

JÁ NÃO É FICÇÃO
O PARADOXO DA VISIBILIDADE E A REALIDADE HÍBRIDA

Dia 3 de 3

Certificação Global e o Chamado à Ação

Nos dois primeiros dias vimos a oportunidade e a ameaça.

*Hoje veremos o que o mundo já exige em resposta,
e o que cada um de nós pode fazer efetivamente.*

João Roberto Peres

Dia 3 — Já não é ficção



**“Regular, validar, proteger e evoluir: o
novo imperativo da Segurança de IoT.”**

**REVENDO:
Absorção &
Compreensão**

**Ciências
Quânticas.**

**Tecnologias
de
Computação
Quântica.**

Sobre os Workshops 1 e 2.

O essencial a ser retido na visão Executiva.

Workshop 1: o que não podemos esquecer.

- **Ciências Quânticas completaram 100 anos em 2025:** A Organização das Nações Unidas (ONU) declarou 2025 como o Ano Internacional da Ciência e Tecnologias Quânticas (IYQ).
- **O estudo da Computação Quântica completa 45 anos em 2026:** - <https://postquantum.com/quantum-computing/feynman-quantum-history/>
- **O primeiro computador quântico comercial** foi posto à venda em **maio de 2011**, produzido pela empresa D-Wave. https://en.wikipedia.org/wiki/D-Wave_Systems <https://outreach.ictp-saifr.org/quantica-computacao-quantica/> <https://physicsworld.com/a/d-wave-sells-its-first-quantum/>
- **O primeiro Computador Quântico comercial da IBM** foi lançado em **janeiro de 2019** - <https://uk.newsroom.ibm.com/ibm-unveils-worlds-first-integrated-quantum-computing-system-for-commercial-use>
- **O investimento mundial** em computação quântica chegou a **US\$ 12.6 bilhões em 2025** - <https://www.mckinsey.com/featured-insights/charts/quantum-investment-surge> <https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point>
- O site “futuro entrelaçado” (**Entangled Future**) – mostra a **dinâmica do crescimento do ecossistema quântico** no mundo mapeando empresas, tipos e localizações — contando com mais de 1.496 empresas cadastradas (30/09/2026). <https://entangledfuture.com/map/>
- **Desmistificamos o mito da criogenia:** Criostatos de diluição de hélio (refrigeradores de chip) **utilizados** para **determinadas tecnologias de processadores quânticos** (qubits supercondutores, qubits de spin em semicondutores / pontos quânticos, qubits topológicos e recozimento quântico / quantum annealing). <https://onlinelibrary.wiley.com/doi/10.1002/tee.70379> - <https://link.springer.com/article/10.1007/s44464-026-00033-9>
- Conhecemos o **chip quântico brasileiro** de projeto CBPF/Unicamp e fabricado na **Unicamp SP** - <https://www.gov.br/cbpf/pt-br/assuntos/noticias/pesquisadores-do-cbpf-e-unicamp-desenvolvem-um-chip-quantico-supercondutor>

O essencial a ser retido na visão Executiva.

Workshop 1: o que não podemos esquecer.

- **Três tecnologias de processamento quântico que operam em temperatura ambiente:** Ressonância Magnética Nuclear (RMN – da SpinQ), vacância de nitrogênio em diamante (Quantum Brilliance) e fotônica (universal da Xanadu – Canadá), entre outras. <https://www.spinq.com/> - <https://parityqc.com/quantum-brilliance-and-parityqc-win-contract-to-build-worlds-first-mobile-quantum-computer> - <https://inflection.com/quantum-computing/>
- O SENAI-SP adquiriu o **primeiro computador quântico de treinamento** em **2023**, o modelo Triangulum da SpinQ (tecnologia RMN). - <https://www.superaparque.com.br/not%C3%ADcias/primeiro-computador-qu%C3%A2ntico-para-fins-educacionais-chega-ao-brasil>
- O **modelo QaaS:** Quantum-as-a-Service – **as principais Big Techs** já oferecem serviços de computação quântica em nuvem há 10 anos. - <https://esr.rnp.br/computacao-quantica/quantum-as-a-service-saas/> <https://aws.amazon.com/pt/braket/> <https://newsroom.ibm.com/2026-05-04-ibm-a-decade-of-quantum-on-the-cloud>
- **Analisamos a situação do ecossistema brasileiro:** Desde as pesquisas acadêmicas distribuídas no mapa do Brasil até as instalações do CIQUANTA (Paraíba Quântica 2026), com dois computadores quânticos já instalados (20 e 100 qubits), com transferência de tecnologia. Vimos o SENAI CIMATEC (Salvador – BA, 2021) e as diversas deeptechs brasileiras. (links disponíveis na apresentação em PPTX).
- **EVOLUIMOS** comparando as arquiteturas de CPU + GPU + NPU integradas à QPU no **processamento híbrido** e **FECHAMOS** o primeiro workshop avaliando os **estágios da computação quântica**.



