Área temática:

Política e Gestão Tecnológica

Título:

Segurança da Informação no Setor Cultural: Estudo de Caso do Instituto Itaú Cultural

AUTORES
IVAN ROBERTO FERRAZ
Universidade Presbiteriana Mackenzie
ivanferraz@hotmail.com

ROBERTO SANCHES PADULA
Pontifícia Universidade Católica de São Paulo
roberpa@uol.com.br

Resumo

Este artigo aborda a Segurança da Informação no setor cultural, em especial a questão dos riscos tecnológicos, por meio de um estudo de caso elaborado a partir da experiência de uma entidade sem fins lucrativos, o Instituto Itaú Cultural. A política de segurança adotada pelo instituto foi herdada de seu mantenedor, o banco Itaú, um dos maiores bancos privados do Brasil.

O estudo de caso é embasado por uma breve revisão bibliográfica que abrange o uso de tecnologia e segurança da informação nos setores financeiro, no qual se insere o banco Itaú, e cultural, onde atua o instituto.

Este artigo mostra que mesmo uma organização que não visa o lucro deve buscar minimizar os riscos tecnológicos provenientes da utilização de tecnologia no desempenho de atividades meio ou atividades voltadas ao negócio da instituição, que no caso estudado são o fomento, articulação e produção de arte. Por outro lado, as medidas adotadas não devem interferir no cumprimento de sua missão.

Por fim, são discutidos os impactos indesejáveis que podem ocorrer ao adotarmos uma política de segurança rígida em uma instituição onde a cultura organizacional exige flexibilidade e onde o objetivo final não é a obtenção do lucro.

Abstract

The approach of this article is the Information Security in the cultural sector, particularly the technology risks involved. It is a case study elaborated from the experience of a non-profit organization called Instituto Itaú Cultural. The institute's security politics was inherited from the Itaú bank, one of the biggest private banks of Brazil, which maintains the institute.

The case is based on a brief bibliographical revision that contains the use of technology and information security in the financial sector, where the Itaú bank acts, and cultural, where acts the institute.

This article shows that even an organization that does not look for profit must be worried in minimizing the technology risks that came from the use of technology in

administrative activities or in activities related to the business of the organization, in this case study, the promotion, joint and production of art. On the other hand, the adopted rules should not interfere with the fulfillment of institution's mission.

Finally, this article tells the impacts that may occur when adopting rigid security politics in an institution where the organizational culture demands flexibility and where the final objective is not the profit.

Palavras chaves

Segurança da Informação, Tecnologia da Informação, Terceiro Setor

Introdução

A tecnologia da informação (TI) está cada vez mais presente no dia a dia de qualquer organização, seja para automatização de seus processos internos, ou para manter sites na Internet, entre outras possibilidades. Mas, na mesma proporção em que se desenvolve a dependência das empresas pelos recursos de TI, cresce também a preocupação com a segurança da informação, por conta da quantidade de vírus existentes, ataques de hackers, sites falsos, roubos de informação, etc. que acabam por impactar o bom funcionamento e a boa imagem da organização.

Há diversos motivos para investir em segurança. Segundo SÊMOLA (2003), a organização pode visar o fortalecimento e valorização da marca, redução de custos, ou ainda pode estar interessada na conformidade com leis e padrões, em certificações internacionais, em uma grande campanha de marketing ou na legítima vontade de estar preparada para suportar projetos futuros. Esses motivos variam em função do setor do negócio, cultura organizacional, disponibilidade de verbas e estratégias de cada empresa. Dessa forma, a necessidade de proteger informações de uma empresa sem fins lucrativos é diferente quando comparada à necessidade de uma organização que visa o lucro.

Este artigo apresenta um estudo de caso que aborda a experiência do Instituto Itaú Cultural, entidade sem fins lucrativos atuante no setor da cultura, mantida pelo banco Itaú, um dos maiores bancos privados do Brasil. A discussão sobre a segurança da informação e riscos tecnológicos no terceiro setor ainda é recente. A escolha deste instituto como protagonista do estudo de caso deve-se a sua política de segurança, herdada da entidade mantenedora. Para uma instituição financeira como o banco Itaú, normas rígidas de segurança são essenciais na manutenção de sua credibilidade no mercado.

