Risi e Tusi são os pilares da segurança da informação

09/06/2006

Não obstante todos os riscos jurídicos inerentes à atividade

empresarial, os administradores deparam-se com uma nova realidade, na qual os meios eletrônicos disponibilizados aos seus prepostos como ferramentas de trabalho podem gerar responsabilidades trabalhistas, cíveis e criminais às corporações.

O Código Civil brasileiro preconiza que os preponentes são responsáveis pelos atos de quaisquer prepostos, praticados nos seus estabelecimentos e relativos à atividade da empresa, ainda que não autorizados por escrito, o que induz à possibilidade de responsabilização pessoal do administrador pelos atos ilícitos praticados pelos seus sistemas.

Diante dessa nova situação e sem legislação específica que regulamente o tema, resta às empresas como única estratégia de defesa a adoção de medidas jurídicas para proteção do patrimônio pela segurança da informação, bem como para resguardar as corporações quanto aos delitos praticados por meios digitais.

Após detalhados estudos técnico-jurídicos, concluiu-se que o plano estratégico da segurança da informação deve basear-se na elaboração de dois instrumentos que dão legitimidade à política de segurança adotada, quais sejam: RISI — Regulamento Interno de Segurança da Informação e Tusi — Termo de Uso dos Sistemas da Informação.

O regulamento terá por escopo atribuir legalmente responsabilidades, obrigações, penalidades, direitos e expectativas de acesso aos usuários. Entretanto, para ter efetivo reconhecimento legal, referido instrumento deve ser elaborado com base na utilização das mais atualizadas e confiáveis diretrizes de segurança mundial, tais como as normas ISO, em especial a ABNT NBR ISO IEC 17799:2005; BS 7799 do British Standard Institute; Data Protection Working Party, da União Européia; normativas nacionais (provimentos, resoluções e decretos); e ainda, observando as legislações ordinárias como o Código Civil, Código Penal, Consolidação das Leis do Trabalho, respeitando obrigatoriamente todas as conformidades legais.

Conjuntamente, é imprescindível a adoção do Tusi, instrumento aplicado aos usuários e/ou pessoas contratadas pela corporação, objetivando legitimar o controle de atividades, e outras considerações visando reforçar a inexistência de expectativa de privacidade, sempre de acordo com as tendências jurisprudenciais do direito nacional e internacional, especificamente para ações correlatas à segurança da informação.

Risi e Tusi são os pilares da segurança da informação, porém válido se faz ressaltar que existem outros documentos que necessariamente devem ser adaptados, sendo dois exemplos os contratos com empresas de Outsourcing e contratos de trabalho.

Além do objetivo principal de proteção da empresa, tais instrumentos refletem ainda na produtividade e qualidade do trabalho desenvolvido, pois por meio deles é possível adotar a monitoração de e-mails, restringir o uso da internet, limitar o uso das máquinas para fins estritamente profissionais, criando fatores inibidores para a navegação de entretenimento durante a jornada de trabalho.

Outrossim, não são raros os casos de concorrência desleal, inclusive no alto escalão, que lesam a empresa, com o envio de informações sigilosas da instituição para concorrentes por meio dos meios eletrônicos.

As vulnerabilidades são inúmeras: jurídicas, técnicas, éticas. Nesse novo cenário, cabe aos administradores a visão estratégica que reúna os profissionais das áreas jurídica, de tecnologia da informação e de recursos humanos, resguardando a corporação e criando uma cultura de proteção de dados por meio das medidas jurídicas adequadas.

Fonte: https://conjur.jumps.com.br/2006-jun-09/risi_tusi_sao_pilares_seguranca_informacao/