O essencial a ser retido na visão Executiva.

Workshop 2: o que não podemos esquecer.

- Revisamos os **conceitos de qubits físicos e lógicos**, a relação dessa **unidade de medida** com o **poder computacional** real na tecnologia de supercondutores (que requer criogenia) e **avancamos para a outra tecnologia** adotada no computador do **SENAI**.
- Detalhamos a **tecnologia de Ressonância Magnética Nuclear (RMN)** para o **processamento quântico de partículas líquidas**, utilizadas como fonte de **qubits físicos** e controladas como **qubits lógicos** para processamento — utilizando como exemplo as **máquinas do SENAI já disponíveis no Brasil (SP/RJ)**.
- Verificamos a necessidade de **memórias SSD/RAM** e **memórias quânticas temporárias** para o uso no processamento quântico híbrido, **encerrando o panorama de recapitulação técnica**.
- Demonstramos como o **poder computacional quântico** e o algoritmo de **Peter Shor** podem quebrar algoritmos de criptografia assimétrica consolidados, como o **RSA (1977)** e o **ECC (1985)**. Além disso, abordamos o algoritmo de Grover, que reduz a eficiência do algoritmo simétrico AES-128 pela metade.
- A **proteção contra o uso dos algoritmos de Shor e Grover por computadores quânticos** já foi estabelecida pelo **NIST**, com o lançamento da **família de algoritmos de Criptografia Pós-Quântica (PQC)** em 2024.
- **O RISCO HNDL** (Harvest Now, Decrypt Later) ‘coletar agora e decifrar depois’ - já é uma realidade global.
- **Em janeiro de 2026**, o **Relatório de Inteligência da ABIN** apontou a **ameaça HNDL** como prioridade de Estado, alertando para os riscos do "**Apocalipse Quântico**" caso a **proteção via PQC** não seja implementada.

O essencial a ser retido na visão Executiva.

Workshop 2: o que não podemos esquecer.

- Avaliamos **o risco da falta de proteção PQC** com um **impacto severo e constante**, pois não é possível saber com certeza se algum país ou grupo já possui computadores quânticos capazes de quebrar os algoritmos RSA e ECC, atingindo **o Q-Day** na atualidade. **Tais atores não anunciarão** essa conquista, aproveitando a vantagem estratégica do seu poder computacional.
- Analisamos a evolução em relação à previsão da **Caltech (2024)**: a antiga estimativa de que seriam necessários milhões de qubits físicos para quebrar o RSA/ECC **foi revista**. Com novas técnicas, correções de erro e persistência, cerca de **10.000 qubits serão suficientes**, o que antecipa a chegada do **Q-Day**.
- Apresentamos os setores mais expostos ao risco de não adotar PQC: o sistema financeiro mundial, sistemas de IoT legados, o sistema jurídico em geral, entre outros.
- Abordamos os **principais algoritmos PQC padronizados pelo NIST** para sistemas legados: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) e FIPS 205 (SLH-DSA).
- Apresentamos os **principais padrões PQC para dispositivos IoT** (criptografia leve): Ascon (NIST SP 800-232), FN-DSA (Falcon — FIPS 206) e abordagens híbridas que combinam PQC com criptografia clássica.
- Abordamos a **distribuição quântica de chaves (QKD) para a Internet Quântica** via fibra óptica: destacamos que ela é recomendada como uma camada adicional de segurança, sem substituir os algoritmos de PQC.
- Demonstramos a **relação do poder computacional quântico** com a **crescente demanda da Indústria 5.0**, destacando o uso de **algoritmos e estruturas** como VQE (Variational Quantum Eigensolver) e QML (Quantum Machine Learning).

