SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS

Soluções simples
Grandes resultados

CONSELHO
DE TECNOLOGIA
DA INFORMAÇÃO
FECOMERCIO SP

FECOMERCIOSP
Representa muito para você.

CONSELHO
DE TECNOLOGIA
DA INFORMAÇÃO
FECOMERCIO SP

FECOMERCIOSP
Representa muito para você.

PRESIDENTE: Abram Szajman
DIRETOR EXECUTIVO: Antonio Carlos Borges
COLABORAÇÃO: Assessoria Técnica da FecomercioSP e Sérgio Roberto Ricupero, gerente de Segurança de Informações Corporativas da Editora Abril

EDITORA
FISCHER2
PUBLISHER: Luciana Fischer **MTB:** 55961
EDITOR CHEFE: Jander Ramon
EDITORA EXECUTIVA: Selma Panazzo
EDITOR ASSISTENTE: André Rocha

PROJETO GRÁFICO
TUTU
EDITORES DE ARTE: Maria Clara Voegeli e Demian Russo
CHEFE DE ARTE: Juliana R. Azevedo
DESIGNERS: Ângela Bacon e Cristina Tiemi Sano
PRODUÇÃO GRÁFICA: Clayton Cerigatto

SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS

Soluções simples – Grandes resultados

SUMÁRIO

SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS

Soluções simples - Grandes resultados

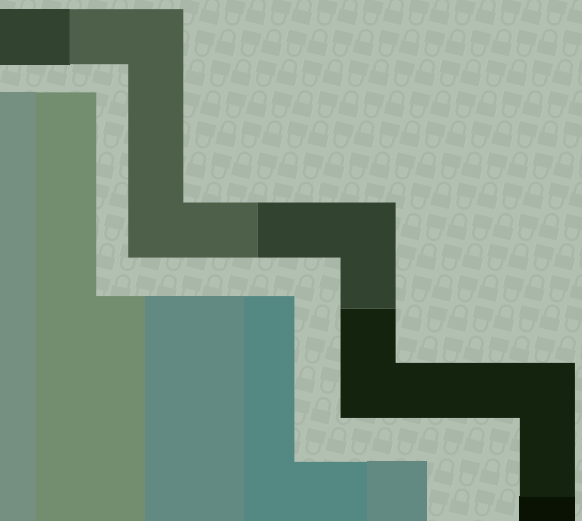
O crescente uso da tecnologia nas empresas brasileiras deixou de ser artigo de luxo, tornou-se uma questão de sobrevivência no mercado. E não apenas pelo aspecto da competitividade, mas também para atender às exigências legais: o empresário precisa implementar ferramentas tecnológicas para cumprir obrigações fiscais e trabalhistas, por exemplo.

Neste cenário, junto com o impulso na demanda por produtos tecnológicos, aumentou também a prática de ilícitos, tais como obtenção indevida de dados, propagação maliciosa de vírus e diversos tipos de estelionatos.

Por isso, com o objetivo de, mais uma vez, auxiliar o empresário na busca de melhores práticas para seus negócios, a FecomercioSP apresenta, a seguir, uma relação de dicas e sugestões práticas para prevenir ocorrências indesejáveis de crimes praticados contra empresas por meio de canais tecnológicos.

1

CUIDADOS NA ESCOLHA E AQUISIÇÃO DE EQUIPAMENTOS



A) *Equipamentos X adequação às necessidades da empresa*

Um dos primeiros passos na busca pela redução de riscos na utilização dos meios tecnológicos é, justamente, a escolha certa dos equipamentos. Além da necessidade de aquisição dos produtos de marcas de renome e de confiabilidade no mercado, também é importante que o empresário tenha plena consciência do que sua empresa precisa e aonde quer chegar com a aquisição de novos equipamentos. É preciso ter um plano. Para começar, o tipo de negócio desenvolvido já pode ser um bom indicativo das ferramentas necessárias, mas o perfil dos usuários também deve ser considerado. São exemplos de pontos relevantes no momento da escolha de equipamentos:

- tipo do negócio e principais riscos inerentes;
- características técnicas dos equipamentos e metas da empresa;
- capacidade de memória, velocidade e facilidade no uso;
- capacidade de interação com outras máquinas e equipamentos; e,
- tempo previsto de obsolescência.

O ideal é que a empresa, com base no planejamento estratégico ou metas periódicas pré-definidas, desenvolva também um planejamento tecnológico. Como as ferramentas não se justificam por si mesmas, o empresário deve se perguntar como a nova tecnologia a ser adquirida pode auxiliá-lo em seus objetivos. Com isso em mente, fica mais simples decidir o que e quanto comprar.

