Segurança com LGPD

1. A IMPORTÂNCIA DA LGPD:
A lei foi criada com o objetivo de proteger dados pessoais e a privacidade dos indivíduos, tanto nos meios físicos como digitais.

2. A LGPD é responsabilidade de quem?
Todos são responsáveis pela privacidade de dados e pela segurança das informações.
Porteiros, vigilantes, TI, setores administrativos, etc. Todos aqueles que têm contato ou que fazem tratamento de dados pessoais de terceiros.

3. Regra principal da lei geral de proteção de dados:
A regra principal é a FINALIDADE.
Todos os dados de pessoas físicas somente devem ser utilizados para a finalidade específica para a qual foram coletados.

4. O que é tratamento de dados?
É tudo que fazemos com os dados que acessamos ou que temos contato. São tipos de tratamento de dados: a coleta, o acesso, a reprodução, o processamento, o armazenamento, a eliminação, a utilização, o arquivamento, a eliminação, distribuição, controle da informação, entre outros.

5. Quais são os dados que devem ser protegidos?
Os dados são divididos em duas categorias, são elas:

5.1. Dados pessoais:
São aqueles que permitem identificar uma pessoa (nome, endereço, número de documento, etc).

5.2. Dados pessoais sensíveis:
São aqueles dados íntimos e que, em caso de eventual incidente, podem trazer consequências mais gravosas aos direitos e liberdades dos titulares. Esses dados necessitam de um cuidado muito maior.
A lei elenca os seguintes dados como sensíveis: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

6. Cuidados necessários:

a) Cuidado com anotações ou informações que você deixa a vista, guarde-as em local seguro.
b) Não comente nada sobre a vida particular ou dados de alguém.
c) Não tire fotos ou compartilhe informações sobre as pessoas que você atende.
d) Tudo isto se aplica a clientes, celebridades, funcionário ou qualquer pessoa física
e) Se perceber uso indevido da senha ou sistemas, comunique ao seu superior imediatamente.
f) O e-mail deve ser usado somente para fins profissionais.
g) Caso receba um e-mail suspeito, mesmo que seja de uma pessoa conhecida, contate a TI.
h) Atenda as determinações da empresa com relação ao uso dos sistemas e acesso aos dados.
i) Em caso de armazenamento de dados em documento físico, os dados devem permanecer pelo tempo necessário para suas finalidades e o documento deve ser posteriormente entregue ao cliente ou, caso este não detenha interesse, entregue ao seu superior para o necessário descarte.
j) No caso de armazenamento de dados em formato digital, a responsabilidade pela gestão dos dados é dos clientes, os quais detêm o controle do banco de dados.
k) VOCÊ É RESPONSÁVEL POR MANTER EM SIGILO OS DADOS QUE ACESSA.

7. Constatando alguma irregularidade, comunique imediatamente ao encarregado através do e-mail: ***protecaodedados@epavi.com.br***

GRUPO EPAVI 50 ANOS
VIVER BEM É VIVER COM SEGURANÇA.