O essencial a ser retido na visão Executiva.

Workshop 2: o que não podemos esquecer.

- Abordamos a **quarta frente quântica**, referente aos **Sensores Quânticos de segunda geração**, destacando uma indústria mundial pujante. Como exemplo, apresentamos o **sensor multivariável da Bosch**, configurável por **software na Edge/Cloud em arquitetura QIoT**. Também mostramos outros tipos e tecnologias de sensores já disponíveis no mercado e alertamos sobre o risco de produtos fake sendo comercializados.
- Evoluímos para o **conceito da arquitetura QIoT** (Quantum Internet of Things — padrão IEEE*), concebida como um **sistema híbrido**. Essa abordagem integra sensores convencionais na ponta (desprovidos de capacidade física para processamento quântico, como termômetros ou câmeras) a dispositivos quânticos nativos. O ecossistema é estruturado em três camadas dinâmicas: Percepção Quântica (Edge), Transmissão Quântica, e Controle e Processamento.
- **Encerrando o segundo workshop**, ressaltamos que a apresentação teve um **caráter didático e executivo** (em detrimento de uma abordagem puramente técnica/científica), e **sugerimos prompts de Inteligência Artificial Generativa (IAG)** para **pesquisas e validação de dados** aos interessados

"O objetivo deste resumo é mostrar que a tecnologia quântica deixou de ser apenas teoria acadêmica e já está impactando o mercado e a segurança da informação (com o surgimento de novos chips, investimentos bilionários e novos padrões de criptografia para proteger nossos dados)."

* A hibridização é a base realista de toda a computação quântica atual (como a norma IEEE P3185 para ambientes híbridos clássico-quânticos). Seria economicamente inviável e fisicamente desnecessário transformar cada pequeno sensor (como o termômetro mencionado) em um dispositivo quântico nativo.

https://www.researchgate.net/publication/390335229_QIoT_IoT_Architectures_in_Quantum_Computing_Era



EVOLUINDO PósQ

O que o mundo pensa e exige ação imediata.

“A computação quântica é a chave para desbloquear as respostas para as perguntas mais complexas do nosso planeta, especialmente na ciência dos materiais e nas mudanças climáticas.”

Satya Nadella, CEO da Microsoft (2024).

“O ambiente quântico está hoje onde a Inteligência Artificial estava há cinco anos.”

Sundar Pichai, CEO da Alphabet (Google)-(2023).

"Não espere o desenvolvimento de um computador quântico perfeito... Comece a integrar os novos padrões regulatórios em seus roteiros de tecnologia imediatamente."

Laurie E. Locascio, Diretora do NIST (Instituto Nacional de Padrões e Tecnologia dos EUA).” (2024).



A Vulnerabilidade Crítica do Hardware Legado

O descompasso temporal entre o ciclo de vida da Internet das Coisas e a longevidade dos algoritmos clássicos.

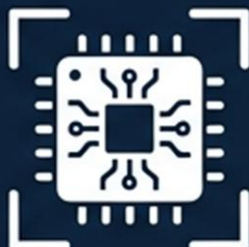
O Gargalo do Ciclo de Vida

Dispositivos instalados em redes elétricas, turbinas industriais e automação predial são projetados para operar por 15 a 25 anos em campo, muito além do Q-Day.



Restrição Computacional

Chips em microcontroladores de IoT possuem restrições extremas de memória RAM e bateria, incapacitando a execução abrupta de algoritmos criptográficos pesados e chaves longas.



Ausência de Cripto-Agilidade

A esmagadora maioria dos módulos IoT atuais não possui arquitetura (OTA seguro) para substituir dinamicamente os algoritmos de criptografia gravados no silício.