B) *Fornecedores confiáveis, assistência técnica e manutenção*

Uma vez decididos o tipo e a quantidade de equipamentos a serem adquiridos, o próximo passo é definir o fornecedor. É sempre bom lembrar que o empresário pode ter sérios problemas ao comprar produtos de origem duvidosa, sem falar naqueles decorrentes da prática de crimes como pirataria, descaminho, contrabando etc. Além da qualidade de tais produtos ser evidentemente comprometida, questões como garantia e assistência técnica também são prejudicadas. Assim, a aquisição de equipamentos tecnológicos para a empresa deve ser vista como investimento na ampliação e segurança dos negócios, e não apenas como custos a serem contabilizados.

Com relação à escolha das marcas dos produtos, é aconselhável buscar informações técnicas completas, bem como a realização de pesquisa de satisfação de usuários dos equipamentos pretendidos. Neste sentido, a internet é uma excelente fonte de informações sobre defeitos e vulnerabilidades recorrentes nos produtos.

Além disso, na escolha da marca dos equipamentos, o empresário deve pontuar, os seguintes fatores:

- a disponibilidade de assistência técnica próxima à empresa; e,
- os custos com peças de reposição da marca ou assistência técnica dos equipamentos.

C) *Escolha de* softwares *de prateleira e customização*

Dependendo do tipo de negócio desenvolvido pela empresa, os *softwares* comerciais, também conhecidos como "*softwares* de prateleira" (Microsoft, por exemplo) já suprem boa parte das necessidades diárias. Para a aquisição de tais produtos é importante que o empresário conheça suas principais características

e, acima de tudo, mantenha-se informado a respeito das atualizações de segurança oferecidas periodicamente pelo fabricante.

Esta medida é importante porque, depois que um *software* é lançado no mercado, o fabricante continua atento às suas vulnerabilidades. Assim, quando uma vulnerabilidade nova é descoberta, o fabricante imediatamente contata os usuários e envia, geralmente de forma gratuita, o pacote de atualizações. A empresa que não está devidamente cadastrada junto ao fabricante (adquiriu um *software* pirata, por exemplo) ou não atualiza seu sistema conforme indicação do fornecedor aumenta potencialmente seus riscos.

Por outro lado, nem sempre os *softwares* de prateleira são suficientes: muitas vezes os programas encomendados se transformam na principal ferramenta do negócio de uma empresa. Por isso, além da definição exata das funcionalidades que se espera do produto customizado, é essencial a atenção na contratação dos profissionais desenvolvedores do programa personalizado.

Assim, a escolha do prestador de serviços de desenvolvimento de *software* para a empresa merece cuidados redobrados, atentando-se aos seguintes pontos:

- procurar contratar empresa após prévia e confirmada indicação de outros parceiros;

- conhecer o currículo e confirmar a capacidade dos profissionais que executarão a atividade;

- estabelecer regras de segurança caso os desenvolvedores trabalhem dentro da empresa durante o período de desenvolvimento;

- alocar um profissional da própria empresa, com conhecimentos técnicos específicos, para acompanhar todas as atividades e serviços prestados pelos desenvolvedores do programa;

- nunca fornecer senhas da empresa ou dar acesso a dados sensíveis para os prestadores de serviços. Se necessário, estas senhas devem ser manipuladas pelo funcionário da empresa que estiver acompanhando os desenvolvedores; e

- não permitir cópia dos dados e cadastros pelos prestadores de serviços. Todas as ações de migração de dados devem ser procedidas apenas pelos funcionários da própria empresa ou, então, em ações pontuais dos terceiros integralmente acompanhadas.

D) *Inventário e destinação final dos equipamentos*

Os bens que compõem o patrimônio tecnológico de uma empresa precisam ser devidamente inventariados, tornando-se possível o acompanhamento total dos incidentes na vida útil dos equipamentos, atualizações e nível de obsolescência.

Como a tecnologia é aperfeiçoada constantemente, por questões de segurança, é importante que o empresário mantenha seus equipamentos em um nível ideal de atualização. Por isso, a troca dos equipamentos após certo tempo de uso pode ser a melhor alternativa para a empresa, se comparada com os custos e riscos com a manutenção e/ou assistência técnica recorrente.