O artigo inicia com uma breve análise sobre a utilidade da TI no setor financeiro e no cultural, sobre a aplicação de medidas de segurança da informação em ambos os setores, e é concluído com a apresentação dos impactos que uma política de segurança da informação voltada a uma instituição financeira pode trazer quando aplicada em uma instituição cultural, identificando a importância de se desenvolver regras e normas que garantam a segurança necessária, mas que ao mesmo tempo estejam alinhadas com o negócio e cultura da empresa, não importando a qual setor da economia ela pertença.

Metodologia

Este trabalho é um estudo de caso da experiência do Itaú Cultural no desenvolvimento de sua política de segurança da informação. O estudo foi elaborado a partir de documentos, normativas e registro de reuniões, que possibilitaram verificar o impacto da política de segurança do banco mantenedor quando aplicada no instituto. Foram também realizadas pesquisas em livros, periódicos e sites especializados que contribuíram para delinear um

quadro teórico e um levantamento preliminar de alguns problemas que podem ocorrer na transferência de procedimentos de uma instituição para outra.

A TI na Indústria Bancária

Dada a característica do serviço bancário, que exige uma série de cálculos sobre uma grande quantidade de dados, a informática passou a ser essencial para os bancos desde os anos 70, em virtude dos grandes volumes de transações realizadas, da grande quantidade de serviços oferecidos aos clientes e da criticidade de grande parte das operações, sem contar a necessidade de controles, internos e externos, e conseqüente mitigação de riscos.

Além desses motivos, os investimentos em TI se justificaram ao longo do tempo para um ganho de vantagem competitiva frente aos concorrentes. Segundo MILLAR apud PIRES, MARCONDES (2004), as regras da competição foram alteradas pelo advento da TI. PORTER apud PIRES, MARCONDES (2004) acrescenta que a vantagem provém da inovação e aperfeiçoamento, gerada por uma direção estratégica visionária.

Pesquisas da FEBRABAN – Federação Brasileira de Bancos (2004) indicam que os bancos investiram 4,2 bilhões de reais em melhorias da TI no ano de 2003, sendo esse valor correspondente a 35% do total aplicado em TI pelos bancos (11,5 bilhões de reais). De acordo com uma pesquisa da FGV-SP, as médias e grandes empresas gastam em tecnologia o equivalente a 4,9% do seu faturamento líquido por ano, enquanto o segmento bancário gasta uma média de 10,4%. O setor financeiro foi responsável por 23% dos investimentos em TI no Brasil em 2004.

A TI no Setor Cultural

Assim como qualquer organização, as Instituições Culturais utilizam a tecnologia no seu dia a dia para automatização de processos, ganhando rapidez e eficiência na execução de tarefas administrativas. Além disso, essas Instituições também fazem uso da tecnologia para a difusão de suas atividades via Internet e os artistas a usam como suporte, meio de produção, para criação de suas obras.

A Internet é usada primeiramente para divulgação das atividades da instituição, onde estão colocados fotos, textos, áudio e vídeos digitalizados. Podem ser incluídos nessa categoria os museus ou exposições virtuais, ou seja, que não estão ou não estiveram em instalações físicas. Inclui-se, ainda nesse caso, a utilização da Internet para transmissão de eventos, como shows, seminários, etc., com a finalidade de alcançar um maior público e criar comunidades digitais (PRADO, 2003)

A rede mundial também é utilizada para uma participação compartilhada, através de bancos de dados ou programas gerados pelos artistas, na qual os ‘espectadores’ têm uma interface para manipulação ou para ação conjunta. Há casos em que são usadas interfaces físicas (câmeras, teclados, mouses, etc.) em locais físicos e outras interfaces lógicas, por estarem distantes, manipuladas pelo terminal do usuário em sua residência.

Segundo SANTAELLA (2004), há diversas variações, como sites interativos, site colaborativos, sites que integram os sistemas de multi-agentes para execução de tarefas, sites que convidam o usuário a adotar uma identidade (avatar), levando a imersão em realidade virtual, através de interfaces perceptivas e sensórias. A arte depende de suportes, dispositivos e recursos, diz a autora. Nesses meios é que se dá tanto a produção, como a exposição ou difusão.

“Os intercâmbios artísticos em rede abrem uma área de ‘jogo’; um espaço social lúdico que acentua o sensível e as estratégias de partilha, mas que procura articular no trabalho artísticos as experiências do indivíduo confrontado com uma realidade complexa e

em movimento, com a desordem do mundo e a de cada um, em particular", coloca PRADO (2003). Os primeiros trabalhos de arte em rede, nas décadas de 70 e 80, eram instalados em pequenas redes internas, montadas somente para o evento onde a obra se encontrava exposta. Ou seja, essa rede era efêmera, com poucos usuários ("grupo de participantes"), e sem nenhuma conexão com outras redes. Com o advento da Internet, abriu-se a possibilidade de haver redes permanentes, com público em qualquer lugar do mundo.

