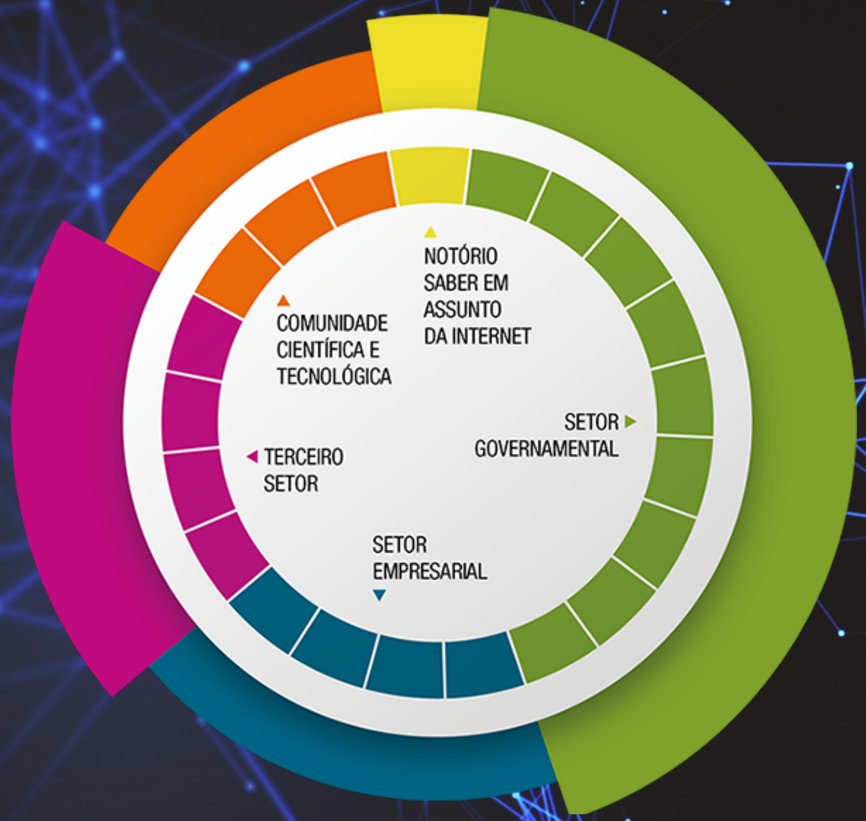
CGI.BR

CÂMARA DE SEGURANÇA E DIREITOS

REDE QUANTICA

SOBRE O CGI.BR

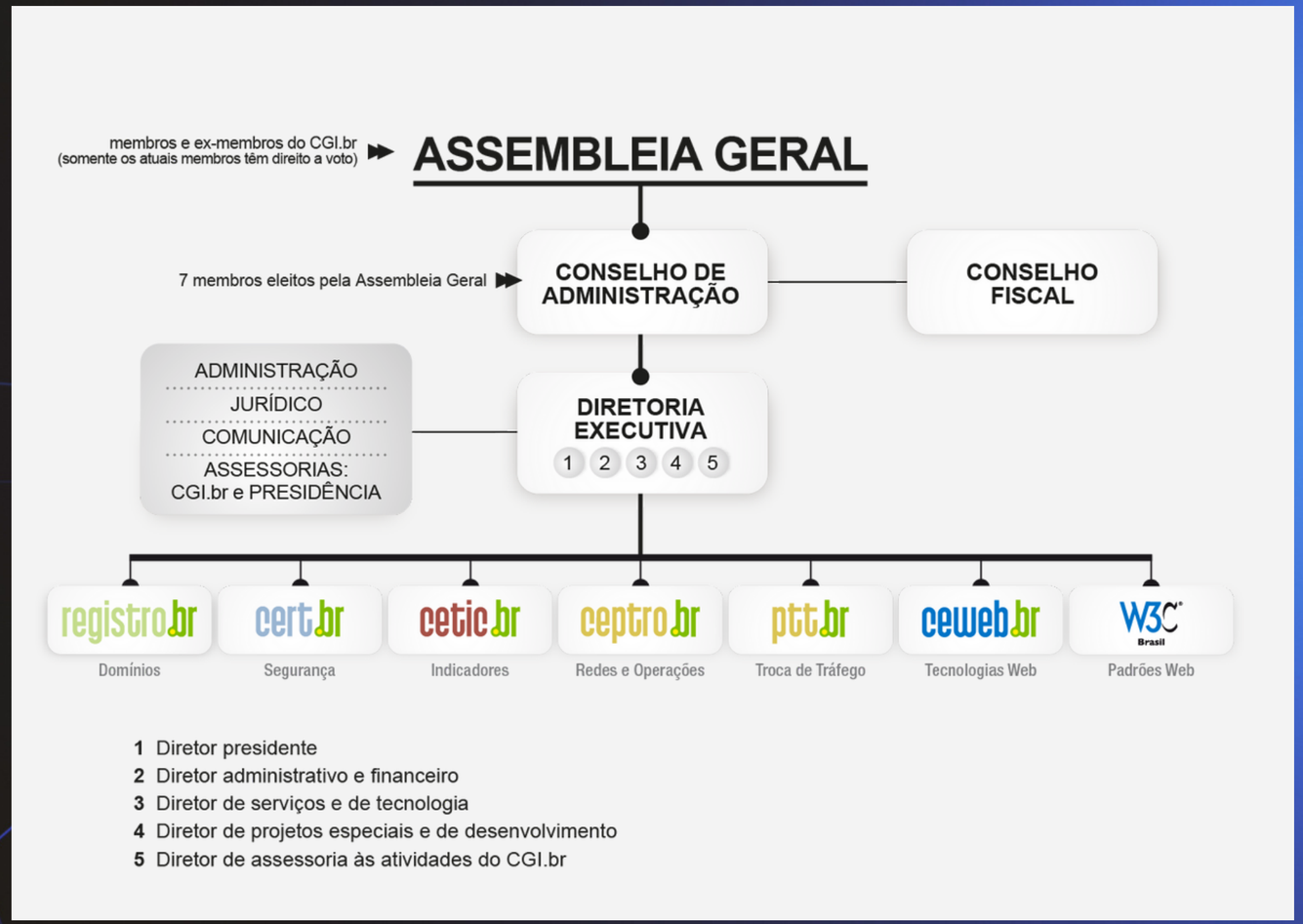


Criação e atribuições

A Portaria Interministerial nº 147, de 31 de maio de 1995, formalizou a criação do CGI.br, definindo suas competências e composição inicial. O Decreto nº 4.829, de 3 de setembro de 2003, atualizou sua estrutura.

1. **Composição Multissetorial**: O decreto reafirmou a composição multissetorial do CGI.br, incluindo representantes do governo, do setor empresarial, da comunidade acadêmica, do terceiro setor e dos provedores de infraestrutura de Internet.
2. **Delineou as competências**, Incluindo a coordenação da atribuição de endereços IP a administração do registro de ccTLD .br.
3. **Promoção da qualidade**, inovação e disseminação dos serviços de Internet, além de seu envolvimento na proposição de políticas e procedimentos relacionados à regulamentação da Internet.

SOBRE O NIC.BR



SOBRE A CÂMARA

A Câmara de Segurança e Direitos na Internet é parte integrante do Comitê Gestor da Internet no Brasil (CGI.br).

Sua atuação se enquadra dentro de um espaço temático especializado, aprofundando discussões e sugerindo ações de interesse do CGI.Br para o cumprimento de sua missão na perspectiva da melhoria da Internet no Brasil, especialmente no que diz respeito a segurança e proteção de direitos.