Alguns itens não devem deixar de ser considerados em um inventário de ferramentas tecnológicas:

- data de aquisição, com arquivo de notas fiscais e termos de garantia;

- relação cronológica dos usuários e das atividades para as quais o equipamento se destina;
- identificação dos *softwares* instalados nas máquinas;
- identificação de manipulação por terceiros (assistência técnica, programadores terceirizados etc.);
- identificação de todas as ocasiões em que os equipamentos foram retirados e devolvidos nas dependências da empresa; e,
- data em que o equipamento deixou de ser usando e informações sobre o descarte ambientalmente correto. Se houver doação dos equipamentos, é importante fazer isso de forma documentada.

Por fim, encerrada a utilização de determinado equipamento, nunca é demais ressaltar, é essencial que se realize a formatação completa das máquinas, preferencialmente com *softwares* especializados em apagar dados definitivamente, antes de se proceder à destinação final.

Concluída esta providência, o material pode ser doado a instituições filantrópicas ou, ainda, a cooperativas de catadores, que darão a destinação final sustentável aos materiais.

2
CUIDADOS NO GERENCIAMENTO E GUARDA DE INFORMAÇÕES

A) *Senhas*

Quando se fala em princípios básicos de segurança da informação, sempre se começa pelo mesmo tema: senhas. Isto porque, seu compartilhamento ou obtenção por meios indevidos é responsável pela maioria das fraudes mundiais realizadas por meios eletrônicos.

As senhas – seja de máquinas, cadastros ou sistemas – são a porta de entrada para um banco infinito de informações altamente relevantes (ora, se não fossem importantes não haveria necessidade de senhas, certo?). Exatamente por ter isso em mente, pessoas mal intencionadas buscam incansavelmente sua obtenção pelos mais diversos meios fraudulentos.

Assim, considerando que o inimigo sempre está atento aos mínimos deslizes, o gerenciamento das senhas de uma empresa merece atenção especial do empresário. Desde sua formulação, concessão, até o bloqueio, todas as providências devem ser muito bem planejadas. Vamos às sugestões:

- nas regras para a formulação das senhas, exija sempre a variedade por tipos de caracteres – letras, números e símbolos;
- estabeleça e monitore o cumprimento fiel de política ostensiva de utilização para funcionários e colaboradores, com regras obviamente proibitivas e punitivas relacionadas ao compartilhamento de senhas com terceiros, ainda que da própria empresa; e,
- providencie a validade temporal das senhas, que devem ser obrigatoriamente alteradas em um período razoavelmente curto de tempo (a cada dois meses, por exemplo).

B) E-mail *e* spam

Se, por um lado, é por meio da captação de senhas que grande parte das fraudes se inicia, não se pode negar que, por outro, é por meio dos *e-mails* que as tentativas de fraude se propagam.

Como comunicação rápida e barata, o canal de recebimento de *e-mail* tem enorme potencial tanto para o bem, quanto para o mal. Aqui, inevitavelmente, vamos falar dos riscos relacionados ao seu uso.

Por meio de *e-mails* e *spams* (*e-mails* abusivos não solicitados e de cunho comercial) os fraudadores enviam arquivos para captação de senhas, disseminação de vírus e outros artifícios para obter informações sigilosas da empresa. Você pode se prevenir com algumas ações simples:

- nunca abra anexos de *e-mails* de pessoas desconhecidas;
- analise cuidadosamente a possibilidade de não abrir anexos, se possível, mesmo de pessoas conhecidas;
- nunca efetue ou preencha cadastros de pesquisas enviadas anexas a *e-mails*;
- delete *e-mails* supostamente enviados por instituições bancárias – bancos de renome não enviam comunicação por *e-mail*;
- ao clicar em *links* enviados por *e-mail*, confirme na barra de endereço se você está sendo direcionado para o local efetivamente desejado (existem muitos *links* falsos que direcionam para *sites* fraudulentos);
- crie uma política interna de utilização de *e-mails* coorporativos – as regras precisam ser claras, objetivas e com possibilidade de imposição de penalidades em caso de inobservância;

- utilize ferramentas legais de monitoramento dos *e-mails* coorporativos da empresa, com a ampla divulgação desta estratégia aos funcionários;
- instale filtros *antispam* e atualize-os com regularidade; e,
- mantenha os sistemas operacionais sempre atualizados e originais de seus fabricantes.

C) *Antivírus*, firewalls *e bloqueios de* sites

Hoje em dia, a perda/divulgação de dados e/ou cadastros de uma empresa pode significar sua falência total. Por isso, a proteção dos equipamentos tecnológicos da empresa contra ameaças de invasão ou vírus também merece adoção de medidas preventivas importantes.