SANTAELLA (2004) diz que "na tradição dos eventos de telecomunicações, aparecem, via rede, os eventos de telepresença e telerrobótica, que nos permitem visualizar e mesmo agir em ambientes remotos, enquanto se espera pelo advento da teleimersão e, com ela, da promessa da ubiqüidade que se realizaria quase inteiramente não fosse pelo fato de que o corpo tridimensional teleprojetado será incorpóreo, impalpável. Em ambos os casos, nas ciberinstalações e nos eventos de telepresença, tanto o mundo lá fora passa a se integrar ao mundo simulado por meio de trocas incessantes, quanto o receptor passa a habitar mentalmente o mundo simulado enquanto seu corpo físico se encontra plugado para permitir a viagem imersiva, algo que a metáfora do filme Matrix soube ilustrar à perfeição".

Segurança da Informação

A informação deve ser considerada um ativo da empresa e seu correto gerenciamento é fundamental para o sucesso de qualquer organização. Devido à sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitados (CACIATO, 2004).

A segurança da informação busca a preservação de 3 princípios básicos por meio dos quais sua implementação é norteada. São eles:

Confidencialidade: "Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas" (SÊMOLA, 2003).

Integridade: "Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais" (SÊMOLA, 2003).

Disponibilidade: "Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade" (SÊMOLA, 2003).

As medidas de segurança que visam preservar esses três princípios podem ser classificadas, em função da maneira como abordam as ameaças, em duas grandes categorias definidas por SILVA, CARVALHO e TORRES (2003) como:

- Prevenção: é o conjunto das medidas que visam reduzir a probabilidade de concretização das ameaças existentes.
- Proteção: é o conjunto das medidas que visam dotar os sistemas de informação com capacidade de inspeção, detecção, reação e reflexo, permitindo reduzir e limitar o impacto das ameaças quando estas se concretizam.

A segurança é um processo em permanente evolução, mutação e transformação, que deve envolver todos os níveis da empresa e ser encarada como um facilitador e como forma de aumentar os níveis de confiança internos e externos (SILVA, CARVALHO e TORRES, 2003).

Dessa forma, a segurança da informação, e conseqüentemente dos sistemas de informação, não envolve apenas fatores tecnológicos; para SILVA, CARVALHO e TORRES (2003), ela engloba um número elevado de disciplinas, dentre elas: segurança de redes, segurança física, segurança do pessoal, gestão de projetos, formação, conformidade, etc.

Entretanto, ao falar em proteção à informação, os fatores relacionados à tecnologia são sempre os mais lembrados. Segundo estudo realizado pela empresa ERNST & YOUNG em 2003, que questionava as empresas entrevistadas sobre os tipos de investimentos relativos à proteção da informação, cerca de 83% das inquiridas apontaram a tecnologia como o principal investimento nos seus orçamentos de proteção da informação, enquanto apenas 29% afirmaram que a maioria do seu orçamento nesta área é gasto em formação e conscientização dos seus colaboradores.

Para MAIA (2005), a gestão de riscos deve ser focada em tecnologia, ambiente, processos e pessoas para que sejam adquiridos elementos que facilitarão o direcionamento dos investimentos em segurança.

Todavia, estimar um risco, atribuindo valores à sua probabilidade e conseqüências, não é uma tarefa fácil, principalmente porque além dos dados insuficientes, os parâmetros utilizados não são muito concretos (FONTES, 2001).

Sendo assim, um projeto de segurança da informação possui um alto grau de incerteza quanto ao seu retorno, de forma que um projeto de novos produtos, com alto grau de certeza, teria muito mais facilidade em justificar o investimento necessário.

A relação custo / benefício traduz a necessidade de garantir uma relação favorável entre os gastos associados à implementação de medidas de segurança e o retorno em matéria de prevenção e proteção. Embora assente no senso comum, este princípio é freqüentemente esquecido, sendo normalmente considerados apenas os custos ou os benefícios isoladamente (SILVA, CARVALHO e TORRES, 2003).

De acordo com pesquisa realizada pela empresa ERNST & YOUNG (2003), 60% das empresas pesquisadas afirmaram que, raramente ou nunca, calculavam o retorno de investimento como parte do seu business case para investimentos em segurança da informação.

