



# Só proteger não basta

*As novas soluções de Segurança da Informação estão cada vez mais conectadas com as ações estratégicas das empresas*



POR ANDERSON GURGEL

**G**RANDES ESTRAGOS SOFRIDOS pela rede corporativa de uma empresa começam, às vezes, devido à simples curiosidade de um funcionário. Para atraí-la, criminosos virtuais utilizam-se de artifícios cada vez mais sedutores para convencer o internauta a baixar downloads e receber mensagens que, abertas, contaminarão as máquinas e derrubarão sistemas de se-

gurança da informação. Caso recente se deu após a tragédia ocorrida na Universidade Tecnológica da Virgínia (EUA), onde 32 pessoas foram mortas e 15 foram feridas pelo universitário Cho Seung-hui, de 23 anos. Mensagens que circularam pelo mundo, prometendo mostrar imagens da tragédia, trouxeram programas espíões, como o TrojanDownloader.Win32.Banload.ccm, que minam a segurança do sistema.



lembra que “envolver a segurança da informação apenas na última semana quando a nova estratégia já está prestes a ser lançada não é uma boa prática para organizações que desejam verdadeiramente esse alinhamento”. Outro ponto destacado por ele é a necessidade de se ter um nível hierárquico adequado, visto que essa área deve se reportar a um comando que possibilite a sua atuação sem sofrer restrições.

Ainda nas recomendações, o consultor de SI acrescenta que é fundamental conhecer o planejamento estratégico da empresa. “Se a organização pretende desenvolver produtos de forma descentralizada e precisa utilizar comunicação sem fio, por exemplo, é necessário que a área responsável por reduzir os riscos se antecipe, busque encontrar soluções e produtos que atendam a necessidade de negócio e sejam eficientes ao longo do tempo”, completa. Isso, para ele, tem tudo a ver com o planejar estrategicamente e de maneira alinhada com a redução de vulnerabilidades.

“A segurança existe por causa do negócio e deve ser adequada à forma de realização, respeitando a legislação, a conduta ética e as características da organização”, completa Fontes. Sendo assim, os responsáveis devem atentar para como fazer isso acontecer na prática. “Sem realizar esses esforços dolorosos, toda a estratégia de segurança da informação da empresa serão sacrifícios inúteis, como dar ‘murro em ponta de faca.’”

Um exemplo de iniciativas alinhando segurança à estratégia de negócios pode ser visto no amplo interesse dos bancos pela oferta de servi-



## TESTE A SINERGIA ENTRE SI E NEGÓCIOS

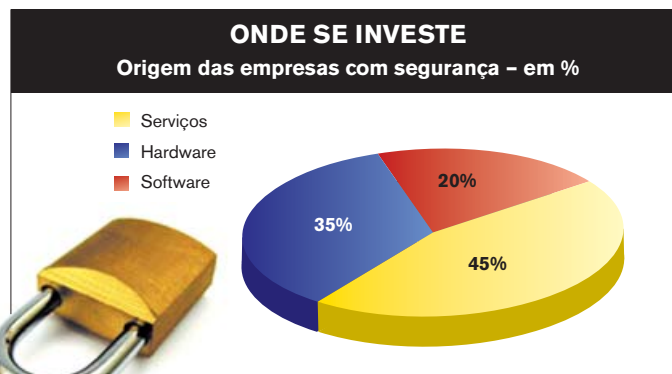
- 1) Verifique se em sua empresa a gestão da segurança participa desde o início do processo de desenvolvimento de novos negócios. Lembrar da SI somente na reta final dos processos, denota pouca visão estratégica da questão.
- 2) Cheque se a área de SI se reporta a um nível hierárquico que possibilite sua atuação sem sofrer restrições.
- 3) Garanta que o gestor de SI conheça o planejamento estratégico da organização para poder fazer o seu plano de pesquisa e ação de acordo.
- 4) Analise se a área de segurança, após receber as devidas informações, estrutura o planejamento estratégico e define ações que cristalizarão esse projeto.
- 5) Não se esqueça de que é o negócio quem deve orientar o sentido e ritmo dos acontecimentos; esses devem se adequar a ele.

Fonte: Edison Fontes

ços no celular, que está sendo conhecido como Mobile Banking. O assunto é tão importante para o setor que será o tema do Congresso de Tecnologia da Informação (Ciab), da Federação Brasileira de Bancos (Febraban), a ser realizado em junho. No Banrisul, por exemplo, para lançar esse novo canal eletrônico de atendimento aos

clientes, a instituição fechou um acordo com a operadora Claro e a empresa de tecnologia Everymobile.