PARICIPANTES DA CÂMARA DE SEGURANÇA E DIREITOS

MEMBRO GOVERNO	ENTIDADE
Larissa Schneider	MRE
Marcelo Malagutti	GSI
Moacir Silva do Nascimento Junior	CNMP
Nathalie Fragoso e Silva Ferro	MJSP

MEMBRO 3 SETOR	3 SETOR
Thiago Tavares	Safernet
Celso Oliveira	AqualtuneLab
Ana Barbara Gomes	CIRIS-BH
Raquel Saraiva	IP.rec

MEMBRO COMUNIDADE C&T	ENTIDADE
Iara Machado	RNP
Thais Batista	SBC
Edmar Candeia	UFCG-IEEE
Alcides Perón	FECAP

MEMBRO EMPRESARIAL	ENTIDADE
Sidnei Batistella	ABRINT
Rodrigo Jonas Fragola	Assespro
Sérgio Sgobbi	Brascom
Wendel Alves	CNDL

AGENDA TEMÁTICA

1. **Segurança Cibernética**
2. **Defesa Cibernética**
3. **Segurança da Informação e Comunicações**
4. **Direitos difusos no espaço cibernético**
   - Criança e adolescente
   - Propriedade intelectual
   - Proteção de dados pessoais
   - Liberdade de expressão
5. **Observatório do processo legislativo**
6. **Observatório da governança global**

PROJETOS EM ANDAMENTO

1. **Glossario de Cibersegurança**
2. **Participação no IETF**
3. **Criação de um HUB para comunidade**

Redes quânticas em um cenário híbrido

Perspetivas de mercado e desafios regulamentares

INTEGRAÇÃO DE NÓS E SISTEMAS QUÂNTICOS EM REDES CONTEMPORÂNEAS.

Como os nós e sistemas quânticos podem ser integrados nas redes existentes?

Quais são os desafios técnicos que enfrentamos, como ruído e diafonia, e quais soluções podemos implementar, como a multiplexação por divisão de comprimento de onda (WDM) e a utilização de filtros ópticos?

Como podemos assegurar a segurança e o desempenho em arquiteturas de redes híbridas, tirando partido das infraestruturas ópticas existentes?

Integração Física

- Desafios na integração de canais de comunicação quânticos e clássicos na infraestrutura óptica contemporânea.
- Importância da multiplexação por divisão de comprimento de onda (WDM) para a segregação de canais quânticos e clássicos.

Supere os desafios físicos.

Problemas como ruído ASE e diafonia em sistemas DV-QKD. As soluções incluem:

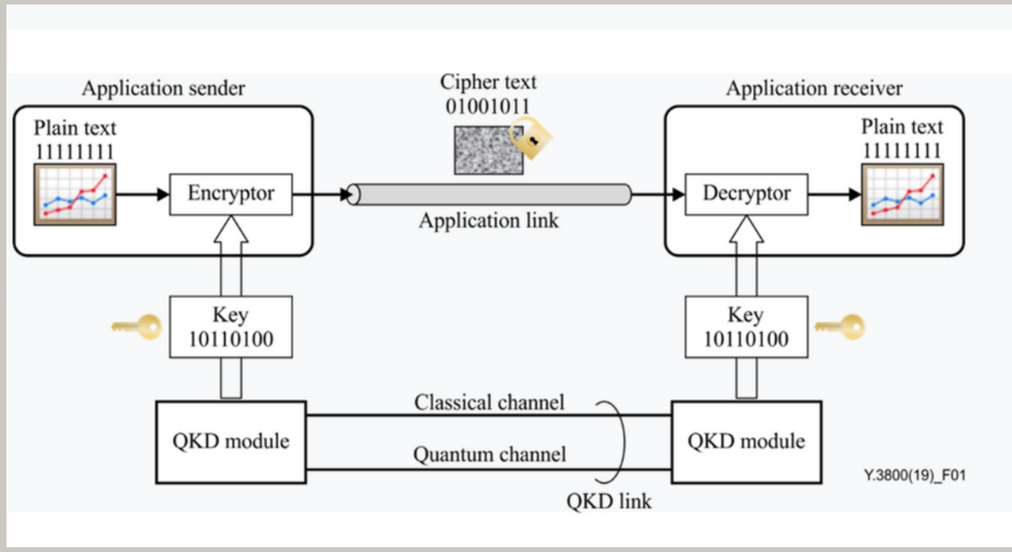
- o emprego de filtros ópticos de elevado isolamento
- a atribuição meticulosa de comprimentos de onda.