SÊMOLA (2003) lembra que não podemos ignorar outros valores, que não apenas o financeiro, capazes de apoiar a justificativa de investimentos em segurança. Ele afirma que a organização pode visar o fortalecimento e valorização da marca, redução de custos, ou ainda pode estar interessada na conformidade com leis e padrões, em certificações internacionais, em uma grande campanha de marketing ou na legítima vontade de estar preparada para suportar projetos futuros.

FONTES (2001) acrescenta que algumas vezes a segurança da informação, ao invés de ser encarada como um investimento, deve ser vista como um custo operacional, uma vez que a sua ausência pode representar um sério risco para o negócio da organização.

Segurança em Instituições Financeiras

A segurança está relacionada à credibilidade e, para uma instituição financeira, a credibilidade é fundamental na conquista e manutenção de clientes.

Por esse motivo, os bancos brasileiros gastam anualmente mais de US$ 1 bilhão em segurança física de suas agências (FEBRABAN, 2005). Entretanto, as preocupações com segurança vão muito além das questões físicas. Com o estreitamento do mercado, a necessidade de se manter competitivo e a crescente demanda por serviços mais eficazes, os bancos viram a automação bancária como parte da solução para sobreviver neste mercado cada vez mais competitivo (SÊMOLA, 1999).

Com o desenvolvimento da automação, cresceram também os riscos tecnológicos e a preocupação com a segurança digital. Uma pesquisa realizada por St. Paul Companies com aproximadamente 1500 executivos nos Estados Unidos e Europa identificou que para as instituições financeiras, o risco tecnológico é atualmente o mais importante (MACSWEENEY, 2001).

Segundo a FEBRABAN (2005), a complexidade e alcance das fraudes parecem acompanhar a especialização tecnológica do sistema bancário. A quantia perdida por meio da fraude e o gasto necessário para combatê-la representam um alto custo para a sociedade.

Para que todos os esforços e investimentos em segurança sejam bem sucedidos, é essencial que as empresas assimilem as novas regras de segurança, transformando-as em parte integrante da sua cultura, incorporando-as às atividades de seu cotidiano com naturalidade. Neste sentido, as instituições financeiras costumam desenvolver uma política de segurança corporativa bastante rígida, com controles e processos rigorosos, diretrizes e orientações claras, objetivas e adequadas que ajudam a minimizar os riscos e reduzir o impacto sobre o negócio (SÊMOLA, 1999).

Segurança da Informação no Setor Cultural

Até mesmo uma instituição sem fins lucrativos pode ser vítima de uma ação criminosa. Por mais altruísta que seja sua missão, ela não oferece proteção, tão pouco imunidade. Portanto, toda instituição cultural deve estar atenta aos riscos operacionais e àqueles ligados ao negócio da empresa.

Conforme descrito no item “A TI no Setor Cultural”, tal instituição pode fazer uso da tecnologia para diversos fins, trazendo inúmeras vantagens para a organização. Porém, os benefícios adquiridos com o uso da tecnologia, como agilidade e eficiência, servem igualmente à ação criminosa (DONEY, 2001).

O responsável pelo gerenciamento de riscos em uma instituição cultural provavelmente estará mais atento aos riscos considerados tradicionais como, por exemplo, o desrespeito aos direitos autorais de determinada obra. Com isso, os riscos que envolvem o uso de tecnologia podem não ser notados tão facilmente. Segundo o NONPROFIT RISK MANAGEMENT CENTER (2001), o terceiro setor não despende atenção suficiente aos riscos associados a fatores tecnológicos. Afirma ainda que toda organização deveria considerar como os riscos tecnológicos podem impedir que sua missão seja atingida. O objetivo final do gerenciamento de riscos em uma instituição que não visa o lucro é liberar recursos para as atividades que são críticas ao desempenho da missão.

Não há estudos que apresentem estatísticas confiáveis sobre a atividade criminosa nesse setor, de forma que não é possível estimar os custos aplicados e prejuízos acumulados.

O caso do Instituto Itaú Cultural

O Instituto Itaú Cultural é uma organização sem fins lucrativos mantida pelo grupo Itaú que tem por objetivo incentivar e promover a produção cultural, a formação do produtor cultural, a comunicação cultural e a preservação do patrimônio cultural do País, em atuação direta e de forma associada.

