

	<i>Artigo</i>	PÚBLICO
---	---------------	---------

Fatores Críticos para o Sucesso da Certificação ISO 27001

Porto Alegre, 29/10/2008. Quando falamos em Segurança da Informação, imediatamente nos vem ao pensamento o imenso universo de Yotta Bytes ($MB=10^6$, $YB=10^{24}$) digitais compostos pelos dados operacionais da empresa. E não estamos totalmente equivocados quanto a isto, pois é neles que estão registrados o histórico de negócios, os resultados financeiros e as evidências do cumprimento de obrigações da organização.

Mas esses dados digitais, na maioria dos casos, já se encontram razoavelmente protegidos, muitas vezes por sugestão ou requisitos dos próprios fabricantes do hardware e software utilizados, sendo que, o tratamento de possíveis ameaças ou vulnerabilidades pós-existentes, é apenas uma questão de investimentos em instalações e tecnologias adequadas.

Além disto, a segurança da informação digital e seus meios de processamento, ao longo dos últimos anos, tem sido objeto de várias normatizações específicas e abrangentes, internacionalmente aceitas, tais como ITIL (Information Technology Infrastructure Library) - um apanhado das melhores práticas de TI reconhecido desde 1990, COBIT (Control Objectives for Information and related Technology) - um framework de referência para a gestão de TI surgido em 1996 - e a BS 7799, homologada em 2000, hoje ISO 27001. Remanescem, porém, ameaças menos prováveis mas de conseqüências, muitas vezes, devastadoras como ações radicais do homem (New York – World Trade Center – 2001) ou fenômenos naturais catastróficos (New Orleans – Furacão Katrina – 2005).

Segurança da Informação, porém, não se aplica exclusivamente aos sistemas e equipamentos de informática, mas também, e talvez mais criticamente, às formas escrita e falada de registro e transmissão das informações, às pessoas, suas relações, cultura e comportamentos.

Estes aspectos, embora bastante empíricos, representam uma fragilidade significativa às informações estratégicas e confidenciais da organização, pois dependem exclusivamente de confiabilidade do corpo funcional, de sua conscientização e comprometimento.

Primeiramente, vemos na consistência do processo de recrutamento e seleção, através da definição detalhada de qualificações e competências desejadas para cada cargo, análise e verificação criteriosa de informações curriculares e de recomendação e na comprovação de idoneidade civil e criminal dos candidatos, uma ação preventiva, em prol da garantia de sigilosidade, devendo ser formalizada no ato da contratação dos servidores, através de termos de conhecimento e comprometimento de responsabilidades para com as formais políticas da organização.

Além disso, a organização deve publicamente expressar sua política de segurança da informação, envolvendo seus fornecedores, clientes e colaboradores, em um processo contínuo de conscientização, compromisso e adequação organizacional.

	<i>Artigo</i>	PÚBLICO
---	---------------	---------

Neste aspecto, a adoção de metodologias organizacionais tais como House Keeping (Programa 5Ss), além de minimizar desperdícios, propicia mudanças comportamentais pela indução de boas práticas tais como, cada coisa em seu lugar, mesa limpa e tela limpa.

Em empresas que ostentam Certificações de Qualidade, como ISO 9000, observa-se um amadurecimento desses processos organizacionais, nos quais a classificação e cuidados com documentos passaram a ser prática diária e natural das atividades laborais, assim como a formalização procedural e normativa de seus processos, gerando uma documentação inequívoca dos desejos, permissões e determinações da alta direção da organização.

A existência destes recursos contribuem significativamente para o processo de estabelecimento de um SGSI – Sistema de Gestão de Segurança da Informação, requisito base da norma ISO 27001, cujo objetivo é garantir a integridade, confidencialidade e disponibilidade da informação, cabendo a organização então, definir os limites (escopo) em que sua avaliação será aplicada, iniciando um processo contínuo de verificação de impacto no negócio (BIA - Business Impact Analysis), analisando os Riscos dentro de uma relação direta entre Impacto x Exposição, definindo controles para sua mitigação e definindo seus níveis de aceitabilidade residual, adequados à importância de cada processo de negócio.

Este processo de otimização organizacional, como podemos perceber, é um bom caminho para a implementação da Segurança da Informação, onde a aderência a norma específica ISO 27001 funciona como um instrumento verificador de eficiência e eficácia, num ambiente dinâmico, de constante mutação, exigindo para sua manutenção, um trabalho dedicado de melhoria contínua.

Régis E. S. Aguiar. Consultor Sênior Associado da e-trust, Administrador de Empresas e Contador, Auditor Líder ISO27001 e ISO9000, atuou como gestor da segurança da informação na primeira certificação na norma ISO27001 no ramo metal-mecânico no Brasil.