www.fermacrisk.com

mariana.ibancovichi@fermacrisk.es

# Riesgo de la computación Cuántica en la CiberSeguridad

**Material:**

Presentaciones: PDF
Ejemplos en Python y R

**Duración:** 40 h

**Price:** 7.900 €

## OBJETIVO

Basilea explica que las ordenadores cuánticos, si alcanzan el tamaño y la potencia suficientes, pueden romper los esquemas de encriptación ampliamente utilizados hoy en día para garantizar transacciones y datos financieros seguros. Esto hace que la computación cuántica sea una de las amenazas de seguridad cibernética más importantes que enfrenta el sistema financiero, ya que expone potencialmente a ataques todas las transacciones financieras y gran parte de nuestros datos financieros almacenados existentes.

Si bien aún no está claro cuándo podría adoptarse la tecnología de computación cuántica a gran escala, su potencial como ciberamenaza para el sistema financiero ya es motivo de preocupación. Los actores malintencionados pueden interceptar y almacenar datos confidenciales cifrados de forma clásica con la intención de descifrarlos más tarde cuando las computadoras cuánticas sean lo suficientemente poderosas para hacerlo.

Reconociendo estos riesgos potenciales para sus sistemas y datos, el sector financiero necesita implementar de manera preventiva tecnologías robustas de comunicación cuántica y protección de datos. Dada la sensibilidad a largo plazo de los datos financieros y la complejidad de los sistemas de IT del banco central, se debe iniciar una fase de transición con mucha anticipación para que se puedan implementar esquemas de cifrado resistentes a la cuántica.

**Consideramos que el reciente descubrimiento del nuevo material para construir superconductores LK 99, a temperatura ambiente, pudiera acelerar el salto cuántico.**

El objetivo del curso es exponer el impacto y riesgos de la computación y tecnologías cuánticas en la ciberseguridad de las entidades financieras, para alcanzar el objetivo explicamos que es la computación

cuántica, los algoritmos cuánticos, mecánica cuántica y la criptografía cuánticas y postcuántica, lattice based, para defenderse de las posible amenazas cuánticas.

El curso explica pormenorizadamente la interacción entre la geopolítica, riesgo reputacional y ciberseguridad, los posibles escenarios que se esperan con el progreso de los ordenadores cuánticos.

Se explica el uso de la inteligencia artificial para fortalecer la ciberseguridad de los bancos. Se explica brevemente la metodología XOI para medir el ciberriesgo.

Se expone la visión global del CiberRiesgo, los ciberataques y pérdidas que han sufrido las entidades financieras, las metodologías y buenas practicas sobre ciberseguridad en los procesos de negocio y se explican algunos estándares técnicos para la gestión y control, tales como el NIST, Cobit 5 e ISO 27001.

Se exponen metodologías de Cyber Risk Appetite, Cyber Risk Limits y Cyber Risk Tolerance para la gobernanza y control del CiberRiesgo.

Se exponen metodologías tradicionales como la regresión logística y otras, innovadoras, de machine learning, tales como: árboles de decisión, naive bayes, KKN, Regresión logística LASSO, random forest, redes neuronales, redes bayesianas, Support Vector Machines, gradient boosting tree, etc

Se explica el uso de la inteligencia artificial y en particular del machine learning y deep learning para fortalecer la ciberseguridad, se muestran modelos avanzados para detectar anomalías, fraudes transaccionales, phishing, ataques cibernéticos, intrusiones y malware.

Se explica al deep learning avanzado, con redes neuronales convolucionadas para el reconocimiento facial, el potente Generative Adversarial Network (GAN) para detectar ataques adversos de algoritmos de machine learning, las redes neuronales recurrentes para la clasificación de eventos del CiberRiesgo y la multicapa perceptron para la detección de intrusiones y anomalías.

**¿QUIÉNES DEBEN ASISTIR?**

Este programa esta dirigido a directores, gerentes, consultores, reguladores, auditores y analistas de riesgos, riesgos operacionales, ciberriesgos así como aquellos profesionales que se encuentren implantando medidas de ciberseguridad. Profesionistas que trabajen en entidades bancarias, cajas de ahorro y todas aquellas empresas que se encuentren expuestas al ciberriesgos.

