VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Estrategias de Ciberseguridad

De la Visión a la Acción

Elder Guerra Villagrán

Consultancy Services Director

ES Consulting

CONSULTING

Experto en Estrategia Empresarial, implementación de de la metodología del **Execution Premium Process**.

Estrategia Empresa, TI, Cumplimiento

Ciberseguridad

Inteligencia Aritficial

Continuidad del Negocio

Facultad Sistemas - UMG
MBA PUC Chile
Candidato a Dr. En Investigación

Kaplan & Norton
BSC & Strategy Certified

Experto Técnico en ISO/IEC JTC1/SC27/WG1 familia ISO 27000

Auditor de certificación en ISO 9001, 20000-1, 22301, 27001, 27017, 27018, TISAX por TUV-NORD.

Elder Guerra Villagrán

Co-Founder &

Consultancy Services Director

Educación Superior

Universidad Mariano Gálvez - Ingeniería de Sistemas

Pontificia Universidad Católica de Chile - Master in Business Administration (MBA)

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Profesionales certificados

- **ISO/IEC 27001:** Information Security Management Systems
- **ISO/IEC 27032** Cybersecurity Management
- **ISO 9001:** Quality Management Systems
- **ISO/IEC 20000-1:** IT Services Management Systems
- **ISO/IEC 27035:** Information Security Incident Handling
- **ISO 22301:** Business Continuity Management Systems
- **CISSP:** Certified Information Systems Security Professional
- CISCO Certified CCNA Security
- **Offensive Security And Penetration Testing**
- **CEH Certified** Ethical Hackers
- **Digital Forensics**
- **SWIFT Customer Security Controls Framework**
- **Web Application Security Testing**
- **Risk Management**
- **Cloud Security**
- **PMP Project Management**
- **Kaplan & Norton Strategy Management**
- **CRISC**
- **CISA**
- **CISM**

En el escenario de negocios, la ciberseguridad es más que una prioridad, es la línea de defensa que protege el corazón de la compañía:

Los Datos.

Nos tomamos en serio el corazón de su empresa.

CS CONSULTING

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Hemos sumado capacidades y experiencias de para conformar una firma que entrega soluciones de ciberseguridad que agregan **valor y confianza**.

Ciberseguridad
Seguridad de la información

Estrategia
TI - Ciberseguridad

Resiliencia

- Equipo de profesionales de alta experiencia
- Experiencia internacional y multisectorial
- Certificaciones de validez internacional
- Miembros del comité técnico de la **ISO/IEC JTC 1**

+50 Profesionales en ciberseguridad

+200 Certificaciones de expertos

+200 Clientes satisfechos

CONSULTING

Panorama Global en materia de Riesgos

1

Estrategia de Ciberseguridad alineada a la Estrategia Institucional

2

The most important global business risks for 2025

1
38%
→
2024: 1 (36%)

Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

2
31%
→
2024: 2 (31%)

Business interruption

(incl. supply chain disruption)

3
29%
→
2024: 3 (26%)

Natural catastrophes

(e.g., storm, flood, earthquake, wildfire, extreme weather events)

4
25%
→
2024: 4 (19%)

Changes in legislation and regulation

(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)

5
19%
↑
2024: 7 (18%)

Climate change

(e.g., physical, operational and financial risks as a result of global warming)

6
17%
→
2024: 6 (19%)

Fire, explosion

7
15%
↓
2024: 5 (19%)

Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)

8
14%
↑
2024: 9 (13%)

Market developments[1]

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

9
14%
↓
2024: 8 (14%)

Political risks and violence

(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)

10
10%
↑
NEW

New technologies

(e.g., risk impact of artificial intelligence, connected / autonomous machines)

Key

- ↑ Risk higher than in 2024
- ↓ Risk lower than in 2024
- → No change from 2024
- (5%) 2024 risk ranking %

Source: Allianz Commercial

Figures represent the number of risks selected as a percentage of all survey responses from 3,778 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

NEW New entry in the top 10 risks

The 14th annual Allianz Risk Barometer survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of Allianz Commercial and other Allianz entities.