No tocante aos antivírus, cujo objetivo principal é evitar a contaminação do computador por *malwares* (*softwares* mal intencionados), pode-se dizer que, atualmente, o mercado oferece uma gama de soluções a baixo custo e que podem ser interessantes para a empresa.

Exatamente por este motivo, a avaliação de um profissional da área de tecnologia é importantíssima na escolha dos *softwares* de proteção em geral, já que, para que a aquisição de uma solução tecnológica seja eficaz, é preciso definir quais são os tipos de riscos a que determinada empresa está sujeita. E os riscos, por sua vez, estão intimamente ligados às atividades empresariais exercidas e às modalidades de equipamentos utilizados.

Assim, se as atividades da empresa têm estreita relação com o envio e recebimento de informações por *e-mail*, por exemplo, o antivírus deve ter foco especial neste segmento.

Além do antivírus, outra forma da empresa ter seu sistema protegido é a utilização dos *firewalls*, produtos para bloquear acessos não autorizados ao sistema. Para sua aquisição, contudo, também é aconselhável que haja a prévia análise de um profissional de TI, para que sua implantação seja estudada em conjunto com a utilização de todas as demais ferramentas de segurança da informação existentes na empresa.

Novamente, não se pode deixar de lembrar que todas as ferramentas de segurança adotadas pela empresa também precisam ser atualizadas constantemente, conforme as indicações do fabricante.

Neste sentido, considerando que o nível de segurança aumenta na medida em que são ampliadas a variedade e a qualidade das soluções adotadas, também é interessante cogitar o bloqueio, no ambiente de trabalho, de acesso a determinados sites ou funcionalidades que potencialmente podem trazer prejuízos. Dentre tais sites podemos citar aqueles que oferecem *downloads* de programas e conteúdos, compartilhamento de arquivos, redes sociais em geral e trocas de mensagens, entre inúmeros outros.

Além disso, se as informações veiculadas nas máquinas da empresa forem de cunho estritamente confidencial (como informações bancárias e dados cadastrais, por exemplo) pode ser prudente adotar a estratégia de bloqueio de acesso a *e-mails* particulares, bem como a possibilidade de cópia de arquivos das máquinas em *hardwares* móveis, como *pen drive* ou HD externo.

É preciso ter cuidado, também, com a criação e gerenciamento de redes internas, já que, se, por um lado, facilitam o acesso a arquivos e informações de interesse comum, de outro, podem causar estragos coletivos, caso haja a contaminação por vírus e outras ações criminosas em geral. As redes merecem, portanto, atenção redobrada de monitoramento e proteção.

Outro ponto que deve ser levado em consideração pelo empresário nos dias de hoje são as soluções que ficam residentes na internet, chamadas de *cloud computing*. Estas soluções ficam residentes em sistemas profissionais e os usuários, de modo geral, só necessitam de uma conexão à internet. Assim, esta pode ser mais uma alternativa a ser avaliada para a estruturação de uma infraestrutura adequada e segura aos negócios das empresas.

SINTETIZANDO:

- *prevenção contra fraudes é sinônimo de utilização de variadas ferramentas, sendo que as minimamente exigidas são os antivírus, filtros* antispam, firewalls *e bloqueio de acesso a certos sites;*

- *as ferramentas adquiridas pela empresa precisam ser constantemente atualizadas, conforme indicações dos fabricantes; e,*

- *a análise das vulnerabilidades da empresa versus as ferramentas adequadas para a proteção desta, deve, preferencialmente, ser feita por um profissional de TI.*

D) Backups *e revisões periódicas*

Independentemente de invasões ou ataques, defeitos e falhas técnicas nos equipamentos ou *softwares* adquiridos sempre podem acontecer. Por isso, a manutenção constante e a verificação das condições dos aparelhos são extremamente importantes para garantir a segurança das informações. O que, em muitos casos, pode representar até mesmo a continuidade do negócio.

A substituição de máquinas antigas, a aquisição de equipamentos recentemente lançados e a constante busca pela modernização e atualização de todo o sistema, certamente, auxiliam na diminuição de riscos. E isso é indissociável de uma boa política de prevenção a crimes e fraudes.

