46 – Fevereiro de 2003

Peopleware: contrate sem arriscar suas informações

Com o início de mais um ano fiscal as empresas se vêem na hora de implementar as estratégias de negócio definidas no Business Plan e pôr em prática as ações que irão criar a infra-estrutura de suporte para que os objetivos sejam alcançados. Os planos de Marketing, o Plano Diretor de Tecnologia e o Plano Executivo de Segurança da Informação são alguns dos instrumentos de orientação que definem prioridades, métricas, montantes orçamentários, projetos e principalmente os recursos físicos, tecnológicos e humanos que irão sustentar seus processos.

Neste período do ano, é comum que as empresas tenham de fortalecer suas equipes e assim, selecionar profissionais que irão integrar a força de vendas, o time da produção, os estrategistas da propaganda, os jornalistas e webpublishers do portal Internet, os técnicos que mantêm a infra-estrutura tecnológica de suporte ao negócios e ainda os consultores e analistas de segurança que irão enriquecer o grupo do Security Office.
É uma fase de aquisição e manutenção de ativos. Novos equipamentos substituem os antigos. Aplicações sofrem atualizações. Mudanças nas instalações físicas ocorrem para hospedar e acompanhar as transformações das equipes e departamentos. Sistemas são adquiridos e se integram aos legados. Funcionários se juntam aos novos colaboradores recém admitidos, para se tornarem co-responsáveis pela operação da empresa. Hardwares de última geração, softwares performáticos e, porque não, peopleware.

Isso mesmo. Uma nova expressão para descrever o ativo humano. Eles representam um dos mais importantes elos da "corrente da segurança". Responsáveis por definições estratégicas, pela gestão de processos e pela operação direta ou indireta de atividades operacionais, o capital humano é uma peça-chave para a gestão de segurança da informação.
Os sistemas e equipamentos, principalmente os computadores, são programáveis e têm o comportamento previsível. Estão adequadamente configurados, instalados e escritos, ou estão com falhas que provocam erros comumente previsíveis e estáveis. Com o ser humano é diferente. Não são máquinas, mas um sistema literalmente vivo e complexo que pode reagir de maneira diferente a cada nova situação e até mesmo em situações já vivenciados inúmeras vezes.
Assim, os funcionários e também os recursos terceirizados, são um ativo que custodia informações valiosas e de propriedade da empresa onde trabalham, informações confidenciais como a senha de acesso, segredos de negócio, estratégias, planos de marketing e produtos.
Para compreender melhor o papel de cada indivíduo, nada melhor do que a analogia com um quebra-cabeças. Cada elemento tem seu papel no todo. A segurança das informações e a redução dos riscos estão ligadas diretamente à cumplicidade de cada peça e ao trabalho sinergético e integrado de todas elas.

Por isso os processos de admissão e demissão tem papel importante no planejamento e gestão de segurança da informação. É preciso estabelecer critérios e empregar um método

ajustável à natureza da cada empresa ou área que ira receber o recursos, a fim de reduzir os riscos de uma má contratação. Uma contratação que adicione perigo à operação da empresa e ponha em risco informações sensíveis que, por erro, descuido ou atitude intencionalmente fraudulenta, pode gerar impactos financeiros, legais ou dados à credibilidade e imagem da empresa contratante.
Não há um conjunto de normas, padrões e critérios de seleção que se apliquem incondicionalmente a todas as empresas, afinal, existem grandes diferenças entre elas, mas podemos eleger um conjunto de dicas e comportamentos coerentes que poderão fortalecer o departamento de recursos humanos na difícil, e agora crítico sob os olhos da segurança, processo de admissão de demissão.

- Valores de família. Avalie os valores mantidos pelo candidato. Seu compromisso com a fidelidade, imagem, moral, ética etc. São bons instrumentos para identificar o perfil profissional e projetar seu comportamento diante de situações em que mantém controle sobre informações valiosas; tem autonomia de direitos de manuseio, armazenamento, transporte e descarte de informações valiosas; é cobiçado e assediado pela concorrência etc.

- Situações de risco. Adote instrumentos de interatividade para apoiar o processo de conhecimento do candidato. As dinâmicas de grupo são interessantes, pois podem simular situações que pareçam estar fora do processo seletivo, mas estão sendo acompanhadas pela equipe a fim de perceber o comportamento do candidato fora da pressão natural do processo de admissão.

- Histórico comportamental. Procure identificar possíveis desvios de conduta que tenham sido cometidos pelo candidato. Faça uma "investigação" de seu histórico. Identifique e converse com seus chefes anteriores. Levante seu comportamento nas relações interpessoais. Procure descobrir sua reação diante de situações extremas: quando fora demitido, promovido ou tivera que assumir grande responsabilidade inusitada. Dependendo da criticidade do cargo que irá ocupar - em função do valor das informações que lhe serão disponibilizadas – visite o bairro onde reside. Converse com os vizinhos, funcionários do edifício e assim, conheça um pouco mais sobre seu estilo de vida.