A tecnologia tem sido vista com muita ênfase na estratégia e modo de ser do banco Itaú, de forma que se entende como incorporada em sua cultura. Sua missão, inclusive, a menciona: “Ser o Banco líder em performance, reconhecidamente sólido e confiável, destacando-se pelo uso agressivo do marketing, tecnologia avançada e por equipes capacitadas, comprometidas com a qualidade total e a satisfação dos clientes”.

Desde a década de 60, o banco usa computadores mainframe IBM para suas operações. Alguns processos já começavam a ser automatizados no Brasil, por iniciativa do próprio Itaú que introduziu o uso de cheques magnéticos. Na década de 70, a área de processamento de dados tinha cinco mil funcionários, entre perfuradores, analistas, programadores e outros.

No final da década de 70, o grupo Itaú criou a empresa de tecnologia chamada Itautec. Sua primeira missão foi desenvolver hardware, software e aplicativos para automatização das agências, com terminais eletrônicos substituindo as antigas máquinas de calcular e certificar. Era o início do processamento on-line das informações de contas-correntes, instalado na primeira agência em 1982.

O banco Itaú passou a ser conhecido pelos slogans 'Banco Eletrônico Cinco Estrelas', 'Pronto para o Futuro' e 'o Banco da Era Digital', enfatizando a imagem do uso da tecnologia em benefício dos clientes. O seu site de home-banking, Bankline, e sua ATM, Caixa Eletrônico Itaú, são reconhecidos no mercado por sua excelência.

Com a publicação da resolução 2054 do Banco Central, de 1998, sobre a necessidade de implementação de rígidos controles internos, o Itaú introduziu normas e procedimentos mais abrangentes que a própria resolução oficial, colocando grande ênfase na segurança da informação. Com isso, reduziu, entre outros, os principais riscos provenientes do uso da TI.

Fortemente presente na cultura do banco, a preocupação com a excelência e o pioneirismo em tecnologia nos diferentes negócios em que a empresa atua se estende também aos projetos que o grupo empreende na área cultural.

Assim, uma das premissas que motivaram a criação do instituto cultural que leva a marca do banco no nome, certamente é a idéia de reunir os conceitos de cultura e arte com tecnologia. Essa relação está explicitada na definição da missão do Instituto e pode ser claramente observada na sua atuação cultural. Sua missão é: “Fomentar, articular e difundir ações que contribuam para o conhecimento, produção e distribuição dos bens culturais, especificamente das artes, no Brasil, enfatizando a utilização das novas tecnologias para ampliar a circulação desses bens e o seu acesso, colaborando assim com o processo de participação social”.

O instituto abriu no final dos anos 80 como Centro de Informática e Cultura, onde eram disponibilizadas biografias e imagens digitalizadas sobre Pintura no Brasil. Era possível imprimir as imagens em impressoras de alta definição. O Banco de Dados Informatizado foi acrescido com a memória fotográfica da cidade de São Paulo. No ano 2000 foi criada a Enciclopédia Itaú Cultural de Artes Visuais, uma evolução deste Banco de Dados, agora disponível na Internet. Em 2002 foi criado o Itaulab, laboratório de mídias interativas do Itaú Cultural, um centro de pesquisa para produções acadêmicas e artísticas, cujos objetivos são a troca de experiências com instituições acadêmicas e a pesquisa utilizando os recursos das novas mídias aplicadas às áreas artísticas e educacionais.

Uma instituição cultural, em uma cidade tão grande como São Paulo, precisa de estratégias para melhor difundir suas atividades, que não devem estar restritas às suas instalações físicas. O instituto, localizado na principal avenida da cidade, onde passam milhares de pessoas diariamente, recebe um grande número de visitantes todos os dias, composto por aqueles que trabalham na região, por pessoas atraídas pelas atividades divulgadas nos roteiros culturais dos jornais e revistas, ou por grupos de estudantes de escolas que agendaram visitas. Dessa forma, o prédio já atinge com facilidade sua lotação máxima. Portanto, se a missão é difundir ao máximo a arte e cultura brasileira, novos meios têm de ser usados para facilitar essa difusão.

A tecnologia se encaixa bem nessa tarefa, seja transmitindo espetáculos, debates ou seminários via rádio e TV, seja transmitindo cursos e congressos via Internet, ou ainda com um site institucional que possibilite visitas virtuais a exposições ou acesso a conteúdo resultante das atividades.

O uso de tecnologia traz consigo a exposição a diversos riscos tecnológicos que devem ser minimizados por meio de uma política de segurança adequada. O banco moldou sua política de segurança de acordo com sua cultura, que visa à redução dos riscos e manutenção da credibilidade da organização no setor financeiro. Esta mesma política foi transferida para o

Itaú Cultural que, apesar de sofrer influência de seu mantenedor, possui cultura organizacional própria, por se inserir em setor distinto.