APLICAÇÕES PRÁTICAS DE REDES QUÂNTICAS

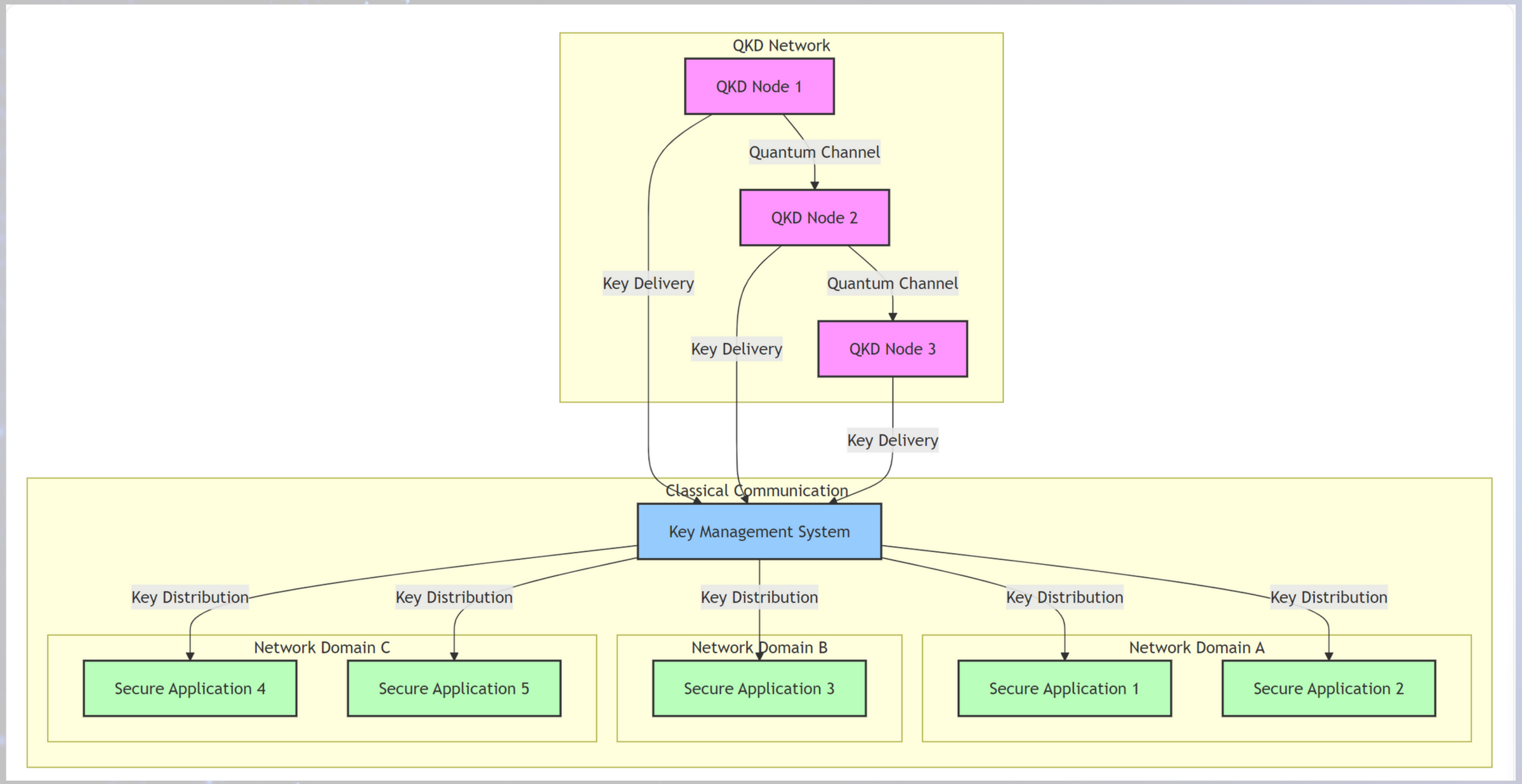
Integração de sistemas de Distribuição Quântica de Chaves (QKD) em infraestruturas de redes ópticas já existentes.