# CiberSeguridad en Basilea III

**Módulo 1: CiberResilencia**

- CiberRiesgos en la banca
- CiberRiesgos en Latinoamérica y Europa.
- Normas y directrices de ciberresiliencia
- Caso Estudio 1: iniciativas regulatorias recientes: los requisitos mínimos de Australia, Alemania y EE. UU
- Cibergobernanza
    - Estrategia de ciberseguridad
    - Roles y responsabilidades de gestión
    - Reconocimiento de la importancia de la junta directiva y la alta gerencia
    - Variedad de enfoques de supervisión con respecto a la segunda y tercera líneas de defensa (3LD)
    - Caso de Estudio 2: Roles y responsabilidades de los directores de seguridad de la información (CISO) en la cibergobernanza
    - Cultura de sensibilización sobre el riesgo cibernético
    - Arquitectura y estándares
    - Fuerza laboral de ciberseguridad
    - Caso de Estudio 3: Marcos para la formación profesional en ciberseguridad y programas de certificación
- Enfoques de gestión de riesgos, pruebas y respuesta y recuperación de incidentes
    - Métodos para supervisar la ciberresiliencia
        - Los especialistas en riesgos evalúan la gestión y los controles de seguridad de la información
        - Las jurisdicciones se involucran cada vez más con la industria para abordar la ciberresiliencia
    - Pruebas de controles de seguridad de la información y garantía independiente
        - El mapeo y la clasificación de los servicios comerciales deben informar las pruebas y el aseguramiento
        - Prueba de Penetración
        - Taxonomía de controles de riesgo cibernético
    - Pruebas de respuesta y recuperación y ejercicio
        - Evaluación de continuidad del servicio, planes de respuesta y recuperación y aprendizaje continuo
        - Ejercicio conjunto público-privado
        - Caso de Estudio 4: “Exercise Resilient Shield”
    - Métricas de ciberseguridad y resiliencia
        - Las métricas de ciberseguridad y resiliencia
        - Indicadores emergentes emergentes de resiliencia
- Comunicación e intercambio de información
    - Descripción general de los marcos de intercambio de información entre jurisdicciones
    - Compartir entre bancos o peers información
    - Caso de Estudio 5: FS-ISAC: características y beneficios clave
    - Compartir de los bancos a los reguladores
    - Compartir entre los reguladores
    - Caso de Estudio 6 - Intercambio bilateral de información sobre seguridad cibernética entre la Autoridad Monetaria de Hong Kong (HKMA) y la Autoridad Monetaria de Singapur (MAS)

# Gestión de los CiberRiesgos

**Módulo 2: CiberRiesgos**

- Visión Actual del Ciberriesgo
- identificación de los Ciberriesgos
    - Malware y otras amenazas

- Ciber-Seguridad en la práctica
    - 
    - Gobierno de la Seguridad
    - Gestión del Riesgo
    - Políticas de Seguridad
    - Política de Salvaguardas
    - Planes de Contingencias
- Auditorías de Seguridad
- Algunos Ciberriesgos
    - Exploits Kits
    - Fuga de información
    - Pishing
    - Ataque DDoS
    - Internet de las cosas
    - Ataque a infraestructuras
    - Botnets
    - Troyanos
    - Malware Avanzado
    - Ransomware
    - APT´s
- Evitación, Aceptación, Mitigación o transferencias de los Ciber-Riesgos (Ciber-Seguros)
- Respuesta a Incidentes
- Aspectos Legales de la Respuesta a Incidentes
- Informática Forense
- Compliance Digital
- Inteligencia en Fuentes Abiertas
- Defensa de la Marca. Derechos de Propiedad Intelectual
- Reputación Digital. Comunicación de Crisis
- Fraude y Gestión de la Identidad Online
- Derecho Informático y de las TIC´s
- Derecho Procesal y Derechos Humanos en el Ciber-Espacio
- Responsabilidad Penal de las Personas Jurídicas
- Criptografía y Sistemas de Autenticación
- Ciber-Seguridad Industrial (IT/OT)
- Ciber-Seguridad Lógica
- Aseguramiento
- CiberRiesgos en la banca
- Robos financieros
- Ataques en las transacciones bancarias
- Robo de tarjetas de crédito
- Banca Mayorista
- Ciber ataque Lazarus en el sistema SWIFT
- Recursos de los bancos destinados en ciberseguridad
- Cloud service provider (CSP)
- Análisis de los principales proveedores CSP
- Análisis y duración de los apagones en el servicio Cloud