Por outro lado, também é medida fundamental em termos de segurança que, periodicamente (e, de preferência, em curto prazo) seja realizado o *backup* (cópia de segurança) de todo o sistema da empresa. Pode parecer exagero, mas as informações consolidadas por uma empresa têm valor inestimável, ainda

que simplesmente perdidas sem favorecimento de um infrator. Isto porque, em regra, refletem anos e anos de conhecimento e trabalho acumulado. E, por precaução, também não é demais sugerir a realização de mais de uma cópia de segurança de tudo, dependendo do grau de relevância das informações.

Desta forma, definitivamente não é investimento inútil a aquisição de máquinas para arquivos de cópias de todas as informações relevantes da empresa.

Pense se todos os seus dados forem perdidos, qual o impacto desta perda sobre o seu negócio?

EM RESUMO:

- *a manutenção e a substituição de equipamentos antigos são importantes;*
- *a utilização de máquinas de qualidade, evitando-se o uso de equipamentos sem garantia, é o mais indicado; e,*
- *a realização de* backups *periódicos é essencial.*

3
ENGENHARIA SOCIAL

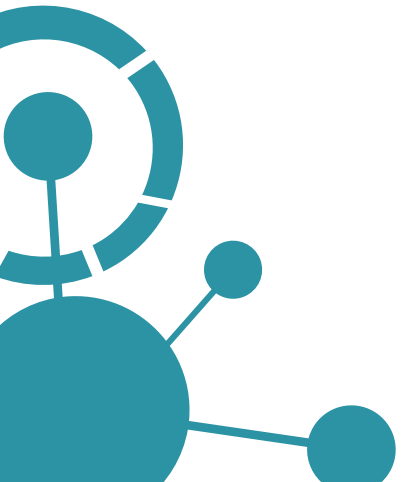
Não só os aspectos técnicos merecem a atenção do empresário que busca aumentar a segurança da informação em sua empresa. A chamada "engenharia social", usada para cometer fraudes, também merece ser seriamente estudada.

Embora o nome assuste um pouco, engenharia social nada mais é do que a utilização de estratégias para explorar o lado mais fraco (ou sensível) do ser humano no intuito de obter informações relevantes. É o uso de técnicas para explorar sentimentos como curiosidade, culpa, solidariedade e medo, para ter acesso aos dados sensíveis de pessoas e empresas. As formas mais corriqueiras são os populares *e-mails* de "clique aqui e veja as fotos de sua esposa", "seu nome foi incluído no Serasa – clique aqui para saber o motivo", "atualize os dados de seu *token* por *e-mail*" etc.

Além dos conhecidos e-mails de *phishing* (pescaria de dados), há também as fraudes cometidas por telefone ("seu filho foi sequestrado") e envio de mensagens pelo celular ("você ganhou a promoção do Domingão do Faustão"), entre inúmeras praticadas amplamente adotadas na busca de vítimas desavisadas. E o pior: novas "armadilhas" são inventadas a cada dia, pois, assim que antigas fraudes são descobertas como tal, os criminosos empenham-se na criação de histórias fraudulentas ainda mais convincentes.

Por isso, se o empresário realmente pretende desenvolver uma política inteligente de segurança da informação, também precisa preparar seu contingente humano para prevenir ataques e, acima de tudo, evitar a consumação de prejuízos.

Para tanto, selecionamos, nos tópicos seguintes, alguns itens relacionados à engenharia social que devem ser analisadas cuidadosamente nas empresas:



A) *Capacitação da equipe (incluindo a diretoria) e monitoramento*

Como dito anteriormente, o principal alvo da aplicação de técnicas de engenharia social nos crimes eletrônicos é o conjunto de funcionários de uma empresa. Quanto menos preparados forem os empregados, maior é a probabilidade de prejuízos.

Por esta razão, é aconselhável o preparo e treinamento constante de toda a equipe de colaboradores, incluindo os integrantes da direção da empresa, para atualização e acompanhamento constante das práticas aceitáveis. Cursos, palestras, cartilhas e campanhas periódicas são excelentes canais para alertar, informar e transformar sua equipe.

Merece cautela especial, também, a utilização das redes sociais. Pessoas mal intencionadas comumente se aproximam de funcionários de certas corporações apenas para obter informações estratégicas para atacar diretamente a empresa (invasão de sistema, envio de arquivos maliciosos, vírus etc.).

Por esta razão, é muito importante que o empresário trabalhe incansavelmente o alerta aos seus funcionários sobre a inadequação da divulgação de informações não autorizadas relacionadas à empresa nas redes sociais.