- Experiências profissionais passadas. Analise as atividades profissionais anteriores. Procure saber se mantinha controle e acesso a informações críticas para a empresa. Meça a responsabilidade que assumia e a natureza dos produtos e serviços oferecidos pela empresa. Deve ser considerado como ponto positivo, ter tido experiência em ambientes e cargos que se assemelhem ao ambiente e cargo disponível.

- Desequilibro financeiro. Não é um instrumento infalível, mas em função do cargo e da natureza da empresa que oferece a vaga, é conveniente pesquisar o equilíbrio financeiro do candidato através de órgãos públicos e privados. Verificar se mantém contas bancárias, se possui crédito no mercado e se tem ou teve o nome no SPC, são bons instrumentos para reduzir a probabilidade de contratar um profissional de risco. É importante frisar que este comportamento, de uma maneira geral, não

desqualifica um possível candidato. Diante desses resultados, a empresa pode promover com ele uma conversa sobre o assunto e assim compreender como o candidato compreende a situação e vê a solução.

- Cultura de Segurança. É importante avaliar se o candidato mantém cultura de segurança herdada de experiências profissionais passadas ou adquiridas gradativamente por conta de treinamentos ou iniciativas de autodidatismo. São profissionais cobiçados, pois encurtam o caminho de envolver os funcionários como co-responsáveis pela gestão de riscos de segurança da informação.

- Business Plan pessoal. Deve fazer parte do processo seletivo, o mapeamento dos planos profissionais do candidato. Saber onde ele quer chegar, quanto gostaria de ganhar, que cargo pretenderia ocupar, são uma forma de perceber se a empresa se adapta ao candidato e vice-versa. As distorções de percepção e insatisfações nascidas durante os anos de trabalho são um risco potencial para desvios de conduta, descontentamentos e atitudes que exponham as informações da empresa. Não confundamos ambição natural e saudável com objetivos ambiciosos perseguidos cegamente, custe o que custar.

- Quoeficiente Emocional. É evidente que este elemento é importante para reduzir os riscos de uma seleção desastrada. O relacionamento interpessoal, a coerência dos planos de carreira, a dedicação à educação continuada e a interatividade profissional são aspectos intimamente relacionados a uma boa escolha. Deve ser valorizada, mas não deve ser encarada como fator exclusivo de seleção.

- Satisfação. É também fator crítico manter os recursos humanos motivamos e envolvidos com a missão e os objetivos da empresa. Esta sinergia deve acontecer no primeiro contato e as expectativas devem ser equalizadas antes mesmo de se efetivar uma contratação. Pessoas felizes e encaminhadas profissionalmente são um sinal de comportamentos coerentes e alinhados aos interessas da empresa. Recursos em cumplicidade com a continuidade operacional e a proteção das informações que conferem saúde à empresa onde trabalha.

- Integração das áreas. Não só procedimentos e normas que compõem os processos seletivos reduzem os riscos de uma contratação e demissão. A segurança da informação se faz pela ação de diversos elementos, afinal, as falhas e riscos potenciais se dão em ativos humanos, físicos e tecnológicos. Por isso, é preciso que as áreas de empresa estejam integradas. Desta forma, é possível – antes de anunciar uma demissão ao funcionário ou contratação ao candidato – sinalizar o fato à área de tecnologia e de rede, por exemplo, que irá administrar as senhas de acesso, o acesso físico ao ambiente, o manuseio de mídias de armazenamento etc.

- Conscientização. Como o objetivo de formalizar a responsabilidade da cada funcionário, sensibilizá-lo, e dar início ao processo de formação de cultura de segurança da informação, as empresas devem adotar o documento chamado Termo de Sigilo e Confidencialidade. São termos preparados de acordo com as características da cada empresa e em sintonia com sua política de segurança,

SÊMOLA

descrevendo o compromisso do corpo estratégico e principalmente, a co-responsabilidade de cada funcionário na custódia e segurança de informações sensíveis. Apesar de ainda existirem lacunas legais e múltiplas interpretações sobre o termo e possíveis abusos de poder na relação de trabalho, seu valor enquanto instrumento de envolvimento e conscientização, já justificam sua aplicação.

Vimos que a gestão da segurança da informação transcende os aspectos tecnológicos e dependem também de áreas antes tidas como satélites e desassociadas ao desafio de gerir a informações e sua proteção. O peopleware, a cada ano, aparece como um dos maiores responsáveis por problemas de segurança, como revela a oitava pesquisa anual da Módulo Security Solutions. É verdade que esses números consideram as atitudes fraudulentas, mas têm o resultado baseado principalmente no descuido, erro, displicência, despreparo e na falta de conscientização dos funcionários. As empresas precisam não só valorizar o capital intelectual, como vêm fazendo há anos, mas precisam formar uma cultura segurança entre seus funcionários e se cercar de controles que fortaleçam os processos que suportam a operação do negócio. Não abandonem o hardware e software, mas reservem boa parte da atenção para o peopleware. As empresas são feitas de pessoas.

Marcos Sêmola *é Mestrando em Economia Empresarial, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor de Gestão da Segurança da Informação na FGV – Fundação Getúlio Vargas, Gerente Nacional de Produtos e Consultor de Segurança da Módulo Security Solutions S.A. É autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2002.*
msemola@modulo.com.br

SÊMOLA