

## **Transformação digital e evolução do local de trabalho impulsionam demanda por certificados digitais e PKI, aponta Estudo de Tendências Globais em PKI e IoT de 2021 da Entrust**

*A falta de propriedade, recursos e habilidades continua a desafiar as implantações de PKI*

**São Paulo, 10 de novembro de 2021** – Estimulado por mudanças organizacionais, o uso corporativo de PKIs (Public Key Infrastructure) e certificados digitais nunca foi tão grande, embora as habilidades relacionadas ao gerenciamento de PKIs sejam historicamente escassas, de acordo com pesquisa do Ponemon Institute, patrocinada pela [Entrust](#), líder global em identidade, pagamentos e proteção de dados confiáveis.

O Estudo Global de Tendências em PKI e IoT de 2021 também revelou que os profissionais de TI continuam testemunhando falta de propriedade clara, recursos e habilidades como os principais desafios para a implantação e gerenciamento de PKIs.

PKIs estão no centro de quase todas as infraestruturas de TI, permitindo segurança para iniciativas digitais críticas, como nuvem, implantação de dispositivos móveis, identidades e Internet das coisas (IoT). Nesse cenário, PKIs são a chave para permitir a transformação digital que essas tecnologias sustentam, o que ganhou ainda mais os holofotes ao longo da pandemia global e seu impacto nas práticas de trabalho.

### **Incentivadores e desafios para a adoção de PKIs**

Quando se trata das principais tendências para o impulsionamento e a implantação de aplicativos usando PKIs, a Internet das Coisas (IoT) continua sendo a tendência de mais rápido crescimento, citada por 47% dos entrevistados, com os serviços baseados em nuvem ocupando o segundo lugar entre os maiores incentivadores, citados por 44%, seguidos pelo consumidor móvel em terceiro, com 40%.

O principal desafio para a implantação e o gerenciamento de PKIs é a falta de propriedade clara - citado por 71% dos entrevistados. Os entrevistados levantaram essa questão como um dos principais desafios nos últimos 5 anos, indicando uma área de preocupação-chave para muitas empresas.

Recursos e habilidades insuficientes foram classificados como segundo e terceiro desafios, respectivamente, com 51% e 46%, respectivamente. Da mesma forma, os principais desafios para permitir que os aplicativos utilizem PKIs foram as atuais PKIs serem incapazes de oferecer suporte a novos aplicativos (55%) e a falta de habilidades (46%).

As áreas com maior expectativa de mudança e incertezas são as mais recentes, como a Internet das Coisas (IoT) - que ocupou o primeiro lugar para 41% dos pesquisados. A segunda e a terceira áreas mais citadas foram mandatos e padrões externos (37%) e mudanças nas tecnologias de PKIs (27%).



# ENTRUST

SECURING A WORLD IN MOTION

“Ao longo dos anos em que temos feito este estudo, está claro que a lacuna entre a crescente demanda pela adoção de PKIs e os desafios que a dificultam parece estar crescendo”, disse o Dr. Larry Ponemon, presidente e fundador do Ponemon Institute.

“Tal lacuna tem o potencial de exacerbar as dores que as organizações já sentem e criar brechas em suas estratégias de segurança. Quando consideramos que os ambientes são mais distribuídos com trabalho remoto, nuvem e IoT, fica claro que há uma necessidade imediata de muitas organizações para obter visibilidade adicional, automação e controle centralizado”.

## **O surgimento das identidades de máquina**

Os certificados TLS/SSL para sites e serviços voltados ao público são o caso de uso mais citado para credenciais de PKIs (81% dos entrevistados). Redes privadas e aplicativos VPN ficaram em segundo lugar (67%, contra 60% em 2020) e a segurança de e-mail ficou em terceiro (55%, contra 51% em 2020), ultrapassando a segunda e terceira posições do ano passado, ocupadas por aplicativos de nuvem pública e autenticação de usuários corporativos. Esses resultados destacam a mudança de foco em garantir que trabalhadores remotos e cargas de trabalho de TI distribuídas possam ser mantidos em segurança.

A pesquisa também revelou que o número médio de certificados emitidos ou adquiridos por organizações ainda está crescendo, com alta de 4,3% de 56.192 em 2020 para 58.639 este ano (e aumento de 50% desde 2019). Embora o número de identidades humanas protegidas tenha sido relativamente baixo nos últimos anos, agora existem mais identidades de máquina (dispositivos e fluxos de trabalho) do que humanas. Esse crescimento em identidades de máquina é impulsionado principalmente pelo uso crescente de IoT, serviços em nuvem e novos aplicativos.