View the full Allianz Risk Barometer 2025 rankings here

ALLIANZ COMMERCIAL

Allianz Risk Barometer

Identifying the major business risks for 2025

The most important global business risks for 2026

Ranking changes are determined by positions year-on-year, ahead of percentages.

The 15th annual **Allianz Risk Barometer** survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of Allianz Commercial and other Allianz entities.

View the full Allianz Risk Barometer 2026 rankings here

1 — Cyber incidents — 42% → (2025: 1 (38%))

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

2 — Artificial intelligence — 32% ↗ (2025: 10 (10%))

(e.g., implementation challenges, liability exposures, misinformation / disinformation)

3 — Business interruption — 29% ↘ (2025: 2 (31%))

(incl. supply chain disruption)

4 — Changes in legislation and regulation — 26% → (2025: 4 (25%))

(e.g., tariffs, new directives, sustainability requirements)

5 — Natural catastrophes — 21% ↘ (2025: 3 (29%))

(e.g., storm, flood, earthquake, wildfire)

6 — Climate change — 19% ↘ (2025: 5 (19%))

(e.g., physical, operational and financial risks as a result of extreme weather)

7 — Political risks and violence — 15% ↗ (2025: 9 (14%))

(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)

8 — Macroeconomic developments — 14% ↘ (2025: 7 (15%))

(e.g., inflation, deflation, monetary policies, austerity programs)

9 — Fire, explosion[1] — 13% ↘ (2025: 6 (17%))

10 — Market developments — 13% ↘ (2025: 8 (14%))

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

Rank		Percent	2025 rank	Trend
11	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*[2]	8%	*12 (9%)*	↗
12	Talent or labor issues	8%	*11 (9%)*	↘
13	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	6%	*13 (8%)*	→
14	Theft, fraud, corruption[3]	5%	*14 (7%)*	→
15	Insolvency	5%	*16 (6%)*	↗
16	Loss of reputation or brand value *(e.g., public criticism)*[4]	4%	*15 (7%)*	↘
17	Biodiversity and nature risks *(e.g., water scarcity)*[5]	4%	NEW	↗
18	Product recall, quality management, serial defects	4%	*18 (4%)*	→
19	Human health risk *(e.g., pandemic outbreak)*	3%	*19 (3%)*	→
20	Pollution event	1%	*17 (6%)*	↘
	Other	2%		

Source: Allianz Commercial

Figures represent the number of risks selected as a percentage of all survey responses from 3,338 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

