Apenas 30% das empresas brasileiras estão totalmente em conformidade com a lei, segundo pesquisa da E-commerce Brasil

Em vigor desde agosto desse ano, a Lei Geral de Proteção de Dados (LGPD) tem causado alguns transtornos nas empresas para colocar em prática os processos internos, necessários para a adequação. Agora, as instituições podem sofrer sanções financeiras caso descumpram a lei, gerando uma verdadeira corrida contra o tempo.

Segundo Ricardo Mesquita, especialista em segurança da informação e gerente de TI na Howden Harmonia Corretora de Seguros, pouco se fala no que realmente importa ser feito. “É necessário fazer uma relação entre as exigências da lei e o que as empresas precisam providenciar, antes mesmo de falarmos em LGPD”, explica.

Ainda de acordo com o especialista, as empresas devem focar em três pilares para se organizar internamente: Segurança cibernética, Governança e Documentação da lei.

Mais do que nunca, as empresas precisam investir na segurança de seus ambientes computacionais, implementando ou melhorando seus firewalls, softwares de antivírus, programas de monitoramento em tempo real de todo o ambiente de rede, links de internet, sistemas de backup e sistemas de contingência, pois paradas críticas em casos de invasões e vazamentos de dados podem deixar a empresa vulnerável. “A segurança cibernética é o primeiro passo para proteger os dados e evitar a exposição inadequada dos mesmos”, informa Mesquita.

A Governança estabelece políticas claras de segurança da informação, como procedimentos de acessos a ambientes críticos, políticas de descarte de informações e de senhas, criptografia e controle de atualizações de segurança dos sistemas operacionais. “Esses são alguns dos documentos necessários para manter todo o ambiente informático sob controle, pois de nada adianta que as empresas tenham um aparato tecnológico moderno sem a gestão adequada”, esclarece.

Ainda de acordo com Mesquita, a implementação da governança de segurança em uma empresa não é simples, por isso “é recomendável contratar uma consultoria especializada para adequá-la ou seguir um framework - biblioteca de melhores práticas -, como a ISO 27001, entre outros, que podem ajudar a reunir os documentos para aplicar a governança”.

Uma recomendação importante é que haja um ‘casamento’ entre o hardware e software implementados, com instruções a todos os colaboradores sobre como utilizar os sistemas, como proceder em casos de emergências, quem deve ser acionado e quais são os caminhos para uma possível retomada em casos de perda de dados e ataques cibernéticos.

O terceiro pilar é a documentação da LGPD, última etapa deste início de adequação das empresas. “É fundamental que haja a definição de um comitê de privacidade, com a nomeação de um Encarregado de Proteção de Dados (ETD) e que seja feito o mapeamento de todos os processos internos de segurança”, diz Mesquita.

Ele complementa ainda, dizendo que “vale observar que as certificações existentes no mercado, como as ISO 27000, podem acelerar este processo, embora não sejam exigidas pela LGPD. Além de diminuir o nível de dificuldade da implementação, elas ajudam no entendimento dos funcionários, que precisam mudar de comportamento, o que nem sempre é uma tarefa fácil”.

O especialista dá algumas dicas valiosas de procedimentos necessários e inerentes às etapas de adequação, já que algumas situações podem acontecer a qualquer momento e é preciso saber o que e como fazer.

1) **Quais são as práticas que devem ser evitadas pelos funcionários no dia a dia para a não exposição de dados?**

O que não fazer: deixar dados expostos em papel ou em bilhetes, receber dados pessoais via Whatsapp, e plataformas de streaming (Meet, Zoom, Teams, etc), por e-mail, em planilhas eletrônicas sem senha, ou qualquer outro meio sem a permissão do dono da informação. É necessário ainda garantir a destruição dos dados pessoais, se assim for solicitado.

2) **O que fazer em caso de emergência, como uma invasão ou falha de segurança?**

A lei é bastante clara nesse sentido: o encarregado de proteção de dados da empresa deve comunicar imediatamente a Autoridade Nacional de Proteção de Dados na evidência de um vazamento de informações, sensíveis ou não, sendo que para isso há um documento que deve ser preenchido para informar as evidências, a natureza e o volume dos dados, entre outras informações necessárias.