A Ameaça de Obsolescência

Sem atualização, equipamentos implantados hoje com criptografia clássica (RSA/ECC) estarão perigosamente expostos e inoperantes antes do fim natural de sua vida útil.

AES128, PRESENT, CLEFIA, HMAC, SHA256...



Cripto-agilidade deixou de ser um luxo das áreas de TI para se tornar um requisito estratégico de longevidade de Capex e continuidade de negócios.

ENTENDER E AGIR



"Para um engenheiro, não há nada mais empolgante do que desbravar territórios desconhecidos."

Frederik Schaal

CTO da Bosch Quantum Sensing

Frase parcial.

Hoje a Internet está mais Segura. O IoT, Ainda Não.



INTERNET - WEB BROWSERS EVOLUÇÃO PARA PQC

- TLS 1.3
- QUIC
- HTTPS
- VPN
- PKI



O QUE ESSES PROTOCOLOS PROTEGEM



Trânsito dos dados protegido de ponta a ponta.

A evolução para PQC começa a tornar esses canais resistentes à ameaça quântica.

Mas existe outra camada: proteger o canal não significa proteger todo o ecossistema criptográfico da organização.

COMUNICAÇÃO SEGURA NÃO SIGNIFICA DISPOSITIVO QUANTUM-READY.

<https://blog.google/chromium/advancing-our-amazing-bet-on-asymmetric/>
<https://www.encryptionconsulting.com/pqc-support-in-web-browsers/>
<https://thehackernews.com/2026/07/microsoft-accelerates-post-quantum.html>

Um Canal Pode Ser Quantum-Safe. O Dispositivo, Não.



SENSOR IoT

Firmware · Identidade · Chaves · Secure Boot



TLS 1.3 + PQC

Canal de comunicação protegido



INTERNET → CLOUD / DATA CENTER

API · PKI · Banco de dados · Backup



MESMO COM PQC NO CANAL, PODEM PERMANECER VULNERABILIDADES EM:

- Firmware
- Assinatura de código
- Armazenamento
- Identidade
- PKI
- Gerenciamento de chaves
- Componentes legados
- Hardware sem capacidade de atualização



QUANTUM-SAFE NA COMUNICAÇÃO NÃO SIGNIFICA QUANTUM-READY NO DISPOSITIVO.

A Capacidade de Evoluir Sem Reconstruir Tudo



UM SISTEMA CRIPTOGRAFICAMENTE ÁGIL DEVE PERMITIR:

- Substituir algoritmos
- Atualizar bibliotecas
- Renovar chaves e certificados
- Atualizar firmware
- Adaptar protocolos
- Migrar para PQC

NÃO BASTA SER SEGURO. É PRECISO SER CRIPTOGRAFICAMENTE EVOLUTIVO.



O Novo Mapa Regulatório

Instrumento	Jurisdição	Natureza	Foco principal	Relação com IoT / Cripto Agility
EU Cyber Resilience Act (CRA)	EU União Europeia	Regulação obrigatória	Segurança de produtos com elementos digitais durante todo o ciclo de vida	Muito alta: secure-by-design, gestão de vulnerabilidades, atualizações, ciclo de vida e evidências de conformidade
US Cyber Trust Mark	US EUA	Rotulagem voluntária	Demonstrar nível de segurança de produtos IoT de consumo	Alta: incentiva segurança verificável, mas não é uma certificação PQC
UK PSTI Act	GB Reino Unido	Lei/regulação obrigatória	Requisitos mínimos para produtos conectáveis de consumo	Média/Alta: segurança desde o projeto, vulnerabilidades e atualização; ainda não é uma regulação específica de cripto-agilidade
Cybersecurity Labelling Scheme – CLS(IoT)	SG Singapura	Rotulagem/certificação por níveis – Voluntária/Obrigatória	Avaliar e comunicar a postura de segurança de dispositivos IoT	Alta: níveis crescentes de avaliação e testes; útil como modelo de assurance
GSMA IoT SAFE / IoTSF	🌐 Internacional	Padrões/frameworks da indústria - Voluntária	Segurança técnica, identidade, Root of Trust, assurance e boas práticas	Muito alta: fornecem componentes técnicos para construir uma arquitetura preparada para evolução criptográfica

Convergência regulatória não é uma particularidade de um bloco econômico. Já se consolidou na prática.

