ALVES FERNANDES

PROTEÇÃO DE DADOS PESSOAIS, CIBERSEGURANÇA E O COVID-19

CONHEÇA OS PRINCIPAIS IMPACTOS PARA SUA EMPRESA

O Projeto de Lei 1179, que visa instituir um Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado (RJET) no período da pandemia do Covid-19, foi aprovado pelo Senado e será apreciado pela Câmara dos Deputados.

Segundo seu texto-base, a vigência da Lei Geral de Proteção de Dados entrará em vigor em 1° de janeiro de 2021, com a ressalva das sanções administrativas, as quais entrarão em vigor em 1° de agosto de 2021.

A LGPD instaura uma profunda transformação no sistema de proteção de dados pessoais no Brasil.

Mesmo que ainda não tenha entrado em vigor, a LGPD já esta sendo aplicada por várias empresas na coleta, uso e compartilhamento de dados.

A proteção de dados pessoais exige atenção ainda maior no cenário atual, onde a adoção de medidas para contenção do COVID-19 são prioridade mundial.

Tanto os órgãos públicos, como as empresas privadas, necessitarão processar mais e diferentes tipos de dados, em especial, os dados sensíveis de saúde relacionados ao COVID-19.

A PROTEÇÃO DE DADOS PESSOAIS E O COMBATE AO COVID -19

APLICAÇÃO DA LGPD EM TEMPOS DE PANDEMIA

	VISITANTES/CLIENTES	COLABORADORES
Hipóteses que autorizam o manuseio de dados referentes ao estado de saúde – os quais são classificados como dados pessoais sensíveis. A LGPD prevê tratamento diferenciado nesses casos - o consentimento a ser fornecido, de forma específica e destacada, para finalidades específicas.	Consentimento específico e em destaque	Cumprimento da obrigação legal dos art. 168 e 169 da CLT.
	Proteção da vida ou da segurança física do titular ou de terceiros	Proteção da vida ou da segurança física do titular ou de terceiros

TRATAMENTO DE DADOS DE SAÚDE RELACIONADOS AO COVID 19

- **Quando é possível coletar os dados sobre o estado de saúde dos colaboradores e visitantes?**

É possível realizar a coleta estritamente com a finalidade preservar a saúde de todos os colaboradores, clientes, parceiros e terceiros no âmbito empresarial.

- A coleta de informações de estado de saúde dos indivíduos deve ser realizada por um profissional da saúde.

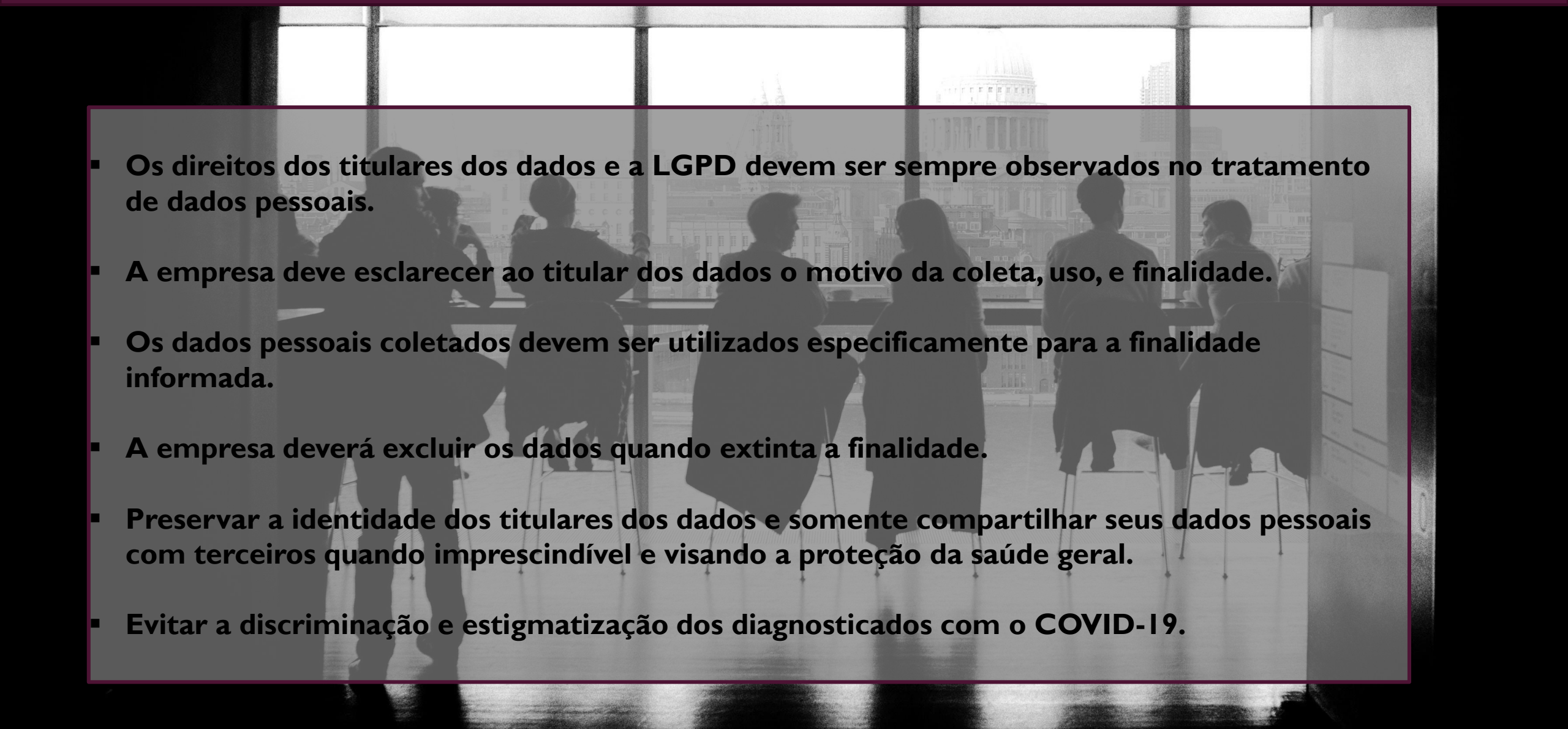
- **Com quem os dados podem ser compartilhados?**

