Por Patricia Peck (*)

Você já teve a impressão de que a TI e o Jurídico não falam a mesma língua? Mas deveriam! Afinal, ambos têm que servir ao negócio para que possa ser feita a gestão adequada dos riscos, inovando com conformidade legal.

Se outros setores da empresa demandam mais conhecimento técnico, como Tributário e Ambiental, por que a TI não recebe também um tratamento de jurídico especializado em tecnologia?

O primeiro passo para que o casamento entre TI e Jurídico dê certo é justamente encontrar o profissional certo para fazer este elo, esta ponte entre ambos. Este perfil hoje é o do advogado de Direito Digital, que não apenas interpreta as leis mas também tem formação técnica, é certificado, estuda e conhece a linguagem da TI e busca se manter sempre atualizado sobre as novas soluções que estão surgindo e que exigem blindagem legal para serem implementadas nas empresas.

Como os cursos de Direito ainda estão atrasados na tarefa de atualizar o conteúdo programático da graduação, cabe ao gestor da TI buscar capacitar o jurídico interno ou procurar ajuda de um escritório terceirizado, pelo menos até que se possa consolidar um conhecimento maior sobre a matéria dentro da própria equipe.

Mas lembre, não é apenas o curso ou a pós em Direito Digital que garante a integração. O advogado tem que ter um certo DNA tecnológico para ser um verdadeiro parceiro do CIO. Muitos riscos conseguem ser mitigados através de uma adequada compreensão de como funcionam as ferramentas e quais seus impactos reais no negócio.

Vamos analisar alguns casos práticos:

CASO 1

CIO: Eu gostaria de implementar uma política de BYOD, já que a alta direção quer poder utilizar seus equipamentos pessoais na empresa (como tablets e smartphones).

Jurídico Tradicional: Você quer deixar que as pessoas possam usar o seu equipamento para o trabalho. Isso é muito perigoso. Como vamos separar a vida pessoal da profissional. Aí vai ser difícil podermos controlar o que as pessoas estão fazendo com as informações da empresa. Por enquanto melhor é proibir, já temos política de segurança que diz que tem que usar o recurso da empresa, e somente para fim profissional.

Especialista Direito Digital: Sim, claro, isso é uma necessidade urgente, pois os colaboradores estão vindo para o trabalho trazendo seus dispositivos pessoais sem que haja uma regra específica aplicada. O maior risco é não ter regra. Agora, podemos iniciar com um piloto para cargos de confiança ou gestores e depois implementar na empresa toda.

Mas, independente disso, dê a pessoa poder escolher se quer trabalhar com seu equipamento ou da empresa, muitos já estão participando de reuniões anotando no tablet pessoal as informações corporativas. Fora os smartphones, que inclusive usam para acesssar as mídias sociais no trabalho, tiram fotos. Ou seja, o perigo de vazamento de informação é elevado, pois a Política de Segurança só fala dos equipamentos corporativos (recursos fornecidos pela empresa) e precisa ser híbrida e tratar dos dois cenários. Assim, o colaborador vai estar ciente claramente do seu dever de proteger a informação da empresa em qualquer dispositivo, seja corporativo, particular ou de terceiro.

No mínimo tem que ter regra que aborde o dever de bloqueio com senha, automático, sobre apagamento remoto, dever de backup na rede, uso de antivírus e a impossibilidade de usar

softwares piratas para manusear informações da empresa, que todo conteúdo que não seja corporativo no equipamento é de exclusiva responsabilidade do proprietário, que é o colaborador. Podemos até, para garantir, fornecer a camada de softwares, incluindo de segurança com assinatura de um termo de responsabilidade.

CASO 2

CIO: A mobilidade é essencial para garantir a competitividade do nosso negócio. Podemos permitir que as equipes trabalhem remotamente?

Jurídico Tradicional: Não, isso é assumir muitos riscos para a empresa, principalmente trabalhistas. Vamos ser acionados para pagar uma fortuna de hora extra e sobreaviso, ainda não já jurisprudência suficiente a respeito, é melhor esperar.

Especialista Direito Digital: Sim, vamos analisar qual a necessidade de mobilidade e quais impactos para o negócio. Para quem tem cargo de confiança não há risco trabalhista de hora extra e sobreaviso. Com a mudança da CLT, art. 6º. Em 2011 é indiferente de quem é a propriedade do recurso. Logo, para equipe geral, aplica-se a Sumula 428 do Tribunal Superior do Trabalho, recentemente atualizada, que diz que o mero acesso ao recurso da empresa, por si só, não configura a sobrejornada, a não ser que haja comprovação de requisição de trabalho. Então podemos elaborar uma norma de mobilidade, gerar ciência da mesma e pôr algumas vacinas legais nas interfaces. Também seria bom implementar um manual para os gestores saberem redigir mensagens corporativas sem aumentar o risco trabalhista (ex: usando termos como para ontem, urgente, para agora), já que a informação pode chegar ao colaborador a qualquer momento.

