

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 26/06/2026 | Edição: 118 | Seção: 1 | Página: 3

Órgão: Presidência da República/Casa Civil/Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil

PORTARIA ITI Nº 38, DE 16 DE JUNHO DE 2026

Institui o Grupo de Trabalho Técnico para estudo, debate e elaboração de proposta para a implementação de criptografia pós-quântica na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe conferem o art. 13, caput, inciso VI, do Anexo I ao Decreto nº 12.103, de 8 de julho de 2024, e o art. 50, inciso VII, da Portaria ITI nº 14, de 10 de março de 2026, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001 e no Decreto nº 10.543, de 13 de novembro de 2020, resolve:

Art. 1º Fica instituído o Grupo de Trabalho Técnico sobre Criptografia Pós-Quântica (GTT-PQC/ICP-Brasil), com a finalidade de estudar, debater e propor as diretrizes e as bases para a implementação de criptografia pós-quântica no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Art. 2º Ao GTT-PQC/ICP-Brasil compete:

I - elaborar diagnóstico abrangente de risco quântico, identificando ativos criptográficos, dependências, níveis de exposição e criticidade de componentes, serviços e processos, com prioridade para os sistemas de assinatura digital e os algoritmos assimétricos em uso na cadeia de confiança;

II - desenvolver o planejamento da migração pós-quântica, com definição de fases, prazos, critérios de priorização, requisitos normativos e modelo de governança do processo;

III - elaborar a estratégia de execução da migração, incluindo roteiros técnicos de transição, abordagens híbridas clássico/pós-quânticas, planos de teste e validação e mecanismos de monitoramento e controle;

IV - articular-se com entidades internacionais de padronização e fóruns técnicos relevantes, com o objetivo de alinhar a estratégia de migração às melhores práticas e aos cronogramas internacionais; e

V - propor ações de conscientização sobre os riscos da computação quântica para a ICP-Brasil junto ao ecossistema de Autoridades Certificadoras, Autoridades de Registro, prestadores de serviços e titulares de certificados, com ênfase nas ameaças à integridade e à autenticidade das assinaturas digitais e à cadeia de confiança, notadamente as ameaças de forjamento retroativo de assinaturas e de subversão da confiança (Sign Now, Forge Later - SNFL e Trust Now, Forge Later - TNFL).

Art. 3º O GTT-PQC/ICP-Brasil será composto por membros permanentes das seguintes unidades:

I - dois representantes do Gabinete do Diretor-Presidente;

II - dois representantes da Diretoria de Infraestrutura Tecnológica - DITEC;

III - dois representantes da Diretoria de Auditoria, Fiscalização e Normalização - DAFN;

IV - dois representantes da Diretoria de Tecnologias de Identificação - DITI; e

V - um representante da Diretoria de Planejamento, Orçamento e Administração - DPOA.

§ 1º Os membros de que trata o caput serão indicados pelos titulares das unidades representadas, no prazo de cinco dias, contado da data de publicação desta Portaria, e designados em ato do Diretor-Presidente.

§ 2º A Procuradoria Federal Especializada junto ao ITI prestará apoio jurídico ao GTT-PQC/ICP-Brasil, podendo ser convocada a participar das reuniões sempre que a pauta envolver questões de natureza jurídica ou normativa, ou sempre que o Coordenador do GTT-PQC/ICP-Brasil entender



necessário.

§ 3º O Coordenador do GTT-PQC/ICP-Brasil poderá convidar especialistas, representantes institucionais e lideranças técnicas de órgãos públicos, entidades privadas, instituições de ensino e pesquisa, associações representativas do ecossistema ICP-Brasil e organismos internacionais para participar das discussões do Grupo de Trabalho Técnico, em caráter colaborativo, técnico e consultivo.

§ 4º A participação de convidados não os torna membros permanentes do GTT-PQC/ICP-Brasil e não vincula as respectivas entidades aos trabalhos e encaminhamentos do Grupo.

§ 5º A relação dos convidados poderá ser ampliada, substituída ou reduzida a qualquer tempo, a critério do Coordenador do GTT-PQC/ICP-Brasil, de acordo com a demanda temática e a necessidade de qualificação técnica dos trabalhos.

§ 6º Cada membro do Comitê Gestor da ICP-Brasil poderá sugerir ao Coordenador do GTT-PQC/ICP-Brasil convidados para participar das reuniões do Grupo, preferencialmente com perfil técnico e experiência nas áreas de criptografia, segurança da informação ou infraestrutura de chaves públicas, observado o disposto nos §§ 3º a 5º deste artigo.

Art. 4º O GTT-PQC/ICP-Brasil será coordenado por um dos representantes da DITEC.

Parágrafo único. Compete ao Coordenador do GTT-PQC/ICP-Brasil:

I - orientar, organizar e alinhar os trabalhos, conduzir as reuniões e consolidar os estudos e as proposições técnicas resultantes dos debates;

II - zelar pelo equilíbrio técnico das discussões, assegurando que as contribuições dos convidados sejam devidamente consideradas, sem prejuízo da competência institucional do ITI;

III - definir o calendário das reuniões, formalizar a respectiva convocação e encaminhar os convites a que se refere o art. 3º, § 3º; e

IV - praticar os demais atos necessários à organização e ao funcionamento do GTT-PQC/ICP-Brasil.

Art. 5º O GTT-PQC/ICP-Brasil reunir-se-á ordinariamente uma vez por semana e poderá ser convocado extraordinariamente pelo Coordenador, sempre que necessário.

§ 1º As reuniões serão realizadas com a presença da maioria dos membros, presencialmente ou por videoconferência, conforme indicado no ato de convocação.

§ 2º As reuniões serão convocadas pelo Coordenador com antecedência mínima de vinte e quatro horas, prazo que poderá ser dispensado se à reunião estiverem presentes todos os membros.

§ 3º As discussões e encaminhamentos serão registrados em atas formalizadas no Sistema Eletrônico de Informações até a reunião ordinária subsequente, assinadas pelos membros presentes e registrada a participação dos eventuais convidados.

Art. 6º O GTT-PQC/ICP-Brasil terá prazo inicial de funcionamento de noventa dias, contado da data de publicação desta Portaria, permitida a prorrogação por igual período, por meio de ato motivado do Diretor-Presidente.

Art. 7º Ao término do prazo estabelecido no art. 6º, o GTT-PQC/ICP-Brasil apresentará ao Diretor-Presidente do ITI, como subsídios técnicos, os seguintes produtos:

I - relatório de diagnóstico de risco quântico para a ICP-Brasil;

II - plano de migração pós-quântica, com cronograma e critérios de priorização;

III - proposta de atualização normativa; e

IV - estratégia de execução da migração, abrangendo roteiros técnicos de transição, abordagens híbridas clássico/pós-quânticas e mecanismos de monitoramento e controle.

Art. 8º A participação no Grupo de Trabalho Técnico de que trata esta Portaria será considerada prestação de serviço público relevante, não remunerada.

Art. 9º Esta Portaria entra em vigor na data de sua publicação no Diário Oficial da União.

ENYLSO FLÁVIO MARTINEZ CAMOLESI

Este conteúdo não substitui o publicado na versão certificada.