O Novo Mapa Regulatório - Check

- O CRA é o elemento mais diferente do conjunto: ele não é simplesmente um selo de segurança. É uma obrigação regulatória abrangente para produtos com elementos digitais. Entrou em vigor em dezembro de 2024; as principais obrigações passam a ser aplicáveis em **11 de dezembro de 2027**, enquanto as obrigações de reporte de vulnerabilidades exploradas ativamente e incidentes graves começaram em **11 de setembro de 2026**.
- No Reino Unido, o regime PSTI para produtos conectáveis de consumo está em vigor desde **29 de abril de 2024**. Fundamentado na norma EU ETSI EN 303 645 / NIS 2.
- Nos EUA, o Cyber Trust Mark é deliberadamente diferente: trata-se de um programa voluntário de rotulagem para produtos IoT sem fio de consumo, administrado no âmbito da FCC. <https://www.malwarebytes.com/blog/news/2025/01/us-cyber-trust-mark-logo-for-smart-devices-is-coming>
- Já Singapura utiliza uma lógica bastante interessante para sua apresentação: o CLS(IoT) possui **quatro níveis**, representados por estrelas, correspondentes a níveis crescentes de avaliação e testes. Para determinados roteadores Wi-Fi, o nível 1 é obrigatório.



<https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-consumers/>

<https://www.appluslaboratories.com/global/en/news/publications/uk-psti-leveling-up-the-security-requirements-for-connectable-products-in-uk>

<https://www.iotsecurityfoundation.org/event/iotsf-august-2025-webinar-post-quantum-cryptography-for-iot-securing-devices-for-the-quantum-future-and-opentitan-the-first-open-source-rot-hardware-platform/>

<https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/iot-safe/>

<https://www.cta.tech/standards/post-quantum-cryptography-for-iot/>

<https://csrc.nist.gov/projects/post-quantum-cryptography>



O Que Já é Lei, o Que Ainda é Adesão



Já é obrigatório

O EU Cyber Resilience Act e o UK PSTI Act já são lei em suas jurisdições, com prazos de conformidade e sanções previstas.



Ainda é adesão de mercado

O GSMA IoT SAFE e o selo de Singapura ainda são voluntários, mas já funcionam como diferencial competitivo de fato em suas cadeias.



A Precisão que a EO 14412* Exige

Migrar para criptografia Pós-Quântica (PQC)



- **Mandado direto:** sistemas federais americanos classificados como Ativos de Alto Valor (HVA) têm migração para PQC exigida por cronograma definido conforme criticidade.
- **Apoio, não mandatário:** operadores de infraestrutura crítica privada recebem orientação e assistência técnica para migração, categoria que a própria norma define como não vinculante. Não é obrigatório, cada um assume o seu risco.



A distinção entre mandado direto e apoio à implementação não é uma nuance a ser interpretada: está expressa no próprio texto da Executive Order.

Tratá-la como obrigação universal é um erro.

**** “EO 14412 - Securing the Nation Against Advanced Cryptographic Attacks”, foi assinada pelo presidente Donald Trump em 22 de junho de 2026.***

O CBOM Como Novo Passaporte

Migrar para criptografia Pós-Quântica (PQC) exige inventário

Cryptographic Bill of Materials: a lista de ingredientes criptográficos



- Documenta todos os algoritmos, tamanhos de chave e bibliotecas criptográficas embarcadas em um produto ou software.
- Já é exigido, direta ou indiretamente, pelo EU CRA, pela Executive Order 14412 e por compradores corporativos exigentes.

Sem CBOM, um fornecedor de tecnologia simplesmente perde acesso a contratos e cadeias de suprimento inteiras, na União Europeia e nos Estados Unidos. Isso já deixou de ser diferencial competitivo para virar condição de entrada.