NEW: New entry in the top risks

Key

↗ Risk higher than in 2025 → No change from 2025

↘ Risk lower than in 2025 (5%) 2025 risk ranking %

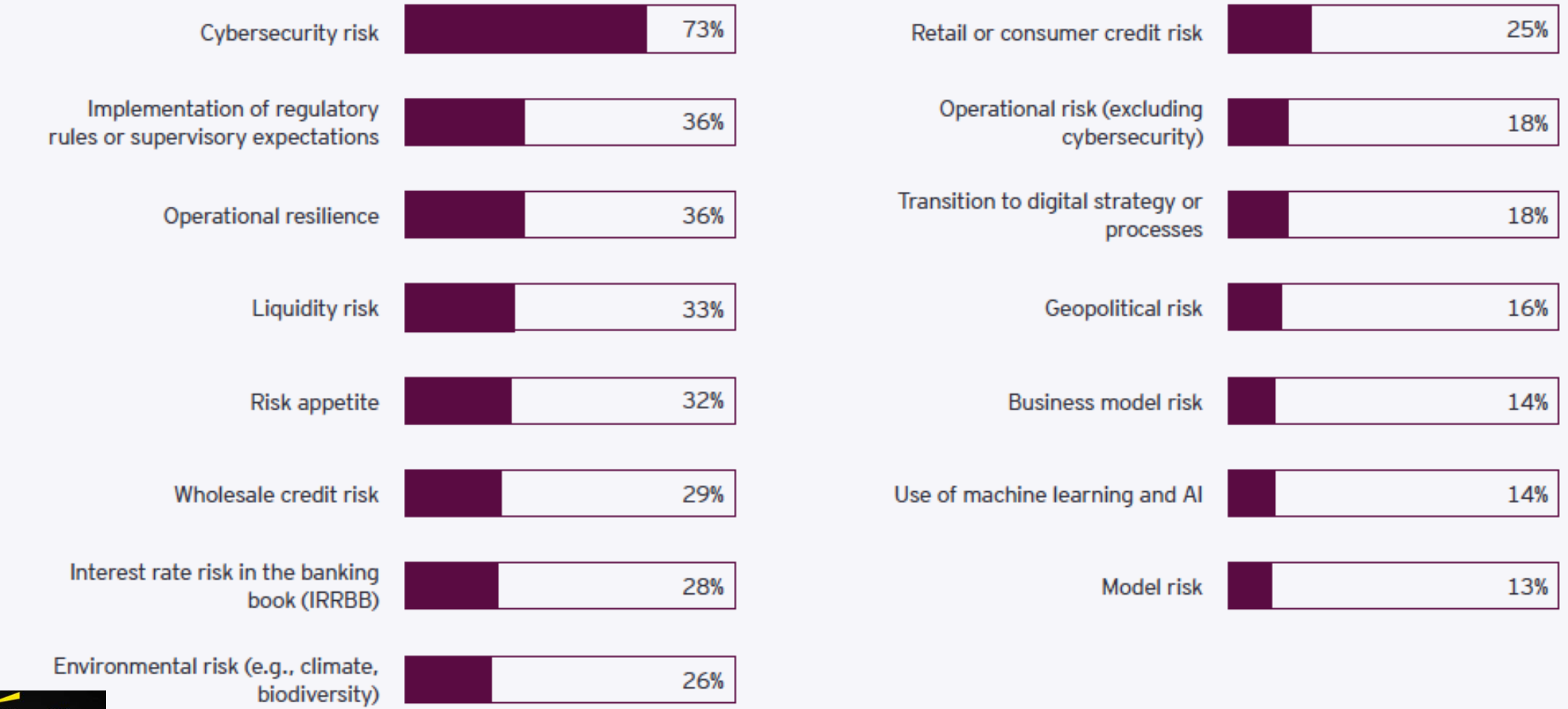
1. Fire, explosion ranks higher than market developments based on the actual number of responses
2. Critical infrastructure blackouts ranks higher than talent or labor issues based on the actual number of responses
3. Theft, fraud, corruption ranks higher than insolvency based on the actual number of responses
4. Loss of reputation or brand value ranks higher than biodiversity and nature risks based on the actual number of responses
5. Biodiversity and nature risks ranks higher than product recall, quality management, serial defects based on the actual number of responses

ALLIANZ COMMERCIAL

Allianz Risk Barometer

Identifying the major business risks for 2026

Figure 1: Over the next 12 months, what are the top five risk management issues that will require the most attention from the CRO?



Perspectiva Global – Cambio de Mentalidad

- Incremento de transformación digital, ciberdependencia e innovación tecnológica, IA, deepfakes, cryptojacking y mas.
- Cada brecha de seguridad cuesta en promedio $3.6 Millones
- Caida de hasta 3% en precio de la acción por 6 meses
- 39% han tenido incidentes en los últimos 2 años
- Incremento en ataques de Ransomware
- 80% creen que el ransomware se está volviendo una amenaza para la seguridad pública
- Incidentes: Tiempo promedio de 280 dias desde la identificación hasta la recuperación.

Perspectiva Global – Cambio de Mentalidad

- La clave será cambiar la mentalidad de Ciberseguridad a Ciber Resilencia.

- La Ciber Resiliencia es la capacidad de una organización para trascender (anticipar, resistir, recuperarse y adaptarse a) cualquier estrés, falla, peligro y amenaza a sus recursos cibernéticos dentro de la organización y su ecosistema, de modo que la organización pueda cumplir con su misión, mantener su cultura y forma deseada de operar.

