Expressão comum no vocabulário de muitos brasileiros nesse cenário de pandemia, o Home-Office exige cuidados especiais por parte das empresas em relação às Políticas de Compliance, e também ao tratamento de dados pessoais, devido a Lei Geral de Proteção de Dados.

No material abaixo, compartilhamos 7 dicas simples, porém relevantes para prevenir vazamentos e manter sua empresa nos trilhos da LGPD.

- **Cuidado com o wifi**

As redes de wi-fi público são inegavelmente muito úteis, no entanto, podem apresentar riscos à segurança digital das informações corporativas por não haver muita segurança sob as conexões de seus usuários. Os roteadores das redes públicas, muitas vezes, não possuem precauções sob seus roteadores ou mesmo possuem protocolo de segurança, como um bom firewall e senha de rede. Mesmo com senha, essas tendem a ser facilmente acessíveis.

Quando ao wi-fi de casa, segue a próxima dica.

- **Não utilize a mesma senha.**

Não utilize a mesma senha para diferentes logins de contas e serviços, pois há grande chance de alguém mal intencionado descobri-la e então ter acesso a todas as contas do mesmo usuário.

Além disso, é importante não fazer uso de senhas fracas ou obvias demais, pois também traz risco a sua segurança digital.

- **Leia toda a política de privacidade.**

Caso não tenha o suporte em casa e precise utilizar algum programa diferente, do que já pré-estabelecido pela empresa, leia as políticas de privacidade, pois elas explicam como seus dados pessoais serão processados, caso utilize aquela ferramenta, assim você possui controle sob as informações que repassa para outras redes que não pré-estabelecidas pela corporação.

Ex.: É muito comum o uso de sites para conversão ou para diminuir o tamanho de

documentos, mas ao usar esses sites tenha consciência de que você está transferindo o conteúdo para o titular do domínio do site e isso traz um grande risco a confidencialidade de documentos corporativos.

- **Armazenamento, protocolo de salvar docs.**

O armazenamento em nuvem de segurança, pré-estabelecida pela empresa, é de suma importância, pois além de disponibilizar informações, facilitar seu compartilhamento e possuir backup, traz também maior segurança aos dados corporativos. Ainda, esses dados são criptografados e em regra acessíveis apenas por aqueles com autorização prévia. Não salve documentos e informações no desktop do computador, pois com esse tipo de armazenamento não possui a mesma proteção que a nuvem.

- **Vedar expressamente impressão**

A proteção de dados pessoais também se aplica a documentos em papel, por isso é importante vedar qualquer impressão de informações em folha para que não fique disponível para terceiros. Documentos em papel geram risco mesmo em caso de descarte irregular.

- **Meio de comunicação apenas por canais de habilitados pela empresa.**

Alerta: importante vedar qualquer tipo de comunicação de informações corporativas por meio de WhatsApp. No mundo ideal, informações corporativas deveriam ser trocadas apenas em mecanismos formais de propriedade da empresa (ou licenciados para ela). Se utilizar o whats, telegram ou programa equivalente, não compartilhe documentos e restrinja a informações cujo conteúdo não gere risco para a empresa.

Ferramentas como Slack são muito utilizadas por corporações que se preocupam com a segurança de informações trocadas entre seus funcionários. Devido ao grande número de funcionário de Home Office é de extrema importância alinhar discursos e valores da corporação, sendo necessário um meio seguro para essa troca.

- **Criar mecanismos de limitação de utilização pessoal de computador corporativo.**

De acordo com o Tribunal Superior do Trabalho “Empresas podem fiscalizar computadores e e-mails corporativos, desde que haja proibição expressa, em regulamento, da utilização para uso pessoal.” Assim. É boa prática empresarial, criar normas de uso para o computador corporativo e até mesmo bloquear alguns acessos, por haver grande risco de retenção de vírus e *pishing* (quando alguém, má intencionado, se passa por uma pessoa confiável para que a vítima clique em um link e tenha todas as informações do seu computador roubadas).