**Módulo 3: Gestión del CiberRiesgo**

- Enterprise Risk Management en el ciberriesgo
- Involucración de la alta dirección
- Ciberseguridad en los procesos de negocios
- Identificación de:
- Activos críticos del banco
- Funciones de negocio críticas
- Socios comerciales críticos: clientes, proveedores, outsourcing
- Data crítica, conexiones críticas

- Principales amenazas al banco
- Framework for Improving Critical Infrastructure Cybersecurity NIST
- Principales Estándares técnicos
    - NIST 800-53
    - Cobit 5
    - ISO 27001
- Politicas y control del ciberRiesgo
- Gobernanza del CiberRiesgo en la práctica
- Líneas de defensa
- Análisis del riesgo
- Mapas de probabilidad e impacto
- Estrategias de mitigación de CiberRiesgo
    - Identidad y gestión de los accesos
    - Protección de la data
    - Security analytics usando machine learning
    - NIST CSF pillars
    - Higiene de seguridad
    - Recovery time objective
    - Recovery point objective
    - SSDLC
    - Gestión del riesgo de la tecnología de terceros
- Arquitectura de seguridad
- Entorno Cloud y mobile security

**Módulo 4: Medición de Ciberataques usando Enfoque XOI: Exposición, Ocurrencia e Impacto**

- Definición de  la exposición
- Selección de los KRIs
- Modelización y condicionamiento de la exposición
- Definición de hipótesis
- Modelización y condicionamiento de la ocurrencia
- Cuantificación de la ocurrencia
- Cuantificación del impacto
- Tipos de indicadores
- Predecibilidad de los indicadores
- Redes Bayesianas
- El modelo de escenario de la red bayesiana
- Interpretación gráfica
- Simulación usando redes bayesianas
- Modelización de XOI para Ciberriesgos en la banca
- Escenarios de CiberRiesgos
- Ciberataques en la banca
- Ejercicio 1: Modelización XOI en ciberataques usando redes bayesianas en Python y R

**Módulo 5: Cyber Risk Appetite**

- Principios de una metodología efectiva de Cyber Risk Appetite
- Definiciones y análisis:
    - Risk appetite framework
    - Risk Appetite Statement
    - Risk Tolerance
    - Risk Capacity
    - Risk Profile
- Establecimiento de Límites en el CiberRiesgo
- Principios de Efectividad del Cyber Risk Appetite Statement
- Establecimiento de Límites y Métricas en CiberRiesgos
- Establecimiento de límites de riesgo y tolerancia en CibeRiesgos

- Incorporación del Cyber Risk Appetite en la toma de decisión, nuevos productos, nuevas líneas de negocio, etc.
- Planes de mitigación

# Machine Learning y AI para la Ciberseguridad

### Módulo 6: Machine Learning

- Inteligencia Artificial
- Definición del Machine Learning
- Metodología del Machine Learning
    - Almacenamiento de la Data
    - Abstracción
    - Generalización
    - Evaluación
- Aprendizaje Supervisado
- Aprendizaje No Supervisado
- Aprendizaje por Refuerzo
- Deep Learning
- Tipología de algoritmos de Machine Learning
- Pasos para implementar un algoritmo
    - Recogida de información
    - Análisis Exploratorio
    - Entrenamiento del modelo
    - Evaluación del Modelo
    - Mejoras al modelo
    - Machine Learning en riesgo crédito de consumo
- Machine Learning en modelos de credit scoring
- Análisis de principales herramientas: R, Python, Microsoft Azure, SAS Enterprise Miner, SAS Visual Analytics, Knime, IBM SPSS Modellller, Spark,,etc.

### Módulo 7: Inteligencia artificial IA para la CiberSeguridad en Banca

- Inteligencia artificial IA para la ciberseguridad
- Detección de anomalías en la seguridad cibernética
    - Modelos avanzados de deep learning
- Uso del Aprendizaje Supervisado en la ciberseguridad
- Uso del Aprendizaje No Supervisado en la ciberseguridad
- Detección y mitigación del Phishing
    - SVM
    - Clustering
- Deep Learning para la detección de ataques y malware
    - Redes Neuronales recurrentes
- Detección de instrusiones
- Network Traffic Analysis
- Detección de botnets
- Machine learning para detectar ataques DDoS
- Detección de fraude en transacciones financieras
- Detección en sensores
- Analítica de fraudes en banca
- Técnicas avanzadas de machine learning para ciberseguridad
- Principales vendors de IA para ciberseguridad
- Herramientas de visualización
- Beneficios de la IA en la ciberseguridad
- Crecimiento de la IA en la ciberseguridad
- Desafíos y limitaciones