Outra estratégia sugerida é a formalização de regras para uma política de utilização dos equipamentos tecnológicos: isto pode ser feito por meio da elaboração de um regulamento interno, que deverá contemplar, no mínimo, diretrizes para os seguintes temas:

- fluxo de conteúdo permitido/proibido por meio dos *e-mails* corporativos;
- relação e/ou tipo de sites cujo acesso é considerado inadequado;
- regras sobre a divulgação de informações da empresa em redes sociais;
- regras sobre a utilização de *hardwares* móveis (*pen drive* etc.) e acesso a contas pessoais de *e-mail*;
- regras sobre a formulação de senhas e proibição de seu compartilhamento;

- disposições sobre a guarda e o sigilo de informações da empresa;

- preceitos sobre permissão/proibição de *downloads* de arquivos diversos nos computadores da empresa;

- alerta para os tipos de fraudes recorrentes praticadas pela internet (este item precisa de atualização constante, sendo o ideal que, assim que o departamento de TI identificar um tipo novo de fraude, todos os colaboradores sejam comunicados imediatamente); e,

- aviso ostensivo sobre o monitoramento do uso das ferramentas tecnológicas pelo empregador (*e-mail* corporativo e acesso à internet, entre outros), se for o caso.

Com relação à possibilidade de monitoramento eletrônico de *e-mail*, cabe aqui um esclarecimento importante. Embora ainda haja certa discussão sobre o tema, o assunto tem sido pacificado por decisões do Poder Judiciário no seguinte sentido: se o *e-mail*/sistema é da empresa e há avisos ostensivos de que o equipamento é para uso exclusivo em serviço e está sendo supervisionado, o monitoramento é considerado legítimo. E, dependendo da gravidade do fato

ocasionado pelo uso indevido pelo funcionário, pode até mesmo fundamentar uma dispensa por justa causa.

Falando em mau procedimento dos funcionários, é bom lembrar que, ao lado da preocupação com os ataques de pessoas externas, o empresário, complementarmente, precisa estar alerta ao cometimento de ilícitos por integrantes de sua equipe. Nos termos da legislação civil em vigor, o proprietário de uma empresa pode ser responsabilizado pelos atos praticados pelos empregados e, havendo danos a terceiros, o empregador poderá ser obrigado a repará-los.

Também é importante frisar que, de acordo com o Estatuto da Criança e do Adolescente, se o empregado praticar pedofilia (armazenar ou divulgar fotos de pornografia infantil, por exemplo) através das ferramentas tecnológicas fornecidas pelo empregador, este último poderá ser responsabilizado se tiver conhecimento de tal prática e não fizer nada para impedí-la.

Ou seja, capacitação, cuidado e acompanhamento do uso das ferramentas tecnológicas pelos funcionários também são medidas impositivas altamente relevantes na prevenção de danos dentro de uma empresa.

B) *Contratação de terceiros e colaboradores em geral*

Além de treinamento e regras para os funcionários, é salutar o estabelecimento de regras e critérios para contratação e prestação de serviços por parte de fornecedores em geral, principalmente aqueles que podem, eventualmente, ter acesso aos sistemas da empresa.

Primeiramente, para as contratações iniciais, em especial aquelas realizadas pela *web*, é preciso buscar indicações confiáveis de outros clientes do fornecedor e confirmar se os dados publicados nos *sites* são verdadeiros (telefone, endereço, tempo de existência da empresa etc.).

Outro aspecto importante a ser verificado refere-se à formação e capacitação técnica comprovada dos prestadores de serviços – profissionais desatualizados ou com conhecimento técnico limitado podem não só prejudicar todo o conjunto tecnológico de uma empresa, como também ocasionar a perda definitiva de dados importantes.

Também não podem ser esquecidas as precauções de praxe no acesso, pelos terceiros, aos dados e sistemas operacionais da empresa: regras precisam ser definidas no tocante à manipulação e possibilidade de cópias, conforme descrito no capítulo 1, "C", deste trabalho. E, havendo regulamento interno para utilização das ferramentas tecnológicas em uma empresa, todos os colaboradores, inclusive terceiros, devem segui-lo.

Assim, é interessante que no contrato escrito de prestação de serviços tecnológicos por terceiros, seja de assistência técnica, manutenção periódica, fornecimento de equipamentos e desenvolvimento de *software*, entre outros haja o estabelecimento prévio e claro de todas as regras básicas de segurança adotadas pela empresa e que, se quebradas, sujeitarão o contratante a uma penalidade que pode ser multa ou até mesmo a rescisão do contrato.