Independentemente do motivo do crescimento, quanto mais certificados uma organização precisa gerenciar, mais crítico se torna o gerenciamento adequado. Com um em cada cinco (20%) dos entrevistados afirmando usar uma lista de revogação manual de certificados e quase um terço (32%) admitindo que não têm uma técnica de revogação de certificados, essas organizações correm o risco de ficar vulneráveis a ataques e enfrentar interrupções em sistemas críticos e a consequente interrupção dos negócios e custos associados.

“PKIs nunca tiveram uma demanda tão alta - seja pela pressão para garantir uma força de trabalho remota ou híbrida no ano passado, seja pelo crescimento contínuo de IoT e serviços baseados em nuvem”, disse John Metzger, vice-presidente de marketing de produto e segurança digital da Entrust. “Ao mesmo tempo, as habilidades e os recursos necessários para implantar e gerenciar PKIs continuam escassos - um problema agravado pela falta de propriedade organizacional clara sobre as implantações de PKIs. Para lidar com essa complexidade, as organizações precisam primeiro de uma estratégia e, em segundo lugar, de produtos para dar suporte a essa transformação. Isso significa



# ENTRUST

SECURING A WORLD IN MOTION

que elas precisam de uma parceira como a Entrust, que não só tem as capacidades tecnológicas, mas também a herança e a experiência para ajudar a ter sucesso nesse ambiente”.

## Principais tendências no Brasil

- Com relação à forma com a qual PKIs são implantados dentro das organizações, os entrevistados no Brasil citaram a autoridade de certificação corporativa interna em 57% das respostas e a autoridade de certificação privada hospedada externamente como um serviço gerenciado em 20% das respostas.
- Quando questionados sobre as técnicas de revogação implantadas, 32% dos entrevistados globalmente responderam nenhuma. No Brasil, enquanto 63% apontaram maior probabilidade de usar protocolos de status de certificado online (OCSP), 33% responderam estar mais propensos a utilizarem CRLs automatizados.
- A penetração da PKIs é chave na estrutura central de TI da organização moderna. E, dada a falta de pessoal qualificado e clareza organizacional, combinada com a falta de práticas consistentes de revogação, é preciso ressaltar os riscos à saúde e integridade dessas CAs e dos aplicativos corporativos centrais importantes que usam seus certificados.
- No Brasil, a média de ACs implantadas por empresa é de 5,99, o que posiciona o país na antepenúltima posição neste quesito entre os 17 países que participaram do estudo.
- Em relação do número de diferentes aplicações (ex. e-mail, autenticação de rede etc.) para as quais PKIs gerenciam certificados, o Brasil aparece na 5ª colocação entre os 17 países estudados, com média de 8,64.
- Em relação aos três maiores desafios na implantação e gerenciamento de PKIs, o maior desafio apontado pelos respondentes do Brasil é a falta de propriedade clara, com 65% de menções, seguido pela falta de habilidades com 42% e pela insuficiência de recursos com 38%.
- No Brasil 50% dos entrevistados citaram novas aplicações como IoT, enquanto 42% citaram mandatos e padrões externos. Já nos EUA, 60% dos entrevistados citaram mandatos e padrões externos e 48% novas aplicações.
- Em relação às tendências mais importantes no estímulo à implantação de aplicações que utilizam PKIs no Brasil, a Internet das Coisas aparece em 50% das respostas, a mobilidade para consumidores em 49% e os serviços baseados em nuvem em 39%.

## Informações adicionais



# ENTRUST

SECURING A WORLD IN MOTION

Landing page: [Estudo Global de Tendências em PKI e IoT de 2021](#)  
Blog: [Seus PKIs estão prontos para transformar em realidade todas as possibilidades de um mundo conectado?](#)

## **Metodologia do estudo de tendências globais de PKIs e IoT de 2021**

O estudo de tendências globais de PKIs e IoT de 2021 da Entrust, conduzido pela empresa de pesquisa Ponemon Institute, é baseado no feedback de mais de 1.900 profissionais de segurança de TI em 17 países: Austrália, Brasil, França, Alemanha, Hong Kong, Japão, México, Oriente Médio (que é uma combinação de entrevistados localizados na Arábia Saudita, Arábia e Emirados Árabes Unidos), Holanda, Federação Russa, Espanha, Sudeste Asiático, Coreia do Sul, Suécia, Taiwan, Reino Unido e Estados Unidos.

## **Sobre a Entrust Corporation**

Protegendo um mundo em movimento seguro, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências perfeitas e seguras, seja cruzando fronteiras, fazendo uma compra, acessando serviços do governo eletrônico ou fazendo login em redes corporativas. A Entrust oferece uma amplitude incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós. Para saber mais visite [www.entrust.com](http://www.entrust.com).

## **Contatos para a imprensa:**

Alessandra Neris - (11) 99104-4938 – [atendimento@talquimy.com.br](mailto:atendimento@talquimy.com.br)