LGPD

Deliberação CAD-A-003/2020, de 06/10/2020 - *Dispõe sobre a criação do Comitê Gestor da Privacidade e Proteção de Dados no âmbito da Universidade Estadual de Campinas.*

Introdução

Informação é um tipo de ativo importante, valioso para qualquer organização. Ataques virtuais têm se tornado cada vez mais comuns no Brasil e no mundo, muitos exemplos de vazamentos de dados pessoais tiveram grande repercussão nos noticiários nos anos de 2020 e 2021. Normalmente, os invasores buscam um regaste por dados pessoais e, de acordo com o *Annual Cybersecurity Report* da Cisco, 53% dos ataques resultam em danos de US$ 500.000 ou mais. Esses ataques podem se tornar cada vez mais comuns, visto que cada vez mais pessoas estão sendo conectadas à rede, de forma cada vez mais profunda.

Em virtude disso, a proteção desse tipo de dado convém diretamente ao bem estar da sociedade. Visando proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, em 2018 foi aprovada a Lei Geral de Proteção de Dados Pessoais, ou somente Lei LGPD, para entrar completamente em vigor em agosto de 2020. Sendo aplicada a qualquer tipo de empresa, sendo pública ou privada, internacional ou nacional. Os principais pontos da Lei LGPD são:

- Uma regra para todos: criação de um cenário de segurança jurídica válido para todo o Brasil;
- Consentimento do usuário;
- Definição do conceito: estabelecer, de maneira clara, o que são dados pessoais;
- Consentimento de menor: consentimento dos pais ou responsáveis; • Abrangência extraterritorial: organizações devem seguir as regras dentro ou fora do país;
- Transferência internacional: o compartilhamento é permitido caso outro país também proteja dados;
- Fiscal centralizado: ANPD;

- Responsabilidade: são definidos agentes de tratamento de dados e funções;
- Gestão de falhas e riscos;
- Transparência: vazamentos de dados devem ser informados; • Penalidades rígidas;
- Finalidade e necessidade: quesitos que devem ser informados aos usuários.

O foco principal deste material é a segurança e sigilo dos dados, que é a primeira seção do capítulo VII da Lei. Nele, determina-se que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Além disso, o agente torna-se obrigado a garantir a segurança da informação prevista na Lei em relação aos dados pessoais. Os sistemas implementados para esse fim devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei. As sansões para o não cumprimento da Lei podem ser de avisos até multas pesadas.

Os três pilares para a segurança da informação são a integridade – garantir que a informação é integra e livre de adulterações em todos os momentos do processo; confidencialidade – somente pessoas autorizadas devem ter acesso à determinada informação; e disponibilidade – a informação deve estar disponível para uso onde e quando for necessária. Com a aplicação desses, a entidade estará mais protegida contra vulnerabilidades tecnológicas, físicas e humanas e suas ameaças, podendo ser estas naturais, involuntárias ou voluntárias.

Dentro da Unicamp, esses pilares devem estar intrínsecos nas atitudes dos funcionários que tem acesso a elas, tendo em mente que não devem ser compartilhados arquivos com dados pessoais quando não for necessário e para pessoas não autorizadas, além disso, é necessário ter cópias de segurança, para o caso de o arquivo ser corrompido e as informações sejam adulteradas. Para que essas informações não sejam extraviadas, é recomendável compartilhá-las somente com o e-mail institucional e para e-mails institucionais,

evitando assim acessos fora da universidade. Uma outra forma de manter o arquivo em segurança é convidar um e-mail para colaborar com o arquivo, ao invés de mandar um link de compartilhamento, ou então restringir o acesso a este.

Para se adequar à Lei, o passo inicial é entendê-la, pois facilitará muito o processo de aplicação na organização. Além disso, deve-se entender qual é o cenário dessa entidade perante a lei e saber como pode ser afetado por ela, pois dependendo do ramo de atividade diferentes medidas devem ser tomadas. Com

esses passos tomados, deve ser criada uma comissão ou equipe de trabalho, com funcionários dos setores que tratam dados pessoais e também a direção da entidade, assim o projeto pode ser mais bem direcionado, assim como seu foco e objetivos.

É importante que sejam mapeados todos os dados tratados dentro da entidade, sendo isso uma parte básica da Lei LGPD. Os dados e seus fluxos devem ser conhecidos para que a implementação dos processos de segurança seja possível. Além disso, os dados devem ser classificados como dados pessoais, dados pessoais sensíveis ou dados pessoais de crianças e adolescentes.

Tendo isso em vista, é necessário a adoção de um Sistema de Gestão e Segurança da Informação (SGSI). Através dele, serão aplicadas estratégias, planos, políticas, medidas, controles e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. A norma ISSO 27001 adota um modelo para descrever a estrutura de um SGSI.

Caso deseje se informar mais sobre a Lei LGPD, acesse os seguintes sites:

https://www.pg.unicamp.br/mostra_norma.php?id_norma=23852

https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-dedados-pessoais-lgpd

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd

https://www.serpro.gov.br/lgpd/cidadao/voce-ja-protege-seus-dados-pessoais

https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd