

Por Jorge Wahl



O ano é 2030, mas pode ser antes ou um pouco depois, sendo a única certeza a de que os dirigentes de entidades fechadas precisam mesmo prestar a máxima atenção. E a razão é que se espera que as EFPCs sejam bastante afetadas quando acontecer, resume Marcus Quintella (foto acima), Coordenador do Subgrupo Tecnologia do Comitê de Inovação e Tecnologia da Abrapp.

Esse algo tão impactante para o qual as nossas entidades precisarão estar preparadas é a chegada da criptografia pós-quântica. Detalhe: a preocupação não é exclusividade de nenhum segmento específico, mas o agravante no caso das EFPC é que a necessidade de proteger os dados se estende por muito mais tempo, pode-se dizer por décadas.

Quintella explica que não é pouco o que precisa ser protegido pela criptografia, seja aquela que existe hoje, ou a quântica quando esta chegar : “Ela não serve apenas para manter dados em sigilo: também está por trás de certificados digitais, assinaturas, autenticação, proteção das comunicações e diversas outras formas de garantir confiança no ambiente digital “, explica.

É o bastante para abranger rotinas envolvendo sistemas, assinaturas digitais, comunicações protegidas, VPNs, integrações com terceiros, bancos, fornecedores e armazenamento de informações. “ Portanto, não estamos falando de uma tecnologia isolada; estamos tratando de uma camada que atravessa grande parte da infraestrutura digital das entidades “, sublinha Quintella.

E a projeção, lembra Paulo Pagliusi, consultor e um dos expositores em evento promovido recentemente pela Abrapp e já alertando os dirigentes para riscos tão próximos, é que a criptografia assimétrica convencional se torne em poucos anos frágil em um ambiente dominado por computadores quânticos.

É que, para determinados problemas matemáticos, algoritmos quânticos podem ser muito mais eficientes. Isso cria a possibilidade de que, no futuro, um computador quântico com capacidade suficiente consiga resolver em prazo viável problemas que hoje levariam um tempo impraticável, afetando com isso mecanismos criptográficos que atualmente consideramos seguros e um dia que não está longe deixarão de ser.

Outro impacto não envolve somente confidencialidade. A criptografia também sustenta assinaturas digitais e autenticidade documental. Se determinado mecanismo criptográfico deixar de ser confiável, tornar-se-à necessário pensar também na preservação da validade de documentos assinados anteriormente e, eventualmente, em processos de renovação ou reassinatura.

Nesse momento, muito provavelmente os dirigentes irão se perguntar quais documentos precisarão ou não continuar comprovadamente autênticos durante muitos anos e como preservar essa garantia ao longo da transição.

Por isso, o primeiro desafio das entidades não é simplesmente comprar uma ferramenta. Antes de migrar é necessário saber o que existe para ser protegido e onde se encontra para quando a hora chegar.

A preparação passa por governar o tema, identificar os ativos e dependências criptográficas, formar um inventário, priorizar os sistemas e informações mais críticos e então preparar uma transição. É claro, nem tudo precisa ser tratado com a mesma urgência.

O momento agora é de se preparar, aproveitando que a ameaça ainda paira no horizonte.

E fazer isso sabendo que mais do que uma corrida para comprar tecnologia, trata-se muito mais de adquirir conhecimento sobre o ambiente, planejar e formar uma cultura de adaptação.

Para Quintella, o desafio das entidades hoje é começar a conhecer sua dependência de criptografia, entender quais informações precisam permanecer protegidas por longos períodos e criar condições para fazer uma transição progressiva quando ela for necessária.

Fonte: [Abrapp em Foco](#), em 06.10.2026.