Implementações em redes metropolitanas com fibras multicore, possibilitando comunicação segura em longas distâncias sem a necessidade de cabos adicionais.

Benefícios: Aumento da segurança em comunicações críticas e diminuição de custos por meio da utilização da infraestrutura existente.



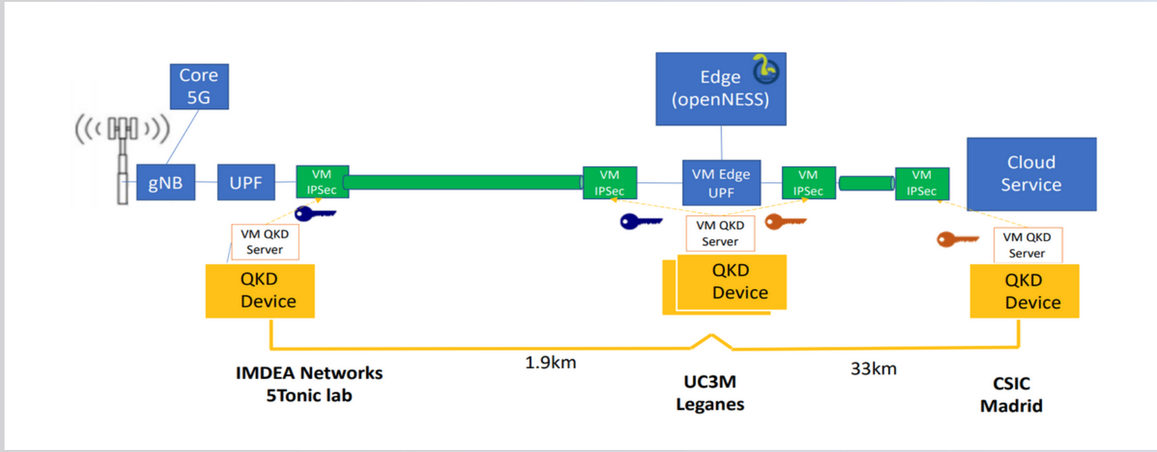
APLICAÇÕES PRÁTICAS DE REDES QUÂNTICAS



EXEMPLOS DE APRESENTADORES E CASOS DE ESTUDO

- **MadQCI**: Descrição de demonstradores como o MadQCI, que avalia a viabilidade de redes quânticas em contextos urbanos.
- **Resultados**: Resultados de testes que demonstram a robustez dos sistemas QKD em ambientes complexos e a sua capacidade de integração com redes 5G.
- **Previsões**: Indicam que o mercado de Quantum-as-a-Service (QaaS) poderá alcançar 26 mil milhões de dólares até ao final da década.

- As empresas de telecomunicações, segurança da informação e infraestrutura digital são as principais beneficiárias.
- A adoção de tecnologias quânticas pode constituir um diferencial competitivo para empresas que pretendem proporcionar segurança de última geração aos seus clientes.



QUANTUM COMO SERVIÇO (QAAS).

O conceito de "Quantum as a Service" (QaaS) representa uma abordagem que visa industrializar e padronizar redes quânticas, promovendo a sua integração nas infraestruturas de rede já existentes.

Componentes essenciais:

- **Quantum Forwarding Plane (QFP)**: O QFP constitui o núcleo do modelo.
- **Módulo QKD**: No âmbito do QFP, os módulos QKD são encarregados da geração e processamento de chaves simétricas, que constituem o principal “produto” nas redes QKD.
- **Repetidores Fiáveis**: Para ultrapassar as limitações de distância impostas pela perda de sinal em canais quânticos, utilizam-se repetidores fiáveis para retransmitir chaves em múltiplos saltos.
- **Key Manager**: Este componente centraliza a gestão de chaves, definindo prioridades e solicitando a criação de novas chaves conforme necessário.

A modularidade do modelo possibilita uma integração fluida com as redes de telecomunicações existentes, aproveitando a infraestrutura atual e incorporando camadas quânticas conforme necessário.

