Diante da necessidade de trabalho remoto e da proteção de dados pessoais, existem práticas de segurança cibernética que podem ser adotadas por advogados.

Nesse sentido, o objetivo deste texto será de apresentar como a **segurança cibernética** deve ser aplicada no meio jurídico.

Antes de tudo, o conceito de segurança cibernética, também chamada de cibersegurança, consiste na prática proteger as pessoas e empresas contra os ataques virtuais.

Em melhores palavras, é a prática de proteção de ativos de informação contra ameaças e ataques relacionados à invasão, roubo e manipulação de dados ou arquivos pessoais e empresariais.

Dessa forma, durante as práticas remotas de trabalho, todos os profissionais, com foco nos(as) advogados(as) precisam praticar a cibersegurança.

A CIBERSEGURANÇA E O TRABALHO REMOTO JURÍDICO

No geral, os(as) advogados(as) se adaptaram muito bem aos requisitos de distanciamento social e à natureza imprevisível da pandemia.

Dessa forma, foram adicionadas novas ferramentas baseadas em uma nuvem aos **arsenais tecnológicos** de seus escritórios de advocacia que tornam possível a transição para o trabalho remoto quando necessário.

No entanto, devido à natureza confidencial de seu trabalho, as praticidades de trabalhar remotamente devem necessariamente estar em conformidade com suas obrigações éticas e legais.

Nesse sentido, para que haja segurança e confidencialidade no trabalho jurídico, existem práticas que podem ser realizadas na colaboração do alcance desse objetivo.

16 PRÁTICAS PARA GARANTIR A CIBERSEGURANÇA JURÍDICA

Nesse tópico, será apresentada uma lista de práticas recomendadas de cibersegurança.

Vale ressaltar que, o rol, embora longo, não é exaustivo. Sendo assim, existem outras práticas que podem ser adotadas para a garantia da segurança.

Portanto, sem mais delongas, aqui está a lista completa de melhores práticas de segurança cibernética:

- Exija senhas fortes para proteger dados e acessar dispositivos
- Use autenticação de dois fatores ou multifatoriais para acessar informações
- Evite usar Wi-Fi não-inseguro ou público ao acessar ou transmitir informações de seu cliente
- Use uma rede virtual privada (VPN) ao acessar ou transmitir informações de seu cliente
- Use e mantenha o **software antivírus** e antimalware atual
- Mantenha todos os softwares atualizados: ao ler esse tópico, instale atualizações imediatamente
- Forneça ou exija que os funcionários usem laptops seguros e criptografados para o trabalho
- Não use unidades USB ou outros dispositivos externos, a menos que sejam propriedade da empresa ou sejam fornecidos por uma fonte confiável
- Especifique como e onde os dados criados remotamente serão armazenados e como serão armazenados em backup
- Salve dados permanentemente apenas na rede do escritório, não em dispositivos pessoais
- Use fornecedores confiáveis para serviços na nuvem
- Criptografe e-mails ou use outras informações confidenciais contra divulgação não autorizada
- Criptografe registros eletrônicos, incluindo backups contendo informações confidenciais, como informações pessoalmente identificáveis
- Não abra anexos suspeitos ou clique em links incomuns em mensagens, e-mails, tweets, postagens ou anúncios online
- Use sites que tenham maior segurança sempre que possível
- Não tenha conversas relacionadas ao trabalho na presença de dispositivos inteligentes, como assistentes de voz

Com a adoção dessas práticas, haverá uma diminuição na possibilidade de ataques cibernéticos e a garantia da proteção de dados confidenciais.

Em conclusão, estas são as principais formas de buscar pela **segurança cibernética**. Continue acompanhando nosso blog e siga nosso Instagram para mais conteúdos.