Por Jeferson D’Addario (*)

Com o crescimento da tecnologia e para oferecer aos pacientes mais comodidade, muitos hospitais, laboratórios e consultórios têm utilizado diversas ferramentas digitais como aplicativos para marcações de consultas, sites para verificação de resultados de exames, além de sistemas para autorização de procedimentos médicos. O fluxo e compartilhamento de informações nesse setor é amplo, por isso a necessidade em garantir a segurança e proteção de dados dos pacientes.

Para prejudicar ou enfraquecer a infraestrutura de qualquer país, o setor de saúde está entre os alvos de ataques clássicos, de acordo com o National Institute of Standards and Technology (NIST). Localizado nos Estados Unidos, o instituto também lista como alvos empresas e instituições em áreas como setor financeiro, governo, transporte, alimentação e telecomunicações.

Apesar dos cuidados com a segurança empresarial e corporativa, existem ameaças cibernéticas que podem ocorrer nesse ambiente como ransomwares, uma forma de código malicioso capaz de sequestrar dados utilizando criptografia. Os criminosos podem exigir resgate por meio de bitcoins ou outra criptomoeda e, mesmo assim, não existe a garantia de que a vítima terá os dados recuperados. Além disso, ainda há tentativas de invasão hacker, sequestro de dados, vírus, fraudes e tentativas de roubo de identidade. Por isso a preocupação com a cibersegurança no setor de saúde está cada vez mais em evidência.

Segundo a pesquisa Global Digital Trust Insights Survey 2022, realizada pela PwC, 83% das empresas brasileiras estimam elevar os investimentos em cibersegurança. É importante destacar que tanto o tema cibersegurança, quanto a gestão de segurança da informação, não são voltados somente para a tecnologia da informação. Para garantir a segurança cibernética na área da saúde, é necessário que toda a empresa esteja envolvida nos processos e protocolos. Só assim será possível estabelecer boas práticas, desde a direção até os colaboradores.

A cibersegurança precisa estar integrada ao planejamento estratégico da organização. Os gestores precisam enfrentar as dúvidas quanto ao tema, buscar conhecimento para poder então agir de forma consciente contra os incidentes cibernéticos. É importante ter um profissional especializado para coordenar uma equipe na gestão de segurança da informação ou avaliar a possibilidade de contratar uma empresa que faça consultoria para desempenhar essa função na organização.

Estabelecer regras de segurança da informação são fundamentais para manter o cuidado com os dados e garantir a melhoria contínua. Além disso, a empresa precisa ter a responsabilidade de educar os colaboradores e mostrar, através de exemplos, o quanto a gestão de segurança pode ser eficaz e ajudar as pessoas como um todo.

A identificação de riscos junto com gestores e equipes técnicas, pode ser um caminho para manter os parâmetros aceitáveis da empresa. Para isso, o ideal é sempre se preparar para o pior cenário que a companhia pode enfrentar. Criar cenários de incidentes e planos de gerenciamento de crises, podem preparar as equipes para reagir com cautela caso isso ocorra no ambiente real.

Com o propósito de auxiliar as organizações, independente de setor ou tamanho, a protegerem seus dados, existe o padrão ISO 27001, que normatiza o sistema de gestão da segurança da informação. A estruturação de processos pode beneficiar as empresas no que diz respeito a segurança de dados, além de oferecer menos riscos para quem investe na organização.

Para estar de acordo com a Lei Geral de Proteção de Dados (LGPD), as organizações da área da saúde precisam aceitar que é necessário o investimento em segurança da informação e cibersegurança. Desta forma, além das empresas mostrarem maturidade corporativa, elas garantem aos clientes e pacientes que estão dentro das normas de segurança e confiabilidade.

(*) **Jeferson D’Addario** é CEO do Grupo DARYUS, professor coordenador do MBA em Gestão e

Tecnologia em Segurança da Informação (GTSI), do MBA em Gestão de Risco e Continuidade de Negócios (GRCN) do Instituto DARYUS de Ensino Superior Paulista (IDESP) e consultor sênior em Continuidade de Negócios e Gestão de Riscos.

Fonte: FBH, em 09.09.2022