Cultura organizacional é um padrão de pressupostos básicos compartilhados que um grupo aprendeu ao resolver seus problemas de adaptação externa e integração interna e que funcionaram bem o suficiente para serem considerados válidos e ensinados a novos membros como a forma correta de perceber, pensar e sentir com relação a esses problemas (SCHEIN, 1992). Segundo o autor, o fenômeno de "cultura" é aprendido essencialmente a partir de dois mecanismos interativos: 1) redução do estado de ansiedade e dor – o modelo de trauma social; e, 2) o reforço e recompensa positiva – o modelo de sucesso. Este tipo de cultura fortemente estabelecida obtém-se a partir do compartilhamento de uma vivência, de um histórico, e não a partir de decisões gerenciais.

Sendo assim, a implementação de uma política de segurança própria do setor financeiro e adequada à cultura do banco pode trazer impactos inesperados quando aplicada em uma instituição que atua no setor cultural.

Políticas de Segurança do Banco e seu Impacto no Instituto

O banco Itaú, por ser extremamente comprometido com a questão de segurança, possui diversas normas e procedimentos que garantem o bom gerenciamento dos riscos. Esta preocupação estende-se ao Instituto Itaú Cultural, que, apesar de não ser do setor financeiro, é mantido pelo banco. Um ataque ao site do instituto, por exemplo, pode oferecer riscos à imagem do mantenedor e ser associado a uma fragilidade da empresa como um todo, para o qual a segurança é um atributo essencial a ser preservado. Este tipo de ataque poderia gerar conseqüências muito mais graves para o banco do que para o próprio instituto, visto que a marca Itaú está associada ao site cultural.

Por conta disso, o instituto acaba por incorporar uma política de segurança que não é própria de sua área, e que pode interferir em alguns processos internos ou, ainda, dificultar relacionamento com outros agentes culturais, que certamente não têm a mesma preocupação em segurança.

Ambas as instituições analisadas utilizam a TI como ferramenta para automatizar processos internos. No caso do banco estão envolvidas, por exemplo, áreas burocráticas focadas na produção, nas rotinas padrão, onde os funcionários não devem ter acesso a e-mail, mensagens instantâneas e sequer acesso à Internet para que sua produtividade seja a máxima possível. Outras áreas trabalham com informações altamente sigilosas, como dados de clientes, dados contábeis do banco, informações estratégicas, de forma que os funcionários devem ter grande restrição à saída de informação, e por isso não podem ter gravador de CD, drive de disquete, saídas USB, ou acesso a e-mail externo. No caso do instituto, existem áreas análogas a essas do banco, mas das quais não pode ser exigida uma produtividade tão grande, pela particularidade dos processos, ou áreas que tratam informações sigilosas, mas menos visadas por terceiros, portanto, menos valiosas.

Outro uso comum da TI é a disponibilização de sites na Internet. Os de bancos contemplam, em geral, a possibilidade de efetuar transações on-line (home banking), como também informações sobre a conta corrente, investimentos, produtos e serviços; notícias financeiras; e informações institucionais. Os principais riscos são quanto a ataque de hackers, que afetem a imagem de uma instituição segura, tanto na possibilidade de roubo de senha ou dados de clientes, quanto na possibilidade de mudança de conteúdo ou em tentativa de tornar o site indisponível. Já os sites de institutos culturais na Internet têm como conteúdo, tipicamente, informações sobre eventos (programação); informações sobre os produtos e serviços; matérias, textos, imagens, etc; notícias culturais; consulta em bancos de dados culturais, biblioteca; transmissão de eventos ao vivo; obras de arte-tecnologia on-line; e

informações institucionais. Os riscos a que esses sites estão expostos são basicamente quanto a ataque de hackers, que afetem a confiabilidade do conteúdo do site ou prejudiquem a imagem de seus mantenedores, e quanto à cibernautas que copiem textos ou imagens para uso particular, que podem expor o instituto a problemas de direitos autorais.

No setor cultural, temos ainda o caso específico de arte-tecnologia, com obras que se realizam na interface entre vários usuários via rede, e a segurança pode ser um inibidor que acabe por invalidar e inviabilizar o conceito utilizado pelo artista. É difícil saber se há como determinar a segurança necessária a uma obra de arte, e se isso não seria uma inferência no trabalho criativo do artista.

