



Entenda como a criptografia protege dados em softwares jurídicos

27/02/2018

Uma preocupação recorrente de advogados ao procurar por um software jurídico, seja para o seu [escritório de advocacia](#), seja para [departamentos jurídicos de empresas](#), é a condição segurança à qual seus dados estarão submetidos quando armazenados no sistema.

Informações de processos, documentos de clientes, documentos dos próprios advogados, entre outras informações confidenciais, estarão cadastradas no software jurídico e qualquer violação pode ter consequências irreversíveis. Nesse sentido, de que modo um software jurídico pode assegurar ao escritório ou departamento jurídico total segurança no armazenamento de dados?

Neste conteúdo você vai encontrar:

[Software jurídico é seguro?](#)

[O que é criptografia?](#)

[Criptografia simétrica ou assimétrica?](#)

[Como identificar se meus dados estão seguros?](#)

Software jurídico é seguro?

O que define se um software jurídico é seguro são os protocolos de certificação digital. Estes certificados garantem que a comunicação e armazenamento de informações em nuvem aconteça por meio de mecanismos de criptografia, como acontece no ProJuris para Escritórios e no ProJuris para Empresas, por exemplo.

O que é criptografia?

Nas civilizações antigas, como Roma, Egito e Grécia, a escrita cifrada permitia que estes povos se comunicassem por meio de códigos que só eles conheciam. Dessa forma, evitavam que informações importantes fossem roubadas por outros povos.

A base da segurança digital consiste nisso. Informações cifradas para impedir que os dados do usuário caiam nas mãos erradas. A criptografia garante que todas as informações estejam disponíveis para o usuário e somente para o usuário.

Criptografia é o mecanismo que traduz informações inteligíveis em informações ilegíveis e desordenadas para qualquer agente externo. Isso impediria, por exemplo, que um hacker acessasse suas informações. Seu funcionamento se dá por meio da codificação das informações e embaralhamento dos dados estruturais.

Criptografia simétrica ou assimétrica?

Existem dois tipos de criptografia, simétrica e assimétrica.

- **Criptografia simétrica:** a mais usada na internet, a criptografia simétrica ficou famosa por ter sido utilizada pelos aliados durante a Segunda Guerra Mundial. É a chamada

criptografia de ponta-a-ponta, porque se fundamenta na ideia de que uma chave usada para ocultar uma informação seja a mesma utilizada para mostrá-la em outra ponta (no caso de troca de mensagens, como é o caso do WhatsApp).

- **Criptografia assimétrica:** foi inventada para corrigir um erro básico da criptografia simétrica. Na criptografia simétrica, a mesma chave é utilizada para garantir a troca de informações entre dois canais, o que facilita a interceptação de terceiros. A criptografia assimétrica é fundamentada em chaves distintas e complementares.

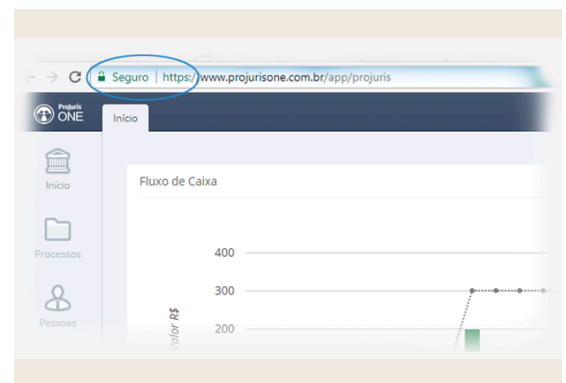
O ProJuris para escritórios, assim como o ProJuris para empresas é certificado pelo protocolo SSL, onde a criptografia assimétrica cria uma chave de sessão que é utilizada na criptografia simétrica.

Como identificar se meus dados estão seguros?

Identificar se um site ou software jurídico on-line tem um protocolo de certificação digital é muito simples. Todo site ou sistema protegido tem, em frente à sua url, o código “https:” e a palavra “Seguro” acompanhada de um cadeado verde, que funciona como uma espécie de carimbo de certificação digital.

Além de se certificar de que seus dados, informações, documentos e processos estão em um ambiente digital protegido, há outros tópicos relativos à segurança aos quais o advogado deve estar atento.

Armazenamento: certificados digitais garantem a proteção contra a interceptação de informações, mas não dizem nada a respeito de armazenamento dessas informações. O que garante que, da noite para o dia, todos meus dados estejam perdidos?



Para sua segurança, se certifique de que o software jurídico trabalha com informações salvas em nuvem. **Cloud torna o backup dispensável.** As informações não estão salvas em um meio físico, mas sim em diferentes servidores, garantindo que possa ser acessada em qualquer lugar do mundo, e somente por você.

Autenticidade de documentos eletrônicos: assim como documentos físicos, em papel, os documentos digitais precisam ser autenticados para atribuir a eles uma validade legal. Neste conteúdo, falamos sobre como garantir essa autenticidade e garantir que o processo eletrônico não obstrua a rotina do advogado, mas a torne muito mais eficiente:

Requisitos para processos eletrônicos confiáveis: todo Processo Judicial eletrônico (PJe) precisa ser seguro e garantir que as informações, além de serem verídicas, não possam ser acessadas indevidamente. Neste conteúdo, listamos os requisitos que tornam um PJe confiável.

No ProJuris é assim. A combinação de protocolos de segurança digital, mecanismos de criptografia e armazenamento em nuvem, o escritório ou departamento jurídico está 100% seguro.



Fonte: <https://conjur.jumps.com.br/2018-fev-27/entenda-criptografia-protege-dados-sofware-juridicos/>