DINO - Divulgador de Notícias

Como um software jurídico pode dar segurança ao compartilhamento de informações

Conheça os cuidados que devem ser observados ao compartilhar informações e saiba como um software jurídico pode ajudar nessa tarefa.

30/09/2016 13:44:30

Advogados trabalham com muitas informações estratégicas. Os clientes confiam aos profissionais dados sigilosos que ficam registrados na nuvem, seja na troca de e-mails ou no uso de serviços de armazenamento, como o Google Drive. Se esse conteúdo cair em mãos erradas, tanto o cliente quanto o escritório de advocacia podem enfrentar sérios problemas. Para evitar essa vulnerabilidade é necessário uma série de cuidados ao compartilhar informações, e um software jurídico, como o SAJ ADV, pode ajudar nessa tarefa.

Levando em conta os resultados desastrosos que podem surgir do vazamento de informações, os advogados devem tomar todas as precauções para garantir que elas estejam seguras. É preciso ter consciência que a falta de segurança dos dados pode acarretar outro problema: a quebra de confiança do cliente. Mesmo que eles não sejam diretamente prejudicados, podem sentir-se inseguros ao perceberem que seus dados não estão efetivamente protegidos. Além do uso de um software jurídico, escritórios de advocacia de qualquer tamanho devem seguir as recomendações que veremos a seguir.

Software jurídico e a prevenção de vazamento de dados

A tecnologia da informação evolui cada vez mais rápido, trazendo facilidades e criando novos hábitos para as pessoas. Contudo, o mesmo movimento é responsável pela criação de novas ameaças, principalmente no ambiente virtual. Nesse contexto, mediante as responsabilidades éticas que afetam a relação dos advogados, é necessário contar com ferramentas que garantam a segurança dos dados do escritório e dos clientes. E por mais que existam uma série de opções genéricas, somente um software jurídico poderá atender as necessidades específicas da relação advogado-cliente. Isso acontece porque essa é uma plataforma pensada para atender às principais demandas do segmento, concentrando em um único e seguro local as informações críticas cruciais para o desempenho das tarefas jurídicas.

A prevenção do vazamento de dados se dá na medida em que o software jurídico é capaz de

reforçar a segurança das informações dos clientes. A ferramenta deve oferecer modos de autenticação que assegurem que apenas usuários autorizados acessem esses dados. Como consequência, o fortalecimento da proteção de dados irá poupar tempo e dinheiro para um escritório de advocacia, além de contornar o problema do know-how tecnológico limitado. O programa pode solucionar alguns desses desafios de segurança, assegurando a privacidade dos clientes.

Cuidados com os dados de comunicação e dados de acesso

Geralmente há dois tipos de dados eletrônicos que devem ser protegidos. O primeiro deles pode ser classificado como “dado de comunicação”, e consiste nas informações transmitidas de um computador a outro, por uma troca de e-mails, por exemplo. O segundo tipo são os chamados “dados de acesso”. Eles podem ser definidos como as informações armazenadas localmente no computador ou em arquivos do escritório. Para mantê-los seguros, existem técnicas e ferramentas, como um software jurídico, que dificultam o acesso de pessoas não-autorizadas.

Dados de comunicação:

A internet é uma ferramenta indispensável, mas é necessário estar sempre consciente de seus riscos. Os rastros deixados na rede podem abrir caminhos para invasões e roubo de dados. Um software jurídico e outras ferramentas, como antivírus e firewalls, são capazes de minimizar esses riscos. O cuidado com as informações sigilosas de clientes deve ser redobrado. Todos os colaboradores do escritório também devem estar cientes de suas responsabilidades quanto à segurança desses dados. Também é importante evitar alguns métodos, como colocar informações no título do e-mail ou compartilhar o conteúdo com muitas pessoas. Isso aumenta o risco de pessoas não-autorizadas conseguirem acesso a dados privilegiados.

O e-mail é a técnica mais comum de transferência de arquivos digitais e uma das mais fáceis de proteger. Há várias maneiras de garantir a segurança da sua comunicação eletrônica. Sistemas de criptografia e o uso de protocolos seguros como SSH (Secure Socket Layer) e SSL (Secure SHell) ajudam a garantir que as informações estão a salvo.

O Secure Socket Layer, é um padrão de segurança global, com o qual é criado um canal protegido para transmitir os dados. O SSL pode ser reconhecimento pelo símbolo do cadeado dourado ao lado da URL do site no navegador. Nesse caso, são os sites que devem adquirir e exibir o certificado digital SSL/TSL para os usuários. Por sua vez, o SSH (Secure SHell) é um protocolo que permite o acesso virtual seguro ao servidor. Em outras palavras, é quando um computador acessa e controla remotamente outro. Porém, criptografando e protegendo os dados trafegados entre as máquinas.

Dados de acesso:

Com a popularização dos computadores pessoais, as pessoas se acostumaram a armazenar suas informações em um único lugar de fácil acesso. Apesar da conveniência, esse procedimento não é do mais seguros. Isso porque com apenas uma senha uma pessoa mal-intencionada pode roubar ou usar de modo indevido esses dados.

Um exemplo é o do advogado que compartilha seu token (certificado digital) com a secretária, para que ela faça o peticionamento digital em nome dele. O certificado digital equivale a uma garantia de identidade, ou seja, que as atividades estão sendo realizadas realmente pelo advogado. Com esse tipo de informação, qualquer pessoa pode realizar diferentes atos, como celebrar contratos, efetuar compras e vendas, transações bancárias, acessar as informações do advogado na receita federal, entre outros, no nome do titular do certificado digital.

Por isso, é preciso pensar em políticas de segurança e boas práticas para o escritório de advocacia. Combinar tecnologia e conscientização é uma estratégia eficaz para garantir a segurança de quaisquer dados.