Abordagem “como serviço”: O modelo QaaS foi concebido para oferecer serviços quânticos numa abordagem “como serviço”, permitindo que as funcionalidades quânticas sejam utilizadas de maneira análoga aos serviços em nuvem, promovendo assim a sua adoção e escalabilidade.

A PADRONIZAÇÃO DAS INTERFACES ENTRE COMPONENTES É FUNDAMENTAL PARA ASSEGURAR A INTEROPERABILIDADE ENTRE DIVERSOS FORNECEDORES E TECNOLOGIAS.

QRNG COMO SERVIÇO - CONCEITO E APLICAÇÕES

O QRNG-as-a-Service disponibiliza geradores quânticos de números aleatórios (QRNG) na nuvem, evidenciando a sua acessibilidade e a crescente relevância na cibersegurança quântica.

Mercado Alvo: Organizações que buscam soluções robustas de cibersegurança em um contexto em que a segurança quântica se torna cada vez mais essencial.

Aplicações de QRNGs:

- Criptografía.
- Simuladores e atividades de amostragem.

Tecnologias empregues: Divisores de fótons, detecção homodinâmica, difusão de fase em lasers, entre outras.

Exemplos de serviços de QRNG:

- NIST (EUA): Serviço de Beacon QRNG.
- Telefónica + Quside/Qcrypt: Criação de soluções quânticas.
- Alibaba + Universidade de Tóquio: Integração de serviços em nuvem.

Caso da Alibaba:
Integração em Servidores Cloud: Quatro tipos de QRNG utilizados.
Melhoria da Segurança: Substituição de números pseudoaleatórios, utilização da operação XOR para reforçar a segurança em serviços críticos.

QRNG-as-a-Service está a consolidar-se como uma solução inovadora para a segurança cibernética, com uma adoção crescente em setores que exigem elevada proteção de dados.

DESAFIOS TÉCNICOS NAS REDES QUÂNTICAS.

As redes quânticas do futuro integrarão os nós quânticos com as infraestruturas existentes, possibilitando comunicações e computação quânticas seguras.

Desafios principais

- **Decoerência**: Perda de informação quântica resultante de interações com o ambiente.
- **O teorema da não clonagem**: proíbe a replicação ou transmissão convencional de dados quânticos.

Propostas de Solução: Implementação de repetidores quânticos e protocolos independentes da medição do dispositivo.

Desafios para a escalabilidade comercial

- **Integração com Infraestruturas Existentes**: É imperativo assegurar a compatibilidade com sistemas tradicionais e a interoperabilidade entre diferentes fornecedores.

- **Normalização e Certificação**: A relevância da normalização para a disseminação das tecnologias quânticas e para assegurar a segurança e a fiabilidade das soluções.

- **Sustentabilidade**: Reflexões sobre o impacto ambiental e económico da implementação de redes quânticas em larga escala.

PADRÕES E INTEROPERABILIDADE

Recomendações da ITU-T sobre QKD:
Y3800: Panorama das redes que sustentam a distribuição quântica de chaves (QKD).
Y3801: Requisitos funcionais para redes quânticas de distribuição de chaves.
Y3803: Gestão de chaves em redes quânticas de distribuição de chaves.

Especificações do ETSI ISG QKD:
ETSI GS QKD 015 V1.1.1: Protocolo e formato de dados para a entrega de chaves.
ETSI GS QKD 004 V2.1.1: Gestão de chaves e comunicação segura em redes quânticas.

Abordagens híbridas para a troca de chaves:

As abordagens híbridas integram métodos quânticos e clássicos de troca de chaves.

- IETF RFC 8784: extensão IKEv2 para a implementação de segurança pós-quântica através do uso de chaves pré-compartilhadas.
- NIST: Diretrizes para a geração segura de chaves simétricas de múltiplos segredos.
- IETF draft-campagna-tls-bike-sike-hybrid-06: Definições de intercâmbio de chaves híbridas aplicáveis ao TLS 1.2.