## Na Mídia

17/08/2022 | LexLatin

# Segurança da informação vai muito além do virtual

### Treinamentos orientam sobre os riscos envolvidos no ambiente off-line?

Tatiana Campello | Cecília Cunha

Estamos cada vez mais conectados e, por consequência, cada vez mais expostos a riscos cibernéticos/Canva

Em meio a tantas possibilidades de falha de sistemas de segurança cibernética, softwares maliciosos (*malwares*), que podem nos infectar com comunicações fraudulentas munidas de engenharia social e buscam obter informações confidenciais por e-mail, SMS, ligações telefônicas (*phishing, smishing, vishing*) e até mesmo por “novas ofertas de

emprego", que chegam por WhatsApp, acabamos deixando de prestar atenção a situações cotidianas que podem colocar igualmente em risco dados pessoais e informações confidenciais das empresas.

Estamos cada vez mais conectados e, por consequência, cada vez mais expostos a riscos cibernéticos, o que faz imprescindível a veiculação de informações sobre como podemos perceber esses riscos a tempo de impedir um incidente de segurança.

É preciso também ter atenção para não nos tornarmos alvos fáceis dos já conhecidos golpes virtuais, seja por um clique despretensioso em um link de domínio suspeito ou por um pagamento equivocado sem a devida atenção aos dados do boleto.

É inconteste que as empresas estão se movimentando a passos largos para implementar internamente treinamentos de segurança da informação, incluindo testes de *phishing*, apresentação de políticas e procedimentos específicos e gestão de incidentes e crises a partir da simulação de invasão aos sistemas. Mas será que esses treinamentos estão atentos e orientam sobre os riscos envolvidos também no ambiente *off-line*?

O mundo mudou, mas nem tanto. A vida presencial segue concomitante à virtual, na qual estamos cada vez mais inseridos, e é, claro, de suma importância estarmos atentos aos processos de digitalização, informatização e virtualização das informações para viabilizar o acesso a esses dados de forma segura através das redes e de sistemas.

Também é preciso discutir sobre os riscos existentes na manipulação física dos dados no dia a dia e no momento de torná-los digitais, ainda que exista uma falsa sensação de que os riscos envolvidos no ambiente tangível sejam menores ou menos relevantes.

Muito se fala sobre a instalação de antivírus nas máquinas para proteger informações sigilosas e confidenciais que estão no ambiente digital, mas pouco se diz sobre o descarte consciente de papéis com mecanismos de trituração, quando há a digitalização destes, por exemplo. Assim como muito se fala sobre criptografia, mas pouco se diz sobre os riscos envolvidos ao se esquecer uma pasta ou um caderno contendo anotações confidenciais e dados pessoais de clientes que não devem ser acessados por terceiros.

A LGPD (Lei Geral de Proteção de Dados Pessoais), ou Lei nº 13.709/18, traz como princípios a segurança e a prevenção, que refletem medidas de segurança da informação técnicas e administrativas, além das preventivas, que buscam proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O universo de possibilidades é, portanto, infinito se pensarmos que, na mesma medida que um acesso não autorizado pode se dar por uma invasão de um *cracker* ao dispositivo corporativo, também pode ocorrer se alguém não autorizado tiver acesso a uma tela desbloqueada de um colaborador, a um documento deixado sobre a mesa, ou ainda a uma conversa com informações confidenciais fora do ambiente adequado.

Fato é que estamos cada vez mais preparados para lidarmos com a informação online ou disposta em ambiente virtual, mas esse preparo deve se estender às informações no ambiente físico.

Não adianta a política de segurança da informação da empresa e os sistemas todos adotados incentivarem de modo automático a mudança de senha de três em três meses, imporem regras específicas e a necessidade de caracteres especiais se, ao modificar a senha, o funcionário a anota em um *post it* e a cola na tela do dispositivo.

A falta de segurança da informação é mais escalável quando ocorre no ambiente digital, porque o acesso, em tese, é a um volume muito maior de dados através de sistemas e data centers, com processamento de informações infinitamente maior - ainda mais em um contexto de Big Data em que vivemos.

Contudo, não se pode esquecer de potenciais consequências dos incidentes de segurança no mundo físico e de analisar quais poderiam ser evitados através da implementação de medidas administrativas de segurança da informação relativamente simples.

Vale aqui a reflexão se os treinamentos e a conscientização interna estão abordando, na mesma medida, a tecnologia, os processos e as pessoas, que são as bases para que se consiga atingir um nível satisfatório de governança e de confiabilidade (integridade, confidencialidade e disponibilidade) em relação à proteção das informações. Porque, ao se falar em segurança da informação, não adianta cobrir o tronco descobrindo os pés.

***Tatiana Campello é sócia das áreas de Propriedade Intelectual, Inovação e Tecnologia e de Privacidade de Dados e Cibersegurança no Demarest Advogados. Cecília Cunha é advogada da área de Privacidade de Dados e Cibersegurança no Demarest Advogados.***