Poderão ser compartilhados com as autoridades de saúde com a finalidade exclusiva de evitar a propagação e preservar a saúde, seguindo os protocolos oficiais.

Dentre as medidas instituídas para o combate ao Covid-19, a Lei Federal nº 13.979/20 dispõe sobre a obrigação das empresas privadas e órgãos públicos compartilharem os dados essenciais à identificação de pessoas com suspeita ou infectadas pelo COVID-19, com a finalidade exclusiva de evitar a sua propagação.

As empresas privadas deverão compartilhar os dados pessoais quando solicitados pelas autoridades sanitárias.

CUIDADO IMPORTANTE - EQUILIBRAR A PRIVACIDADE COM O INTERESSE PÚBLICO



- **Os direitos dos titulares dos dados e a LGPD devem ser sempre observados no tratamento de dados pessoais.**
- **A empresa deve esclarecer ao titular dos dados o motivo da coleta, uso, e finalidade.**
- **Os dados pessoais coletados devem ser utilizados especificamente para a finalidade informada.**
- **A empresa deverá excluir os dados quando extinta a finalidade.**
- **Preservar a identidade dos titulares dos dados e somente compartilhar seus dados pessoais com terceiros quando imprescindível e visando a proteção da saúde geral.**
- **Evitar a discriminação e estigmatização dos diagnosticados com o COVID-19.**

CIBERSEGURANÇA E O HOME OFFICE

Como manter a segurança de dados durante ao home office?