### Módulo 8: Ciberseguridad y AI Avanzada

- Detección de actividad sospechosa
- Algoritmos de aprendizaje automático para la detección de intrusos Detección de malware mediante transformadores y BERT
- Detección de reseñas falsas
- Detección de texto generado por máquina
- Detección de noticias falsas con redes neuronales gráficas
- Modelos de ataque con aprendizaje automático adversario
- Desarrollando robustez contra ataques adversarios
    - Adversarial machine learning
    - Ataques adversos para la ciberseguridad
    - Tipología de ataques adversos
    - Muestras adversarias
    - Generative Adversarial Network (GAN)
    - Fast Gradient Sign Method (FGSM)
- Creación de muestras de malware adversarial utilizando GAN
- Protección de la privacidad del usuario con aprendizaje automático

## Computación Cuántica

### Módulo 9: Computación Cuántica y algoritmos

Objetivo: La computación cuántica aplica los fenómenos mecánicos cuánticos. A pequeña escala, la materia física exhibe propiedades tanto de partículas como de ondas, y la computación cuántica aprovecha este comportamiento utilizando hardware especializado. La unidad básica de información en la computación cuántica es el qubit, similar al bit en la electrónica digital tradicional. A diferencia de un bit clásico, un qubit puede existir en una superposición de sus dos estados "básicos", lo que significa que se encuentra en ambos estados simultáneamente.

- Futuro de la computación cuántica en los seguros
- ¿Es necesario saber mecánica cuántica ?
- Aplicaciones y hardware de QIS
- Operaciones cuánticas
- Representación de Qubit
- Medición
- Superposición
- Multiplicación de matrices
- Operaciones de Qubits
- Múltiples Circuitos cuánticos
- Entanglement
- Algoritmo de Deutsch
- Transformada cuántica de Fourier y algoritmos de búsqueda
- Algoritmos híbridos cuánticos-clásicos
- Quantum annealing, simulación y optimización de algoritmos
- Algoritmos cuánticos de machine learning

### Módulo 10: Introducción a la mecánica cuántica

- Teoría de la mecánica cuántica
- La función de onda
- La ecuación de Schrödinger
- La interpretación estadística
- Probabilidad
- Normalización
- Impulso
- El principio de incertidumbre

- Herramientas Matemáticas de la Mecánica Cuántica
- El espacio de Hilbert y las funciones de onda
- El espacio vectorial lineal
- El espacio de Hilbert
- Dimensión y bases de un Espacio Vectorial
- Funciones cuadradas integrables: funciones de onda
- Notación de Dirac
- Operadores
- Definiciones generales
- Adjunto hermitiano
- Operadores de proyección
- Álgebra del conmutador
- Relación de incertidumbre entre dos operadores
- Funciones de los Operadores
- Operadores Inversos y Unitarios
- Eigenvalues and Eigenvectors de un operador
- Transformaciones unitarias infinitesimales y finitas
- Matrices y Mecánica Ondulatoria
- Mecánica de matrices
- Mecánica Ondulatoria

**Módulo 11: Circuitos de corrección de errores de números cuánticos**

- Código de corrección de errores clásico versus error cuántico
- Código de corrección
- Circuito de corrección de errores cuánticos
- Funcionamiento del código de corrección de errores cuánticos
- Tipos de Blunder en Quantum Computer
- Bit Flip Code
- Elementos estabilizadores que detectan errores
- Barreras en el método de corrección de errores existente
- Fase de Flip Code
- Implementación de Circuito cuántico de fase Flip Code
- Bit Flip y Fase Flip Code
- Bell States
- Implementación QCL del código de corrección de errores cuánticos
- Aplicaciones del circuitos de corrección de errores cuánticos
- Configuración de la simulación
- Implementación de sistemas de hardware
- Distribución de claves cuánticas
- Spin o polarización
- Criptografía cuántica usando el operador XOR
- Pseudocódigo para la criptografía cuántica propuesta
- Sustitución aleatoria
- Principales aspectos destacados de los reemplazos arbitrarios
- Cálculo de desarrollo de claves en cifrado XOR
- Reemplazo híbrido
- Ventajas de la criptografía cuántica propuesta
- Detección de errores
- configuración de hardware
- Pseudocódigo
- Flujo de código del receptor
- Flujo de código del transmisor
- Configuración de simulación
- Configuración del receptor