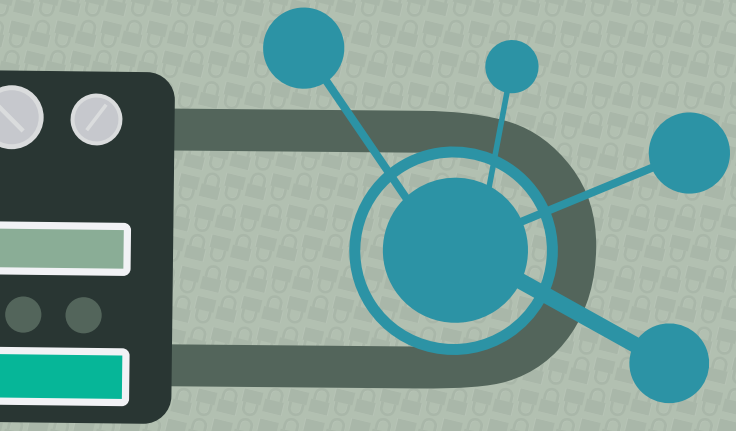
Finalmente, também é importante enfatizar que a terceirização de serviços na área de tecnologia da informação deve seguir rigorosos padrões jurídicos para a sua completa configuração. Se houver desvio das finalidades contratuais (ter-

ceirização da atividade fim da empresa, por exemplo) e, principalmente, nas hipóteses em que o serviço for prestado por pessoa física, com subordinação, habitualidade e mediante salário, poderá ficar caracterizada uma relação de emprego (nos termos da Consolidação das Leis do Trabalho), e não de uma simples prestação de serviços terceirizados.

Neste caso, desvirtuada a terceirização, serão devidas aos trabalhadores envolvidos todas as verbas trabalhistas decorrentes da relação de trabalho, independentemente de o serviço ter sido prestado dentro da empresa (na sede, filiais etc.), fora dela ou por empresa interposta.

Aliás, reforçando este entendimento, recentemente foi publicada a Lei 12.551/2011, também conhecida como Lei do Teletrabalho, que definiu não haver distinção, para fins de reconhecimento dos direitos trabalhistas, entre trabalhadores que prestam serviço dentro da empresa e aqueles que realizam o serviço à distância (em casa ou outros locais), desde que estejam caracterizados os pressupostos da relação de emprego (subordinação e habitualidade, por exemplo).

4
PLANEJAMENTO E OUTROS CUIDADOS



Bem, como visto até aqui, quando se fala em segurança da informação, obrigatoriamente se considera a tomada e conjugação de diversas providências de naturezas variadas.

Desta forma, para organizar a adoção de todas estas medidas é essencial a elaboração de um planejamento estratégico para todo o sistema tecnológico, com indicação de objetivos, metas e ações estruturantes.

Evidentemente, para a elaboração de um plano eficaz e factível, o auxílio de profissionais experientes em cada uma das áreas a ser trabalhada é impositivo. Assim, contando sempre com a ajuda de especialistas, é interessante que o empresário enumere providências e prioridades que pretende executar, tendo em vista, além da segregação dos assuntos por natureza:

- os fatores de maior vulnerabilidade de seu sistema;
- os pontos frágeis que podem trazer grandes prejuízos financeiros e de imagem, entre outros;
- as medidas mais fáceis e de baixo custo, com resultado imediato;
- as ações dispendiosas, mas com resultados importantes em curto prazo;
- a forma de organização da documentação de todas as mudanças e aquisições; e,
- as providências para manutenção e acompanhamento da nova estrutura.

Este último ponto é tão importante quando a tomada inicial de providências, pois somente o monitoramento e a revisão constante de todas as ferramentas garantirão a solidez e os resultados esperados da estrutura montada.

Apresentamos, a seguir, outros pontos que podem auxiliar o empresário no planejamento e manutenção com segurança de seu sistema:

A) *Consultorias externas e implantação de Normas Regulamentadoras*

Além dos acompanhamentos internos a serem regularmente realizados, também tem sido adotada por muitas empresas a estratégia de contratação de auditorias/consultorias externas para a verificação periódica do sistema. A grande vantagem desta providência é que ao mesmo tempo pode-se aferir e confirmar a qualidade técnica dos profissionais internos e, por outro lado, também se pode obter sugestões de medidas complementares a serem adotadas.

O acompanhamento por terceiros garante, assim, a atualização constante do sistema e o acompanhamento da qualidade técnica dos funcionários de TI da própria empresa.

