Por Ana Paula Cardoso Pimenta (*)

As recentes notícias sobre incidentes de segurança da informação, com uma ocorrência no Superior Tribunal de Justiça, uma tentativa no Tribunal Superior Eleitoral e o ocorrido na última sexta-feira (27), contra o Tribunal Regional Federal da 1ª Região, chamaram atenção para os riscos de segurança da informação, com vazamentos de dados que podem alcançar as organizações, inclusive as EFPCs.

De acordo com a LGPD – Lei Geral de Proteção de Dados Pessoais, em seu artigo 46, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Além dos padrões técnicos de TI – Tecnologia da Informação e SI – Segurança da Informação, que podem ser adotados com o objetivo de proteger os dados pessoais, é importante que todo o corpo funcional das entidades esteja atento aos riscos de vulnerabilidades de dados pessoais aos quais as organizações estão expostas.

A necessidade de prevenção, que é um dos princípios da lei, impõe que os usuários que trabalhem para os agentes de tratamento enxerguem além do óbvio, já que os sinais indicadores das catástrofes e riscos aparecem e podem ser percebidos por qualquer empregado.

Para isso, é importante que os colaboradores sejam informados e estejam à vontade para cooperar,

pois, de quem menos se espera, poderá ser percebida a falha ou o sinal de invasão. É indispensável, portanto, envolver as equipes com conscientização e treinamentos, fazendo com que se sintam parte do que importa, para que sejam um time alerta e comprometido. E isso serve para todos os tipos de riscos.

Seguem algumas dicas que podem ser adotadas nos treinamentos e trabalho remoto:

Ter cuidado com o acesso às VPNs – Rede Privada Virtual – manter o acesso logado somente durante o tempo do expediente de trabalho, para evitar ataques de hackers oportunistas);

Não acessar VPNs ou arquivos corporativos em nuvem por dispositivos em locais de rede wi-fi pública;

Usar senhas corporativas com critérios de criação capazes de prevenir a dedução de terceiros e frequentemente renová-las;

Ter atenção à atuação dos hackers por meio de engenharia social – técnica usada pelos cibercriminosos em geral para obter informações, invadir sistemas e ter acesso a dados pessoais, como: e-mail de bancos pedindo para trocar senha, cavalo de tróia enviado por meio de “ofertas irrecusáveis”, links conhecidos com alteração de caracteres quase imperceptíveis, entre outros.

Essas são apenas dicas que, caso a caso, poderão ser adotadas e/ou complementadas, a depender da realidade das organizações.

Apesar de não existir a possibilidade de evitar todos os riscos, o componente humano é também fundamental para que as entidades fechadas estejam adaptadas à LGPD. Os dirigentes podem e devem estimular a cultura da proteção de dados como uma forma de evidenciar o cumprimento da lei, já que a adoção de medidas administrativas, nos termos do art. 46, é um dever imposto aos agentes de tratamento.

Além disso, ainda que nenhuma pessoa jurídica esteja livre de sofrer um ataque cibernético ou outro tipo de incidente de segurança, certamente a Agência Nacional de Proteção de Dados exigirá que as organizações demonstrem que tomaram as medidas possíveis para prevenir esses riscos e que reagiram prontamente na hipótese da ocorrência de um incidente de segurança, inclusive, fazendo as comunicações cabíveis quando evidenciados riscos ou danos relevantes aos titulares.

(*) **Ana Paula Cardoso Pimenta** é Data Protection Officer e advogada do SERPROS Fundo Multipatrocinado.

Fonte: Abrapp em Foco, em 30.11.2020