**Módulo 12: Comunicaciones cuánticas**

- Seguridad Teórica de la Información
- RSA-129
- Grover's algorithm
- Shor's algorithm
- Fourier Transform algorithm
- Quantum Key Exchange
- Quantum networking
- SIGINT y adopción de cifrado
- Secret sharing
- Generación cuántica de números aleatorios (QRNG)
- The NIST Randomness Beacon
- Distribución de clave cuántica
- BB84
- Cómo funciona QKD
- Por qué QKDI es seguro
- Quantum Money
- Quantum Computing y Bitcoin
- QKD gana impulso
- QKD Comercializado, Miniaturizado
- Internet cuántico

**Módulo 14 : Prueba cuántica del sistema financiero**

- La ciberamenaza cuántica para los sistemas de TI del banco central
    - Por qué la computación cuántica representa una ciberamenaza
    - La amenaza potencial para las técnicas criptográficas actuales
- Cómo defenderse de la amenaza cuántica
    - Una cooperación internacional organizada por NIST
    - Las soluciones se pueden implementar ahora
- Cómo preparar y crear entornos cuánticos seguros
    - Criptografía poscuántica vs criptografía cuántica
    - Los bancos centrales deben prepararse ahora
- Proyecto Leap
    - Objetivos y alcance
    - Diseños de soluciones
    - Implementación y pruebas
- Hallazgos
    - Agilidad criptográfica
    - Actuación
    - Seguridad
- Conclusión y próximos pasos
- Necesidad de un plan de migración
- Desafíos de implementación
- Próximos pasos

**Módulo 15: Criptografía cuántica y distribución de claves cuánticas**

- Fundamentos de la Criptografía Cuántica
- Principio de incertidumbre de Heisenberg
- Enredo cuántico
- Polarización de fotones
- Teorema cuántico de no clonación
- Distribución de claves cuánticas

- Distribución de claves cuánticas basada en preparar y medir
- Protocolo BB84
- Otros protocolos basados en preparar y medir
- Una distribución de clave cuántica basada en entrelazamiento
- Protocolo de Ekert's
- Variantes BB84 enredadas

**Módulo 16: Firmas digitales postcuánticas y Lattice Based Cryptography**

- Introducción
- Firmas digitales y su seguridad
- Firmas seguras en ROM
- Modelización del adversario cuántico
- Competencia de estandarización NIST PQC
- Lattice Based Cryptography
- Introducción a Ring-LWE
- Muestreo gaussiano discreto
- NTRUSign
- GPV  Framework
- Fiat-Shamir con cancelaciones
- Esquema de firma CRISTALES-DILITHIUM
- Firmas basadas en MQ
- Problemas difíciles basados en MQ
- Firmas de aceite y vinagre
- Firmas HFE
- Firmas basadas en técnicas de clave simétrica
- Firmas basadas en isogénias supersingulares

## Cloud computing

**Módulo 17: Computación en la nube y riesgos de seguridad**

- Descripción general de los modelos
- Marcos de evaluación de riesgos de seguridad
- Modelos de evaluación de riesgos de la nube
- Modelo de evaluación de riesgos de adopción de la nube
- Análisis de riesgos consultivo, objetivo y bifuncional
- Marcos de evaluación de riesgos de la nube
- Marco de gestión de riesgos de seguridad en la nube
- Marco de gestión de riesgos de seguridad de la información
- Marco de evaluación de riesgos de seguridad
- Análisis de rendimiento de los modelos y marcos existentes

## Riesgos Cibernéticos Físicos

**Módulo 18: Riesgo cibernético físico**

- Disuasión cibernética
- Comprender el riesgo físico cibernético
- La amenaza para las empresas
- El arte de lo posible: lo que pueden y no pueden hacer los ciberataques físicos
- Escenarios ciberfísicos
- Una nota sobre la clasificación de los poderes cibernéticos
- Escenario 1: Intercambio de ataques asimétricos: Ransomware en infraestructura crítica
- Escenario 2 – Represalias cibernéticas ofensivas: sabotaje ciberfísico de infraestructura crítica

- Escenario 3 – Intercambio de ataques simétricos: escalada de ataques destructivos en infraestructura crítica
- Seguro físico cibernético

**Módulo 19: Análisis de Riesgo de Evaluación de la Interdependencia de vulnerabilidades En Sistemas Ciber-Físicos**

- Perspectiva de control de amenazas
- Métodos para esquematizar la gravedad del outbreak
- Método cuantitativo de la severidad del outbreak
- Método cuantitativo de probabilidad de consecución de outbreak
- Impacto de las vulnerabilidades y modo de utilización
- Modelización de ataques en un CPS
- Supervisión en línea en un sistema ciberfísico