3) **Quais são os documentos LGDP que as empresas precisam ter?**

Existem cerca de 30 documentos, processos e formulários que as empresas precisam ter para

estarem adequadas à LGPD. Um deles é o Aviso Geral de Privacidade e Proteção de Dados Pessoais, que deve constar no site da empresa.

O Comitê de Privacidade, formado por profissionais para dar apoio ao encarregado de Proteção de Dados (DPO), também deve ser informado e estar contido em um estatuto, para que todos saibam quem são os responsáveis pela Segurança Cibernética.

É preciso estabelecer as políticas de gravação de dados, de compartilhamento de dados, de resposta a incidentes e preparar um questionário para fornecedores e parceiros, que também devem estar em dia com a segurança da informação.

Em caso de perda de dados ou invasão, a empresa deve preparar o Relatório de Impacto de Proteção de Dados, documento que precisa ser entregue à Agência Nacional de Proteção de Dados, caso exista qualquer perda ou invasão.

É importante ressaltar que toda a equipe de funcionários precisa ser treinada para que fique claro para a auditoria que a empresa está comprometida com a proteção dos dados.

Poucas empresas se prepararam para a implementação da LGPD e, com a pandemia, alguns processos sofreram atrasos. O home office e os procedimentos inerentes ao trabalho remoto tornaram a necessidade de investir em segurança cibernética ainda maior, reforçando a adequação à lei.

Um exemplo a ser seguido

Para atender às exigências da LGPD, Mesquita explica como foi o processo de adequação que permitiu a Howden Harmonia estar à frente e se adequar antes do término do prazo estipulado. “Os procedimentos tiveram início em meados de 2019, quando foi contratada uma consultoria especializada para nos auxiliar na construção do projeto de adequação à lei. Nesse período foi criado o Comitê de Privacidade e nomeado o encarregado de proteção de dados. Também foi elaborado o portal de repositório de informações, para mapear todos os processos, além de providenciarmos toda a documentação com políticas e procedimentos ajustados aos processos da empresa. Foi necessário adquirir equipamentos de segurança e softwares de gestão para a realização de processos internos, além da realização de um treinamento para todos os colaboradores sobre os procedimentos para proteção dos dados e segurança da informação” detalha o especialista.

A empresa está em constante auditoria da matriz, em Londres, que auxiliou na implementação da governança de segurança da informação, o que elevou o Score de segurança ao patamar desejado pela sede da Howden Harmonia.

Sobre Ricardo Mesquita

Ricardo Mesquita é gerente de TI, especialista em segurança da informação, infraestrutura de redes e proteção de dados pessoais. É tecnólogo em processamentos de dados pelo Colégio Pentágono e bacharel em administração de empresas pela Universidade Metodista de São Paulo. É Certificado em Data Professional Officer, gestão de segurança de rede, ITILv2 , PCI e System Engineer pela Microsoft. Mesquita atua no mercado de tecnologia há mais de 30 anos, tendo em seu histórico profissional passagens por empresas como Volkswagen do Brasil, Microsoft, Telemar, SAP, Banco Itaú, nas áreas de TI, Negócios, Estratégia e Operações de Risco envolvendo Sistemas Críticos.

Howden Harmonia Corretora de Seguros

A Howden Harmonia nasceu da fusão entre o Grupo Howden, maior grupo de corretores independentes do mundo, e a Harmonia Corretora de Seguros, que há 40 anos no mercado brasileiro foi pioneira na prestação de serviços de consultoria e administração de riscos. Hoje, a Howden Harmonia é uma das maiores corretoras do país e conta com presença em São Paulo,

Campinas, Poços de Caldas e Blumenau. Sua atuação é focada nas áreas de Grandes Riscos e Gestão de Benefícios, mantendo parcerias com as principais seguradoras e operadoras do mercado para garantir o melhor atendimento aos seus clientes, nacionais e multinacionais.

Fonte: Segs, em 06.10.2021