Como exemplos de medidas herdadas da política de segurança do banco e adotadas pelo instituto, podemos citar:

- Reestruturação da rede de computadores de forma a isolar a rede interna.
  - Motivo: minimizar os riscos e conseqüências de um ataque de hacker via Internet
  - Impactos gerados: inviabilização de algumas obras de arte-tecnologia
- Restrições quanto ao uso de disquetes, gravadores de CD, e-mail, mensagens instantâneas e portas USB
  - Motivo: inibir a saída de informações confidenciais
  - Impactos gerados: dificuldade na gravação de back-ups, transferência de arquivos e informações com pessoas de fora do instituto e na conexão de câmeras, scanners, etc.
- Monitoramento dos acessos à Internet com filtro a sites de conteúdo considerado inadequado
  - Motivo: evitar acesso do público e de funcionários a sites inadequados através da rede do instituto
  - Impactos gerados: dificuldade de acesso a sites importantes, classificados erroneamente como de conteúdo impróprio
- Padronizações de configurações de estações de trabalho
  - Motivo: impossibilitar que os usuários instalem softwares não certificados, incorrendo em problemas com vírus ou softwares piratas
  - Impactos gerados: dificuldade de visualização de sites, CD-ROMs ou obras de arte-tecnologia
- Burocracia em processos internos de criação de usuários e concessão de acessos a sistemas e diretórios
  - Motivo: limitar a quantidade de usuários, concedendo acessos somente a quem realmente necessita
  - Impactos gerados: falta de agilidade na execução de tarefas

Essas medidas também levam a um aumento de custos em tecnologia. No caso do banco, que é do setor privado, esse acréscimo se justifica pelo retorno financeiro esperado, em consonância com seu objetivo de gerar lucro aos seus acionistas. Para o instituto, uma organização do terceiro setor, o orçamento visa cumprir sua missão na arte e cultura, e nesse caso, pode ser difícil justificar o peso do custo dos investimentos em segurança comparado ao custo das atividades culturais.

Outra diferença decorrente das especificidades do setor no qual cada uma dessas organizações se insere, e que deve ser considerada, é relativa ao grau de restrições que funcionários e colaboradores estão predispostos a aceitar. Entende-se como normal um banco colocar restrições aos seus funcionários, pois está clara na cultura da empresa a necessidade de controle das atividades e limitações em função da segurança. Já em instituições culturais, seus colaboradores acreditam que devem ter maior liberdade de expressão, criação e troca de

informações, e assim, as restrições podem ser consideradas cerceadoras e limitadoras da qualidade do trabalho.

Considerações

O banco Itaú e o Instituto Itaú Cultural desenvolveram culturas organizacionais muito diferentes por conta dos setores no qual estão inseridos. Ao mesmo tempo, compartilham valores no caso da segurança da informação. Isso ocorre em função do relacionamento institucional entre eles e para atender as necessidades do banco mantenedor.

É certo que, como grande parte dos projetos desenvolvidos pelo instituto está associada à pesquisa e atividades em ambientes digitais, que trabalham com conceitos de interatividade via Internet ou redes locais, existe uma exigência específica de preservação da segurança destes ambientes. Sendo assim, muitas das medidas adotadas pelo instituto por transferência das políticas praticadas pelo banco mostram-se realmente necessárias.

Por outro lado, essa necessidade de controle coloca ao instituto uma questão sobre a liberdade que é exigida no mundo cultural e artístico, gerando uma preocupação sobre como conciliar as limitações impostas pelos cuidados com a segurança com a necessidade de troca e acesso a informações.

Para reduzir o impacto negativo que pode ser criado no instituto, as medidas devem ser coerentes com as necessidades de segurança e também com as atividades necessárias para que a organização cumpra sua missão. Por isso, um estudo específico sobre as necessidades e seus impactos deve fundamentar a decisão sobre quais medidas são efetivamente necessárias, buscando sempre uma alternativa que garanta maior flexibilidade e que esteja alinhada com a sua cultura e objetivos, evitando interferir no bom andamento das atividades culturais.

Referências Bibliográficas

BANCO CENTRAL DO BRASIL. Disponível em: <http://www.bcb.gov.br/>
Acesso em 17 Abr. 2005

BANCO ITAÚ. Disponível em: <http://www.itau.com.br>
Acesso em 17 Abr. 2005

CACIATO, Luciano Eduardo. *Gerenciamento da Segurança de Informação em Redes de Computadores e a Aplicação da Norma ISSO/IEC 17799:2001*. Monografia (Especialista em Análise de Sistemas). Campinas, 2004. Disponível em: <http://www.rau-tu.unicamp.br/>. Acesso em: 25 Abr. 2005.