VISIBILIDADE PRIMEIRO

CBOM: Antes de Migrar, é Preciso saber o que Existe

*Cryptographic Bill of Materials
(inventário de materiais criptográficos)*



DEVICE / SOFTWARE / SISTEMA



O que usa criptografia?

Qual algoritmo?

Qual biblioteca?

Qual protocolo?

Qual chave/
certificado?

Onde está
implementado?

Quem fornece?

Pode ser
atualizado?

Não se pode migrar aquilo que não se consegue identificar.

CBOM → Visibilidade → Priorização → Migração PQC → Crypto Agility

O Roadmap de Cinco Fases



A Segurança da Organização



1

Inventário

Mapear chaves, certificados e bibliotecas em uso

2

Análise de Risco

Classificar dados pelo tempo de vida da confidencialidade

3

Migração PQC

Adotar agilidade criptográfica e os padrões do NIST



4

Testes via QaaS

Experimentar otimização quântica sem investir em hardware

5

Governança Contínua QC

Revisão periódica frente aos marcos regulatórios e tecnológicos

Utilizar padrões consagrados do mercado mundial >

<https://pqcframework.org/>

Onde você e Sua Organização Provavelmente Estão?

Para pensar...

Um termômetro de maturidade, apenas ilustrativo, sem exposição de dados de ninguém.



Inconsciente

Ainda não mapeou o tema como pauta de risco

Curiosa

Já ouviu falar, ainda sem responsável formal ou ações

Em diagnóstico

Iniciou inventário criptográfico básico

Em migração

Já testa PQC em sistemas piloto



<https://pkic.org/wg/pqc/pqcmm/> PQC Maturity Model (PQCM)

<https://www.digicert.com/content/dam/digicert/pdfs/post-quantum-cryptography-maturity-model-whitepaper-en.pdf>

<https://www.encryptionconsulting.com/pqc-security-maturity-model/>

Governança e Responsabilidade do Conselho

O dever de diligência (duty of care) dos administradores.



- O NIST já publicou os padrões oficiais de PQC. O desconhecimento da ameaça quântica deixou de ser **excludente de ilicitude**.
- A LGPD (Art. 46) considera o **estado da tecnologia** ao avaliar a adequação das medidas de segurança, incluindo inquestionavelmente os padrões PQC.

Manter dados sensíveis sob criptografia sabidamente vulnerável, sem planejamento de transição, já pode ser caracterizado como falha no dever de segurança pela ANPD ou pelo Judiciário.

<https://conteudo.soluti.com.br/instrucao-normativa-iti-no-35-2026-e-a-nova-era-da-criptografia-pos-quantica-no-brasil/>

<https://ancd.org.br/icp-brasil-inicia-planejamento-para-migracao-a-criptografia-pos-quantica/> (ITI 26 de junho, a Portaria nº 38/2026)

<https://ibsec.com.br/criptografia-pos-quantica-urgencia-e-estrategias/>

<https://peckadv.com.br/criptografia-hoje-violacao-amanha-a-problematica-do-harvest-now-decrypt-later-frente-aos-limites-do-direito-penal-e-da-regulacao-de-incidentes-no-brasil/>

<https://esr.rnp.br/ciencia-de-dados/fiscalizacao-anpd-como-preparar-empresa/>

PQC na Prática: Cláusula Contratual Pronta

Ação jurídica para blindar seus contratos de TI e IoT contra o risco quântico.



Cláusula de Agilidade Criptográfica e Conformidade PQC

- **Crypto-Agility Sem Custo:** Atualização e troca de algoritmos via software/OTA sem custo adicional de arquitetura ou troca precoce de hardware.
- **Escopo Flexível (Variantes A e B):** Regras específicas para proteção de canais em Nuvem/Software ou segurança física e atualização remota para IoT/AIoT.
- **Transparência e Responsabilidade:** Exigência de CBOM (inventário de algoritmos), plano contra mitigação de interceptação retroativa (HN DL) e responsabilização por algoritmos obsoletos sob a LGPD.

"Agilidade criptográfica em contrato é a garantia de que a atualização tecnológica não virará um custo imprevisto."

