organizações que adotam metodologias de segurança e recursos da TI com objetivos de Garantir a segurança das informações. As dimensões éticas devem ser consideradas pelas organizações na elaboração e implementação da metodologia de segurança, atenuando os efeitos nocivos da TI, analisando os aspectos da segurança e as vulnerabilidades existentes na estrutura tecnológica dos sistemas de informação.

4. REFERÊNCIAS BIBLIOGRÁFICAS.

MANÁS, Antônio Vico. **Administração de sistemas de informação**. São Paulo: Érica, 1999.

GIL, Antônio de Loureiro. **Segurança em informática**. 2. ed. São Paulo: Atlas, 1998.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: tecnologia da informação - código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2001.