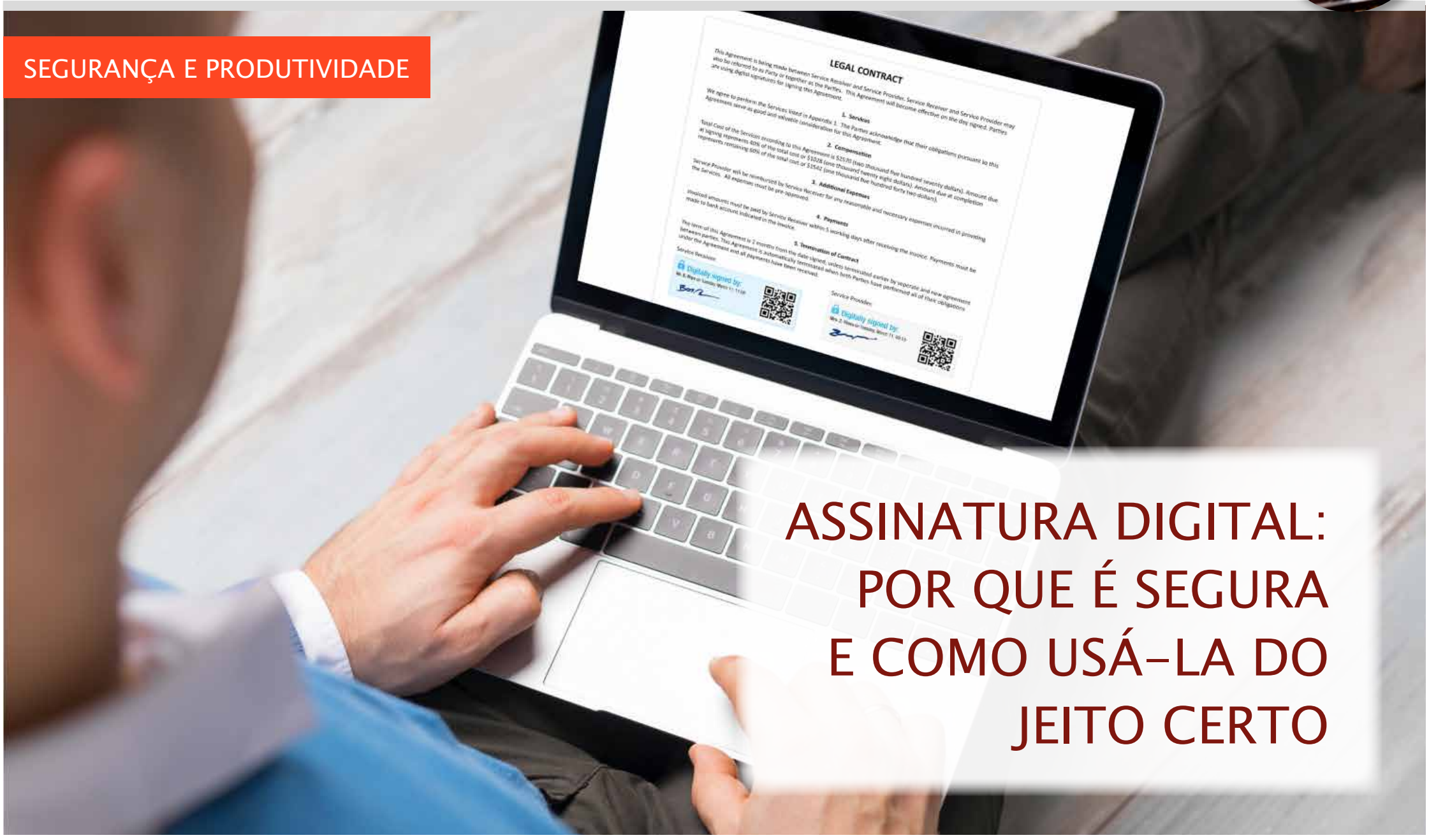
Kaspars Grinvalds_CANVA



SEGURANÇA E PRODUTIVIDADE

ASSINATURA DIGITAL: POR QUE É SEGURA E COMO USÁ-LA DO JEITO CERTO

Nos últimos 12 meses, mais e mais organizações aceleraram seus processos de transformação digital devido ao impulso para o trabalho remoto. Novos dados revelam que 57% dos líderes latino-americanos afirmam que planejam adotar um modelo operacional diferente do que tinham antes da pandemia. O objetivo é garantir a segurança dos funcionários e obter maior produtividade.

Stephen Davidson (*)

Entre os líderes latino-americanos pesquisados, mais da metade (58%) afirma que sua principal motivação é criar uma experiência geral melhor para os funcionários, de acordo com um novo White Paper da IDC patrocinado pela Unisys Corporation (NYSE: UIS), intitulado Digital Workplace Insights ™: Paridade digital e de experiência para apoiar a força de trabalho híbrida.

No Brasil, o trabalho remoto pode chegar a 22,7% das ocupações existentes, algo em torno de 20,8 milhões de pessoas, segundo estudo do Ipea, publicado no início de junho. Para chegar a essa conclusão, o Ipea examinou mais de 400 funções diferentes, replicando uma metodologia da Universidade de Chicago, que produziu um ranking global sobre teletrabalho com 86 países. Nesse ranking, o Brasil ocuparia a 47ª posição, com 25,7% das ocupações passíveis de serem realizadas remotamente.