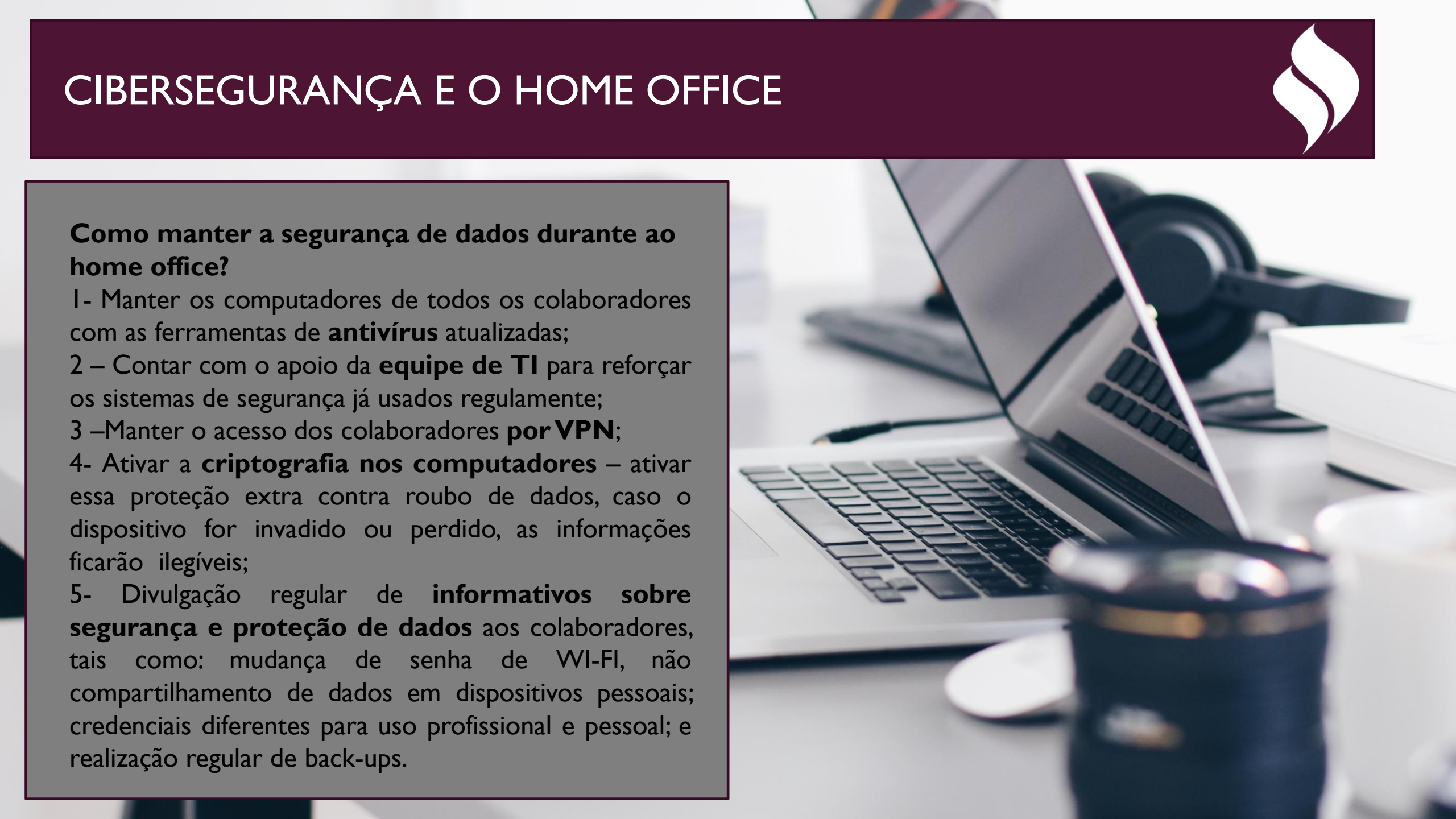
1- Manter os computadores de todos os colaboradores com as ferramentas de **antivírus** atualizadas;

2 – Contar com o apoio da **equipe de TI** para reforçar os sistemas de segurança já usados regulamente;

3 –Manter o acesso dos colaboradores **por VPN**;

4- Ativar a **criptografia nos computadores** – ativar essa proteção extra contra roubo de dados, caso o dispositivo for invadido ou perdido, as informações ficarão ilegíveis;

5- Divulgação regular de **informativos sobre segurança e proteção de dados** aos colaboradores, tais como: mudança de senha de WI-FI, não compartilhamento de dados em dispositivos pessoais; credenciais diferentes para uso profissional e pessoal; e realização regular de back-ups.



CIBERSEGURANÇA - PRINCIPAIS RISCOS

- **Cuidado extra com Hackers** – o uso de **spam** (e-mails e mensagens com informações e links falsos) e **phishing** (endereço de e-mail que tenta se assemelhar ao real) irá se adaptar ao home office, portanto, toda a equipe deve ficar alerta e confirmar solicitações suspeitas por telefone com quem as enviou.

- **Golpistas se passando por colegas de trabalho** – aproveitando que muitas empresas estão em trabalho remoto, golpistas podem se passar por colegas **solicitando dados sobre operações e clientes**. Evitar responder a mensagens incomuns sem a confirmação verbal de parceiros e superiores.

VAMOS CONVERSAR MAIS A RESPEITO?

Elizabeth Alves Fernandes
Elizabeth@alvesfernandes.com

MBA Executivo - IESE Business School, 2017.
Doutorado em Direito - USP.
Mestrado em Direito - USP.
LLM – European College - Itália.
Bacharel em Direito - USP, 2005.

ALVES FERNANDES
+55 11 **3842-3930**
Rua Afonso Braz, 864, 4º Andar, Vila Nova Conceição
04511-010, São Paulo - SP, Brasil