CYPRIANO, Fábio. Decepção Artificial. *Folha de São Paulo*, São Paulo, 14 de agosto de 2004.

DONEY, Lloyd. Nonprofits Aren´t Immune to Computer Crime. *Nonprofit World*, Vol. 19, No. 2, p. 30 a 33, Março/Abril 2001. Disponível em: <http://nonprofitrisk.org/>. Acesso em: 25 Abr. 2005.

EMÍLIA, Andreza. *Banco é o setor que mais investe em tecnologia no Brasil*. Telecom & TI, 2004. Disponível em:
<http://noticias.aol.com.br/negocios/telecomunicacoes/2004/06/0003.adp>. Acesso em 17 Abr. 2005.

ERNST & YOUNG. *Proteção da informação é decisiva na estratégia de negócio das empresas*. Disponível em: <http://www.youngnetwork.net/>. Acesso em 20 Abr. 2005.

FEBRABAN. *Segurança: Um compromisso de bancos e clientes, em todo o mundo*. Disponível em: <http://www.febraban.org.br/>. Acesso em 18 Abr. 2005.

FEBRABAN. *Bancos gastam mais de US$ 1 bilhão em segurança*. Disponível em: <http://www.febraban.org.br/>. Acesso em 18 Abr. 2005.

FONTES, Edison. *Segurança da Informação: Investimento ou Custo Operacional?*. 2001. Disponível em: <http://www.securenet.com.br/>. Acesso em 19 Abr. 2005.

INSTITUTO ITAÚ CULTURAL. Disponível em: <http://www.itaucultural.org.br> Acesso em 16 Abr. 2005

MACSWEENEY, Greg. Technology Risk Still Not Understood. *Insurance & Technology*, 2001. Disponível em: <http://www.insurancetech.com/>. Acesso em 21 Abr. 2005.

MAIA, Marco Aurélio. Gestão de Riscos: o que avaliar?. *Módulo Security Magazine*, 2005. Disponível em: < http://www.modulo.com.br/>. Acesso em 19 Abr. 2005.

NONPROFIT RISK MANAGEMENT CENTER. *Full Speed Ahead: Managing Technology Risk in the Nonprofit World*. [S.I.: s.n], 2001. Disponível em: <http://nonprofitrisk.org/>. Acesso em: 25 Abr. 2005.

PIRES, Marcel Ginotti; MARCONDES, Reynaldo Cavalheiro. *A vantagem competitiva nas organizações financeiras: uma análise baseada na Teoria dos Recursos.* [S.I]: EMA/ANPAD, 2004.

PRADO, G.; LAURENTIZ, S. *Arte telemática: dos intercâmbios pontuais aos ambientes virtuais multiusuário*. São Paulo: Itaú Cultural, 2003.

SANTAELLA, Lúcia. *A Arte do Silício*. Disponível em: <http://www.itaucultural.org.br/>. Acesso em: 25 Abr. 2005.

SCHEIN, E. H. *Organizational Culture and Leadership.* 2. ed. San Francisco: Jossey-Bass Publisher, 1992.

SCHOTI, Camila. *Bancos: gastos com tecnologia totalizaram R$ 12,5 bilhões em 2004*. InfoMoney, 2005. Disponível em: <http://www2.uol.com.br/infopessoal/noticias/_HOME_OUTRAS_329130.shtml>. Acesso em 17 Mai. 2005.

SÊMOLA, M. *Gestão da Segurança da Informação – Uma visão executiva.* 3. ed. Rio de Janeiro: Elsevier, 2003.

SÊMOLA, Marcos. *Automação Bancária: e a segurança?*. 1999. Disponível em: <http://www.semola.com.br/>. Acesso em 19 Abr. 2005.

SÊMOLA, Marcos. *Preciso justificar os investimentos, mas como?*. 2003. Disponível em: <http://www.semola.com.br/>. Acesso em 19 Abr. 2005.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B**.** *Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial*. Portugal: [s.n], 2003. Disponível em: <http://www.centroatl.pt/>. Acesso em 20 Abr. 2005.

Intranet do Banco Itaú.
Acesso em 16 Abr. 2005.

Intranet do Instituto Itaú Cultural.
Acesso em 16 Abr. 2005.