CASO 3

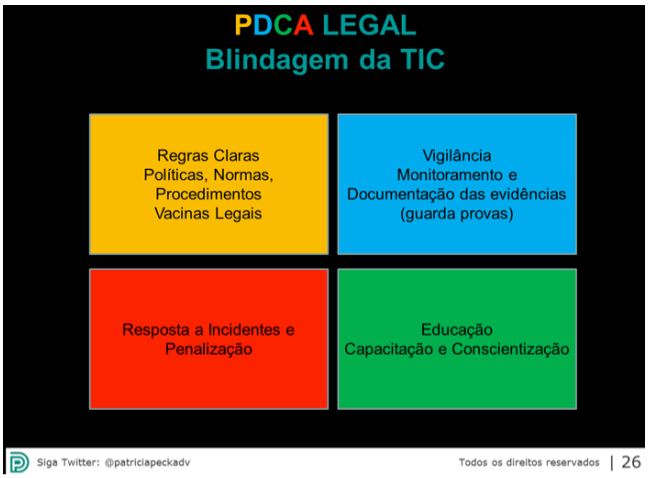
CIO: Precisamos aumentar o nível de segurança da empresa. Posso implementar uma solução de DLP ou isso têm risco de privacidade?

Jurídico Tradicional: Implementar mais monitoração? Mas isso vai invadir a privacidade, eu acho que não pode não. Inclusive, esse é o problema da mobilidade e do BYOD; como separar o que for íntimo do empregado do que for da empresa. Isso é muito arriscado.

Especialista Direito Digital: Se fizermos o aviso prévio escrito de ambiente físico e lógico com monitoramento ostensivo não. Aí estamos em conformidade com o Marco Civil, a Constituição Federal de 1988, art. 5º. Inciso X e com a Lei de Interceptação.

O mais importante é deixar claro que o DLP funciona com uma varredura automatizada, ou seja, por busca de tipo de imagem, hash de documento, palavra-chave, marca d´água, e não que seja uma varredura humana. Devemos inserir este aviso no acesso da VPN, acesso Remoto, rodapé de Email, toda equalquer interface inclusive de sistemas na nuvem. Assim, mesmo a pessoa acessando de fora da empresa, com equipamento pessoal, sabe claramente que a informação corporativa é monitorada, e não a sua máquina em si. Onde a informação da empresa for, a segurança acompanha.

Ciclo PDCA Legal para blindar a TI



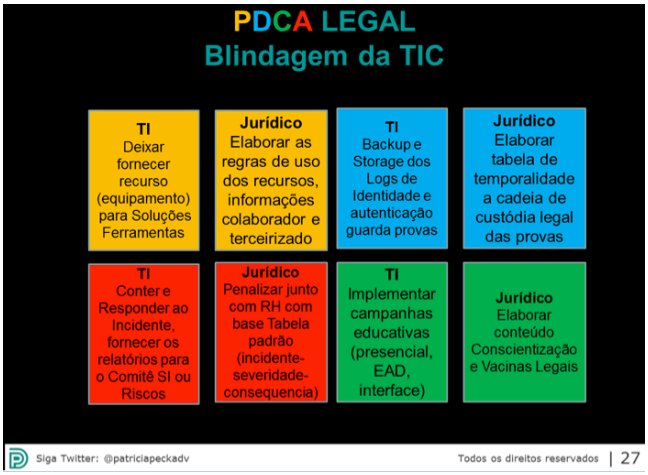


Tabela de Compliance

- Lei n.º 12.965/2014 (Marco Civil da Internet)
- Lei n.º 12.846/2013 (Lei Anti-Corrupção)
- Lei nº 12.850/2013 (Provas Eletrônicas)
- Decreto n.º 7962/2013 (Lei do Comércio Eletrônico)
- Leis de nº 12.735 e 12.77/2012 (Crimes Eletrônicos)
- Decreto n.º 7.845/2012 (Lei de Tratamento da Informação Classificada)
- Lei nº 12.551/2011 (Lei Home Office e Teletrabalho)
- Lei nº 12.527/2011 (Lei de Acesso a Informação)
- Lei nº 9.610/1998 (Lei de Direitos Autorais)
- Lei nº 9.609/1998 (Lei de Software)
- Lei n.º 9.296/1996 (Lei de Interceptação)
- Lei nº 9.279/1996 (Lei de Propriedade Industrial)
- Constituição Federal de 1988

Para concluir, o que o CIO precisa é construir uma relação que permita muito mais respostas, soluções legais de como mitigar riscos, do que continuar ouvindo NÃO do Jurídico.

Dizer simplesmente NÃO ou TEM RISCO não é pensar estrategicamente, nem tampouco apoiar o negócio. O Jurídico não deve ter medo de encarar os novos desafios trazidos pelos avanços tecnológicos, deve sim ter muito medo é de ficar obsoleto.

(*) Patricia Peck Pinheiro é advogada especialista em Direito Digital.
Twitter: @patriciapeckadv
Apresentadora do programa web “É Legal” (www.youtube.com/programaelegal)
Sócia fundadora do escritório Patricia Peck Pinheiro Advogados
(patricia.peck@pppadvogados.com.br) e da empresa de cursos Patricia Peck Pinheiro Treinamentos e do Instituto ISTART de Ética Digital que conduz o Movimento Família mais Segura na Internet (www.istart.org.br).

Fonte: CIO, em 27.05.2014.