Tempos caóticos exigem medidas imediatas. Riscos, Teletrabalho e a LGPD, o que fazer agora?

SANDRO TOMAZELE

GRUPO JML

PESSOAS • SERVIÇOS • TECNOLOGIA

Desconsiderando as atuais questões políticas e sanitárias provocadas pelo coronavírus, focando no ambiente corporativo e tendo em vista que o nosso Brasil não pode parar, mas precisa adequar-se ao momento atual – mantendo os serviços fundamentais e movimentando a economia dentro do possível – é fato observado que muitas pessoas estão em teletrabalho (trabalho remoto ou *home office*) imbuídas deste espírito de superação.

Quando a covid-19 começou a ser detectada no país, em pouco tempo se instalou um ambiente caótico. Com poucas informações e pouca experiência a respeito de doenças que se espalham tão rapidamente e, ainda, com a demora da OMS em declarar o caso do coronavírus uma pandemia, ficamos (e não apenas o Brasil) desguarnecidos em relação a boas práticas e a protocolos para lidar com tal situação.

Uma das primeiras medidas de boa parte das organizações foi colocar os colaboradores em teletrabalho em resposta à chegada do vírus, uma resposta acertada na minha visão. No caos não há tempo para planejar, pesquisar, pensar, testar... As medidas precisam ser tomadas urgentemente. Não sendo eficazes, eficientes ou efetivas, tomam-se novas medidas em substituição ou em complemento à primeira. Prejuízo maior será verificado caso se apresente uma demora ao agir.

A solução

Passado o momento caótico, que é o que se verifica agora, entramos na fase complexa do problema. Já se têm informações necessárias, se detectaram procedimentos e protocolos a serem seguidos – ou novos foram definidos –, uma nova rotina organizacional foi estabelecida e assimilada e algumas melhorias nessas rotinas já são realizadas. Pronto! Pronto?

Não, ainda não está pronto! Os recursos disponíveis são limitados, é preciso priorizar as atividades e, mais do que nunca, gerenciar bem os recursos. GESTÃO! Esta é a chave para mitigar as perdas, os prejuízos, os danos e maximizar os ganhos, as entregas e aumentar a chance de se atingirem os objetivos de negócio.

Prever e solucionar

Neste ponto é que proponho a gestão de riscos. Não sob a forma tradicional, mas de maneira ágil, voltada para as atividades críticas ou para as que apresentam muitos ou grandes problemas. As dificuldades estão aí! E a gestão de riscos é uma ótima ferramenta para identificar problemas em potencial, priorizá-los e apontar soluções igualmente priorizadas. Se você tem um modelo de gestão de riscos corporativos, aplique-o, de forma simplificada, mas aplique-o agora! Se não tem, desenvolva um modelo simplificado e comece já!

Como lidar com questões relacionadas ao teletrabalho e a CLT? Quais são e como tratar os riscos relacionados à saúde do trabalhador em *home office*? O que fazer com a falta ou atraso de matéria-prima? Quais os riscos relacionados à qualidade dos serviços prestados e como resolvê-los ou minimizá-los? E quanto aos riscos de cybersegurança ou aos de segurança da informação, considerando os computadores menos protegidos, normalmente utilizados em teletrabalho?

É só um pequeno extrato contendo grandes temas, sob os quais emergem uma série de riscos. A gestão de riscos corporativos bem executada neste momento tem o potencial de sanar grande parte destas questões, priorizando os riscos dentre todos os que forem identificados.

Na minha organização, por exemplo, estamos planejando workshops virtuais com representantes das diversas unidades para executarmos um processo simplificado de gestão dos principais riscos que nos afetam nesta crise.

Proteção de dados pessoais

E quanto à LGPD, sua organização já havia iniciado os preparos? Este é um momento crítico para a proteção de dados pessoais. Considere que os acessos à rede interna de sua organização estão vindo de diversos computadores pessoais, utilizados pelos teletrabalhadores e que, provavelmente, não houve tempo hábil para aplicar neles os controles de segurança da informação adequados (*firewall* do sistema operacional, atualização dos programas, do sistema operacional e do antivírus, restrições de acesso, vulnerabilidades dos equipamentos de internet domésticos, entre outros).

Os cybercriminosos sabem muito bem que o ambiente doméstico é muito mais vulnerável do que o ambiente corporativo. Também sabem que agora existe uma forte possibilidade de que muitas conexões originadas em residências estejam acessando recursos críticos para as organizações (bancos de dados, sistemas restritos, dados sigilosos, dados pessoais etc.). Se os cuidados associados à segurança da informação não forem adequadamente avaliados – e, adivinhe? A base da segurança da informação é a gestão de riscos! – o risco de incidentes envolvendo dados pessoais será enorme, naturalmente, considerando a quantidade de vulnerabilidades que o teletrabalho, sem as devidas adequações, traz.

Nesta esteira, o CTIRGov[1], Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, mantém o seguinte informe em seu *site*:

> [...] está ocorrendo um aumento de diversas atividades de criminosos cibernéticos no intuito de obter vantagens através da disseminação de aplicativos maliciosos que enganam o usuário a instalar programas que na verdade são malwares voltados para capturar informações das pessoas ou exigir o resgate de arquivos que foram criptografados.