## Riesgos Emergentes: Geopolítico y Reputacional

**Módulo 20: Criptodivisas, ciberseguridad y energías verdes**

- La geopolítica de la moneda criptos
- Impacto de la energía verde
- Aplicar lecciones de la historia a un nuevo contexto
- Medición de la ciberseguridad en el riesgo geopolítico
- Cambio climático, energías renovables y reconfiguración del riesgo geopolítico
- Criptomoneda, finanzas descentralizadas y el equilibrio de poder global

**Módulo 21: Medición del Riesgo Geopolítico**

- Medición del riesgo geopolítico
- Inteligencia artificial aplicada a los riesgos geopolíticos
- Machine Learning y Deep Learning
- Enfoques cuantitativos versus cualitativos
- Calificaciones de riesgo geopolítico
- Identificar señales de alerta temprana
- Identificar problemas clave
- interpretación de tendencias en datos financieros y económicos.
- Gestionar la información
- Creación de índices de geopolítica
- Análisis de los principales indices
- Posibles sesgos en los índices
- Tipología de artículos para mejoras de índices

**Módulo 22: Medición del Riesgo Reputacional**

- Definición y naturaleza de la Reputación
- Identificación del riesgo reputacional
- Valoración del riesgo reputacional
- Expectativas de los Stakeholders
- Áreas de riesgo y categorias de stakeholders
- Riesgo Reputacional Interno
- Riesgo Reputacional Externo
- Valoración a través de escenarios e impacto
- Uso de los Risk Control Self Assessment en riesgo reputacional
- KRIs importantes del Riesgo Reputacional
- Caso Práctico de presentación de resultados a la Alta dirección

### Módulo 23: Medición Avanzada del Riesgo Reputacional (RR)

- Modelización avanzada del riesgo reputacional
- Relación de eventos de riesgo operacional
- Variables financieras que influyen el RR
- Probabilidad del Riesgo Reputacional
- Modelización con regresión logística

### Módulo 24: Gestión Avanzada del Riesgo Reputacional

- Gobernanza del riesgo reputacional
- Roles y Responsabilidades del Consejo, CEO, CRO y CFO
- Expectativas y Gestión de los Stakeholders
- Integración del Riesgo reputacional en el Risk Appetite Framework
- Valoración a través de escenarios e impacto
- Análisis tipo Traffic Light de probabilidad e impacto
- Reporting del Riesgo Reputacional
- Mitigación del Riesgo Reputacional
- Impacto del entorno social
- Relación con ONGs y Medios de comunicación
- Puntos Claves en la gestión del riesgo reputacional
- Otros temas:
    - Online Reputation Management
    - Reputación social en banca

## Ciberseguridad, Geopolítica y tecnologías cuánticas

### Módulo 25: CiberSeguridad, Geopolítica y Escenarios

- El panorama cibernético mundial
- Geopolítica
- Tecnología emergente
- Amenazas emergentes
- Leyes y reglamentos
- Modelización de las amenazas
- Escenarios futuros de tecnología cuántica
- Escenario 1: Gobierno Superior y Dominante
    - Criptoanálisis
    - Firmas falsificadas y sistemas jurídicos
    - Ataques a Contraseñas y Otros Sistemas de Autenticación
    - Teledetección
    - QKD e Internet cuántico
    - secreto y filtración
    - Contramedidas en un escenario dominado por el gobierno: perturbación, negación, degradación, destrucción y engaño
- Escenario 2: tecnologías cuánticas podrían cambiar la gobernanza y la ley
    - Implicaciones para la primacía humana
    - Tecnología Cuántica y Derecho Espacial
    - Tecnología Cuántica y Ciberseguridad
    - Tecnología cuántica y privacidad
    - Secretos y su valor en el tiempo
    - Reglamento de descifrado
    - Desafíos del poder del gobierno
    - El enfoque europeo de los derechos de privacidad
    - Predicción cuántica
    - Desarrollo de productos

    - Justicia
    - Salida de patentes de Quantum Technology
    - El invierno de la computación cuántica es un escenario probable para 2030
- Escenario 3: Público/Privado, Bloque Este/Oeste
- Escenario 4: invierno cuántico
- Escenario 5: Super conductores LK99