Pelo acordo, foi criado o Banrisul Mobile Banking, serviço que promete aos correntistas acesso à conferência de saldos de conta corrente, poupança integrada e fundos com resgate automático e mensagens da



Fonte: IDC



# A caminho da massificação

*Bancos testam novos sistemas, enquanto vai se popularizando a ferramenta preventiva da certificação digital*



SC/110

www.revistarazao.com.br

**N**O SETOR BANCÁRIO, campeão em investimentos em novas tecnologias de segurança da informação, vários modelos de ação estão sendo testados. A lógica do sistema, mais que reduzir fraudes, é aumentar a confiabilidade e credibilidade dos clientes – fator que é fundamental para a saúde das instituições financeiras. O Bradesco alardeia, em campanhas para o consumidor, os investimentos em biometria. Na peça publicitária, o banco diz que é o “pioneiro na utilização do reconhecimento biométrico das veias da palma da mão dos seus clientes”.

No BNP Paribas, uma das maiores redes internacionais de bancos – atua em 85 países, entre eles o Brasil, desde 1995, e tem 100 mil funcionários –, a novidade foi a adoção de medidas que pretendem garantir a proteção e autenticidade das informações. A equipe responsável por SI revela que as políticas de segurança são criadas pela matriz e seguidas pelas subsidiárias em todo o mundo, sendo que uma das ferramentas escolhidas pelo banco para eliminar as vulnerabilidades do ambiente é o Altiris Security Expressions, da Altiris, um gerenciador de riscos acoplado ao sistema. Com as ferramentas adotadas, a equipe responsável pode avaliar se as po-



## INTEGRAÇÃO À GOVERNANÇA

Leonardo Viegas (foto), coordenador do Comitê de Capacitação do Instituto Brasileiro de Governança Corporativa (IBGC), comenta que a segurança da informação é elemento crucial para o desenvolvimento de melhores práticas empresariais. Ainda mais no mundo bancário, onde regras dos órgãos reguladores tornaram-se extremamente rígidas, após os escândalos bilionários envolvendo fraudes de informação nos balanços da gigante norte-americana Enron.

Viegas faz uma reflexão cruzando os quatro pilares de Governança Corporativa com as demandas de gestão da informação. Inicialmente, ele analisa a questão da equidade, que tem a ver com a igualdade de direitos entre as pessoas. Isso, em termos de SI, se relaciona com os níveis de acesso à informação que devem ser estruturados nas Políticas de Segurança da Informação de cada empresa. Assim, todos os colaboradores do nível operacional terão acesso a informações iguais, mas distintas das informações que serão disponibilizadas aos envolvidos na estratégia da empresa. "A informação tem de ser organizada em níveis, nem todos os dados são para todos, há questões estratégicas que precisam ficar sobre sigilo." Ele cita o caso de segredos industriais e o acesso a conta dos clientes em instituições financeiras

O segundo pilar da Governança Corporativa que pode ser relacionado com SI é o da transparência. A partir da lógica da equidade, o acesso à informação deve ser pleno, dentro dos direitos de cada relacionamento empresa-colaborador ou mesmo empresa-cliente. Um bom exemplo disso acontece em sites de e-commerce e logística ou mesmo nos de Relação com Investidores. "É uma maneira de

reduzir o risco do processo", comenta Viegas. Quando se faz uma compra em uma loja virtual como o Submarino ou Americanas, todas as etapas do processo são informadas ao cliente, por meio de e-mails.

Alguns sites permitem ao cliente rastrear a compra, ao longo dessas etapas. Dentro disso, até mesmo a expansão de soluções de RFID, identificação por radio-freqüência, mostra-se como uma grande oportunidade para aumentar o controle sobre as mercadorias, garantindo a segurança do produto ou serviço e um melhor uso da informação gerada em cada etapa do processo.

O terceiro elemento é a prestação de contas. No caso de empresas abertas e instituições financeiras, órgãos regulatórios

monitoram os procedimentos para evitar quebras ou perda de confiança que acabam prejudicando o mercado como um todo. A SI é fundamental para que o processo seja eficiente, oferecendo dados sobre a realidade dessas instituições na hora certa, sem privilegiar ninguém e sem também gerar mecanismos fraudulentos, como no caso da Enron.

Por fim, o quarto ponto da Governança Corporativa a ser relacionado com SI é a responsabilidade socioambiental corporativa. Item mais complexo, esse ponto é crucial para a relação das empresas com a sociedade. Basta ver o caso da Serasa que presta um serviço crucial para o mercado e para o consumidor. Se as informações forem fraudadas ou mesmo perdidas, o prejuízo social e financeiro é muito grande. "Toda a empresa pode afetar positiva ou negativamente o ambiente, ter cuidados com os procedimentos gerenciais e a segurança dos mesmos é fundamental para que as relações sejam as melhores possíveis", acrescenta Viegas.