Além deste tipo de serviço, a empresa pode também optar pela adoção das normas e padrões técnicos expedidos pela Associação Brasileira de Normas Técnicas (ABNT), que culminaram na certificação da empresa em, por exemplo, gestão de riscos da informação.

Para este assunto específico, inclusive, existe a Norma ISO 27.005 que trata detalhadamente da gestão de riscos de segurança da informação, bem como outras da série ISO 27.000 que podem ser empregadas como orientações gerais para a gestão da segurança nas organizações. Há, também, as normas do *Payment Card Industry* (PCI) e do *Data Security Standard* (DSS). Obtendo estas certificações, a empresa, além de garantir processos internos eficientes, demonstrará, publicamente, a parceiros e clientes sua transparência e preocupação na gestão da segurança de seus dados.

B) *Atenção constante às regras jurídicas*

Ao lado dos aspectos técnicos e organizacionais da segurança da informação, é igualmente importante que o empresário esteja atento aos cuidados jurídicos necessários para executar as medidas de proteção de seus dados. Alguns pontos a serem considerados são:

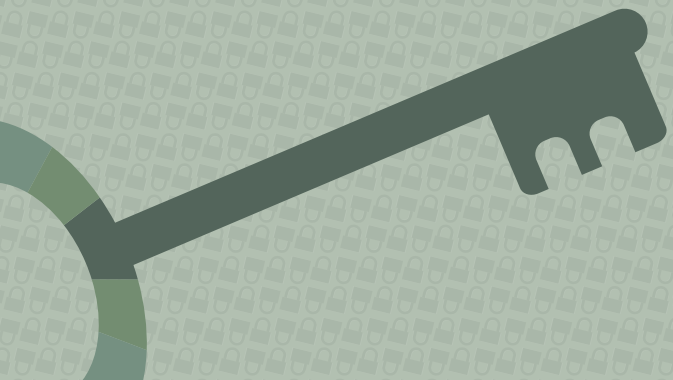
- análise e atualização dos contratos com clientes, com atenção ao Código de Defesa do Consumidor (CDC) e outras leis relacionadas;

- análise e atualização dos contratos de trabalho dos funcionários e/ou criação/atualização de regulamento interno relativo ao uso das ferramentas tecnológicas da empresa;

- análise e atualização dos contratos com fornecedores relativamente às regras de segurança da informação, compartilhamento e divulgação de dados; e,

- adoção de medidas jurídicas para prevenir ou combater eventuais ameaças ou lesões ao direito da empresa à segurança da informação.

5
CONCLUSÃO



No decorrer deste pequeno consolidado de dicas foi possível perceber que a segurança da informação é algo que merece atenção especial nas empresas, ainda mais em um mundo em que os negócios, aquisições e transações circulam cada vez mais pelos meios tecnológicos e virtuais.

Neste cenário, para uma empresa se manter sadia e produtiva, é imprescindível que faça, periodicamente, o *checkup* de todo o seu sistema operacional, garantindo, assim, a continuação da produtividade e de novos negócios.

Contudo, para que isso seja possível, faz-se necessária a formulação de planejamento estruturado que contemple medidas de naturezas diferentes que, devidamente conjugadas, formarão a "armadura de proteção" da empresa. Esta armadura pode, então, ser confeccionada com base nos seguintes fatores:

- avaliação sobre os riscos a que seu negócio está sujeito;
- cuidado na aquisição de equipamentos, produtos e serviços;
- gerenciamento, guarda e proteção adequada de informações;
- gerenciamento dos *softwares*, de modo geral, em relação às suas atualizações;
- medidas de prevenção contra técnicas de engenharia social;
- planejamento, organização e acompanhamento contínuo. É preciso entender que a segurança é um processo contínuo e cíclico e que deve ser reavaliada periodicamente; e,
- atenção aos detalhes jurídicos.

Finalmente, não se pode negar que ataques covardes e pessoas mal intencionadas, infelizmente, sempre existirão. Entretanto, se o empresário estiver devidamente preparado para enfrentar esta realidade, ao invés de desapontar clientes, parceiros comerciais, ou, simplesmente lamentar os prejuízos, poderá exercer seu papel de protagonista em segurança da informação e, com medidas simples, passar a frustrar planos de criminosos.

Enfim, nos dias atuais o empresário precisa entender que a sociedade demanda por segurança, urgentemente, em todos os seus aspectos. Seja no mundo real ou no mundo virtual.

FECOMERCIOSP

Representa muito para você.