A IBM realizou uma pesquisa[2] sobre privacidade de dados em 11 países, incluindo o Brasil. A conclusão foi, segundo o estudo: *as pessoas estão insatisfeitas com a maneira com a qual a maioria das empresas lida com suas informações: no Brasil, 96% dos entrevistados acham que as organizações não tratam seus dados como deveria*. Ainda de acordo com a pesquisa, *60% dos brasileiros já teve dados vazados*.

1 CTIRGOV <https://www.ctir.gov.br/noticias/#2020CibercrimesCOVID19>, acessado em 27/3/2020.

2 <https://www.tecmundo.com.br/seguranca/148277-60-brasileiros-teve-dados-vazados-diz-pesquisa.htm>, acessado em 27/3/2020.

São números alarmantes. Com a obtenção ilícita de dados pessoais, os cybercriminosos podem, por exemplo, adquirir bens em nome dos titulares dos dados, como no caso ocorrido em Brasília[3] em que os fraudadores roubaram dados pessoais armazenados em vários órgãos do governo e com eles emitiram, junto ao Detran-DF, a segunda via da CNH, o que possibilitou o financiamento de veículos em nome das vítimas.

Segundo a reportagem do UOL[4], datada de 16/06/2019, já se observava uma alta nos casos de vazamentos de dados no governo federal, sendo que *esse tipo de incidente cresceu pouco mais de 19 vezes em seis anos e virou o segundo maior tipo de ataque sofrido pelos sistemas do governo federal*, segundo a reportagem.

Por fim, para citar um último exemplo de vazamento de dados pessoais, em matéria jornalística, o UOL[5] reporta que 2,4 milhões de usuários do SUS tiveram seus dados vazados na internet e faziam parte deste conjunto os nomes, endereços e números de CPF dos titulares dos dados envolvidos no incidente.

Legislação vigente

Vale destacar que a Lei de Crimes Cibernéticos, **Lei 12.737/2012**, já tipifica o crime de vazamento de dados pessoais de terceiros, com penas que variam de três meses a três anos de prisão. Além daquela Lei, o Código de Defesa do Consumidor, **Lei 8.078/1990**, também ampara o consumidor nos casos de vazamento de dados, manipulação indevida ou qualquer outro dano relacionado ao tratamento inadequado dos dados pessoais.

Então, é um terrível engano argumentar que, devido ao fato de a Lei Geral de Proteção de Dados Pessoais (LGPD), **Lei 13.709/2018**, não estar em vigor, a adequada proteção dos dados pessoais é dispensável. Como visto, não é!

E como começar a se preparar para a conformidade com a LGPD? No cenário atual de coronavírus e teletrabalho, realizar a gestão de riscos de segurança da informação, considerando todos os ativos (equipamentos, documentos, pessoas, processos de trabalho etc.), é o caminho mais indicado. Em seguida, recomendo a implantação do programa de governança de dados pessoais.

3 <https://g1.globo.com/df/distrito-federal/noticia/2019/09/24/operacao-investiga-esquema-que-fraudava-dados-em-tribunais-federais-e-do-df.ghtml>, acessado em 27/03/2020.

4 <https://www.uol.com.br/tilt/noticias/redacao/2019/06/16/vazamento-de-dados-cresce-e-ja-e--2-maior-ataque-digital-ao-governo-federal.htm >, acessado em 27/03/2020.

5 <https://www.uol.com.br/tilt/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios--do-sus-sao-vazados-na-internet.htm >, acessado em 2/03/2020.

O que o futuro reserva?

Note que vivenciamos um momento ímpar na história, estamos modificando e criando processos de trabalho, procedimentos, testando as estruturas e o conhecimento já adquirido, remodelando as culturas organizacionais. Os momentos de estresse, como o que ora se apresenta, são os mais propícios para melhorias de processos, inovações ou disrupções. Muitos deles permanecerão após se dissipar a crise iniciada pelo coronavírus.

Permanecerão porque o custo para retornar ao processo anterior é alto, ou porque a cultura da organização adaptou-se bem ao novo processo, ou porque o processo trouxe ganhos para a organização, ou por outros motivos. Se os aspectos relacionados à governança, aos riscos e à conformidade não forem observados desde agora, corre-se o grande risco de os trabalhos de adaptação num futuro próximo serem muito mais complexos e, por consequência, mais caros do que se iniciando agora. É como minha sábia avó materna, que Deus a tenha, dizia: **é melhor prevenir do que remediar!**

GRUPO JML

PESSOAS • SERVIÇOS • TECNOLOGIA

JULIANO JOSÉ LOPES

PRESIDENTE DO GRUPO JML

41. 99183-8386

@juliano.lopes@jmlgrupo.com.br

Deseja receber mais conteúdos sobre Gestão de Riscos Corporativos e LGPD?

Entre em contato diretamente comigo.

IRIS/2020

SOFTWARE DE GESTÃO DE RISCOS E LGPD

SAIBA MAIS

Acompanhe no portal da JML o lançamento do primeiro programa de gestão de riscos online