A assinatura digital de documentos, ou o processo de indivíduos ou organizações adicionando uma assinatura eletrônica a um documento, permitiu uma nova flexibilidade e eficiência de negócios, eliminando a necessidade de uma assinatura manuscrita. Essas assinaturas eletrônicas permitem que as partes assinem em qualquer lugar, a qualquer hora, economizando tempo, proporcionando às empresas uma vantagem competitiva e melhorando a experiência do cliente.

Na verdade, muitos processos de negócios mudaram para sempre como resultado da pandemia, mas sem a segurança adequada, a transformação digital é vulnerável a ataques e possíveis falhas de serviço. As assinaturas digitais oferecem mais comodidade do que as assinaturas tradicionais e, se feitas corretamente, podem ser ainda mais seguras para garantir a confiabilidade e validade jurídica na hora de assinar contratos, acordos ou qualquer outro tipo de documento.

Por que usar um serviço de assinatura digital de documentos? – Garantir a confiança entre as partes é fundamental para indivíduos e organizações que conduzem negócios. Com a redução das interações face a face, há uma necessidade maior de construir confiança e validação em documentos assinados para trocar seus contratos com segurança, especialmente quando não se usa o papel.

Utilizar uma solução de assinatura de documentos o ajudará a construir essa confiança e segurança, eliminando a necessidade de interações pessoais e assinaturas manuscritas. Além disso, apenas com um provedor certificado você pode assinar documentos que sejam juridicamente vinculativos e reconhecidos como iguais a uma assinatura manuscrita.

Vantagens de um serviço de assinatura digital de documentos:

- Integra-se com muitos sistemas de gerenciamento de documentos, permitindo o manuseio suave das transações de assinatura.
- Permite fluxos de trabalho online e trabalho remoto, eliminando a necessidade de mensageiros e assinaturas manuscritas.
- Legalmente válido para a maioria das formas de transação/assinatura.
- Permite assinaturas em qualquer lugar, a qualquer hora, em qualquer dispositivo.
- Fornece identidade validada para que o indivíduo assine com segurança ou para que as organizações processem a assinatura em massa / e-selos.
- Pode ser usado para assinar todos os tipos de documentos.
- É altamente seguro.
- Reduz o impacto ambiental da impressão e envio pelo correio.
- Diminui o custo e o erro humano.
- Melhora a competitividade de uma organização.
- Aumenta a satisfação e a experiência do cliente.

- Como a assinatura digital de documentos é segura com a PKI - Ao trabalhar remotamente ou com partes em locais diferentes, é fundamental garantir que seus documentos e contratos sejam transferidos com segurança, e você pode verificar com quem está fazendo negócios. Uma das maneiras mais seguras de proteger a assinatura de documentos digitais é por meio da tecnologia de infraestrutura de chave pública (PKI), que prova a identidade e a autenticidade do remetente e evita adulteração do documento.

Com a PKI, uma assinatura digital é um hash criptografado de sua mensagem ou documento que permite aos destinatários verificar se o conteúdo não foi alterado e verificar a identidade do signatário. Ao contrário de uma assinatura digitalizada, uma assinatura digital protegida com PKI é virtualmente impossível de falsificar.

Para garantir que um documento seja legalmente válido, uma solução de assinatura de documento deve estar em conformidade com os rígidos padrões governamentais. As operações europeias da DigiCert são um Provedor de Serviços de Confiança Qualificado (QTSP) credenciado, o que significa que somos credenciados para fornecer certificados digitais qualificados para o mais alto nível de assinatura digital: o Qualificado de Assinatura Eletrônica.

Uma Assinatura Eletrônica Qualificada atende aos requisitos do regulamento eIDAS (No. 910/2014), que é reconhecido em todo o mundo como o equivalente legal a uma assinatura manuscrita. Na verdade, o nível de confiança é tão alto que o regime Qualificado é um padrão de referência para identidade eletrônica, assinaturas eletrônicas e supervisão de Autoridade de Certificação em todo o mundo. Além disso, certos setores têm regulamentações, como HIPAA, que exigem trilhas de auditoria para garantir que os documentos assinados estejam em conformidade.

tolgart_CANVA

Assine documentos com DigiCert® Document Signing Manager – Como líder global em PKI, a DigiCert desenvolveu o Document Signing Manager, uma solução multifuncional fácil para assinatura digital de documentos. Com isso, as organizações obtêm maiores níveis de soluções confiáveis de assinatura digital que atendem aos mais altos padrões legais da UE, juntamente com recursos locais dedicados e especialização. Não importa onde você esteja no mundo, a DigiCert tem uma solução de assinatura para o seu caso de uso.

Permite assinaturas digitais em conformidade com padrões globais rigorosos, incluindo EU eIDAS, Swiss ZertES e os requisitos técnicos da Adobe Approved Trust List (AATL). Além disso, por ser uma solução em nuvem, não há necessidade de investir em hardware; você só paga pelo que consome. A assinatura digital de documentos elimina a necessidade de assinaturas manuscritas, diminui custos, economiza tempo e deixa uma pegada ambiental menor.

(*) - É gerente sênior de Governança, Risco e Conformidade da DigiCert (www.digicert.com).