<https://www.migalhas.com.br/quentes/459145/governo-se-prepara-para-a-era-quantica-diz-advogada>
<https://oabdf.org.br/criptografia-pos-quantica-e-desafios-da-ciberseguranca-entram-em-debate-na-oab-df/>



Pesquisa Imediata com Claude



Proposta de Prompt:
*Usar a técnica de
“zero-shot prompting.”*

"Redigir um rascunho de memorando fictício de designação de responsável pela migração para criptografia pós-quântica (PQC) em uma empresa hipotética que opera dispositivos IoT, utilizando exclusivamente as seguintes referências, com nomes, números e categorias fixos, sem alteração, aproximação ou complementação por conta própria: NIST FIPS 203 (ML-KEM), NIST FIPS 204 (ML-DSA) e NIST FIPS 205 (SLH-DSA), categoria padrões técnicos PQC finalizados; Executive Order 14412 (EUA, 2026), categoria instrumento regulatório federal dos EUA, sem efeito vinculante direto sobre a empresa fictícia; LGPD, art. 46, categoria fundamento legal brasileiro para o dever de diligência. O memorando deve:

- (1) citar a EO 14412 apenas como referência de um movimento regulatório internacional, nunca como norma vinculante para a empresa, distinguindo essa categoria da categoria dos padrões técnicos NIST citados;
- (2) vincular a designação à elaboração do CBOM (Cryptographic Bill of Materials) como inventário criptográfico dos dispositivos IoT da empresa;
- (3) situar a designação no âmbito da governança de segurança da informação e da governança de tecnologias quânticas emergentes, fundamentando o dever de diligência exclusivamente no art. 46 da LGPD;
- (4) usar cenário, empresa e nomes fictícios, sem dados reais de pessoas ou empresas;
- (5) não introduzir nenhuma norma, padrão, órgão regulador, sigla ou número de publicação além dos listados acima, nem agrupar referências de categorias distintas sob um mesmo rótulo; qualquer necessidade de referência técnica adicional deve ser sinalizada como pendente de verificação, nunca afirmada como fato."

Passos necessário na evolução QIoT

O que você já pode fazer hoje.



A validação de amanhã não avaliará apenas se o dispositivo é seguro hoje, mas se ele consegue permanecer seguro no futuro.

Do Secure by Design ao Quantum-Ready IoT

Sua organização pode potencializar a conquista da evolução em segurança IoT. Grande oportunidade para todos!!!



Organismo de Certificação Governamental



Entidade terceirizada, formalmente acreditada por órgãos oficiais (como o Inmetro no Brasil) ou reguladores de mercado (como a Anatel para rádio e telecomunicações), que realiza testes laboratoriais baseados em normas de conformidade estritas e emite certificados de Segurança e Governança IoT.

Certificado



Organização Validadora de Melhores Práticas de Segurança IoT

É uma instituição (frequentemente consórcios industriais ou associações setoriais sem fins lucrativos, como o **Fórum Brasileiro de IoT**, CSA ou a IoT Security Foundation – (IoTSEF) que avalia o alinhamento de uma empresa ou de um projeto às práticas de governança e cibersegurança recomendadas internacionalmente.

Declaração e Selo



Quais Ações Executivas Você Pode Tomar hoje?



Não importa se você Aconselha ou Dirige uma empresa, um órgão de governo, uma associação ou uma instituição de ensino:

Lidera uma empresa

Propor Nomear um responsável por diagnóstico e leve o tema ao comitê de risco

Atua em governo

Propor Avaliar se as políticas sob sua responsabilidade já acompanham os cronogramas vistos hoje

Representa uma associação

Leve o tema ao Radar de comunicação e capacitação do setor

Atua no ensino

Avalie se a Grade Curricular já contempla PQC e certificação de segurança

O ponto comum entre todos esses caminhos é o mesmo: o desconhecimento deixou de ser uma posição segura para qualquer profissional.



THE END

Tempo Extra para dúvidas e network

Vamos continuar neste mesmo link – para quem desejar sair desejamos bom descanso.

Esta extensão se mostrou mais eficiente do que a com novo link.