-Definición del reporte-

"Las instituciones no serán juzgadas porque sufrieron un ciberataque sino por su capacidad de respuesta."

In collaboration with Accenture

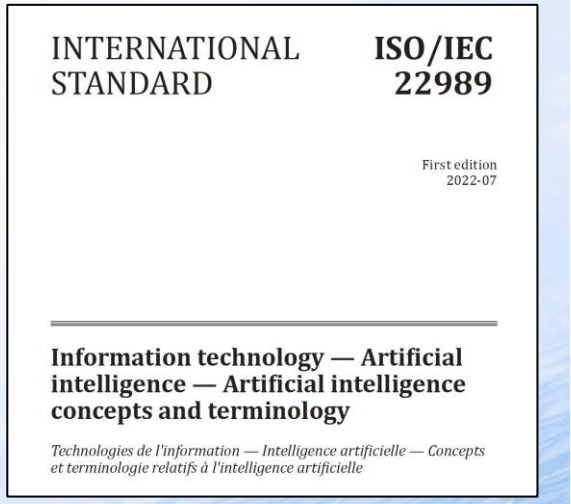
WORLD ECONOMIC FORUM

Global Cybersecurity

Robet Silvers – US Department of Homeland Security
Secreraty for Strategy Policy and Plans

Buenas prácticas internacionales

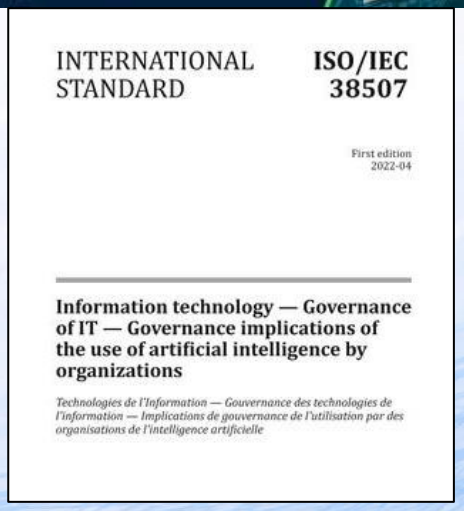
ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM


INTERNATIONAL STANDARD ISO/IEC 22989

First edition 2022-07

Information technology — Artificial intelligence — Artificial intelligence concepts and terminology

Technologies de l'information — Intelligence artificielle — Concepts et terminologie relatifs à l'intelligence artificielle


INTERNATIONAL STANDARD ISO/IEC 38507

First edition 2022-04

Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

Technologies de l'Information — Gouvernance des technologies de l'information — Implications de gouvernance de l'utilisation par des organisations de l'intelligence artificielle

ISO 27035 Cybersecurity Incident Response

ISO 27017 International Organization for Standardization

ISO 27018 International Organization for Standardization

CSA cloud security alliance®


INTERNATIONAL STANDARD ISO/IEC 23894

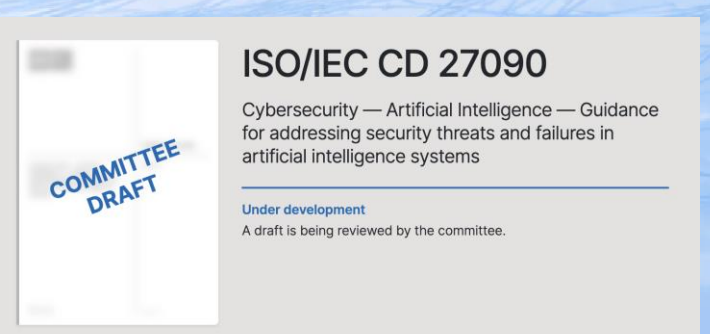
First edition 2023-02

Information technology — Artificial intelligence — Guidance on risk management

Technologies de l'information — Intelligence artificielle — Recommandations relatives au management du risque

AMERICAN EXPRESS · mastercard · PCI DSS COMPLIANT · VISA

ISO 19011 Auditor



ISO/IEC CD 27090

Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems

Under development
A draft is being reviewed by the committee.

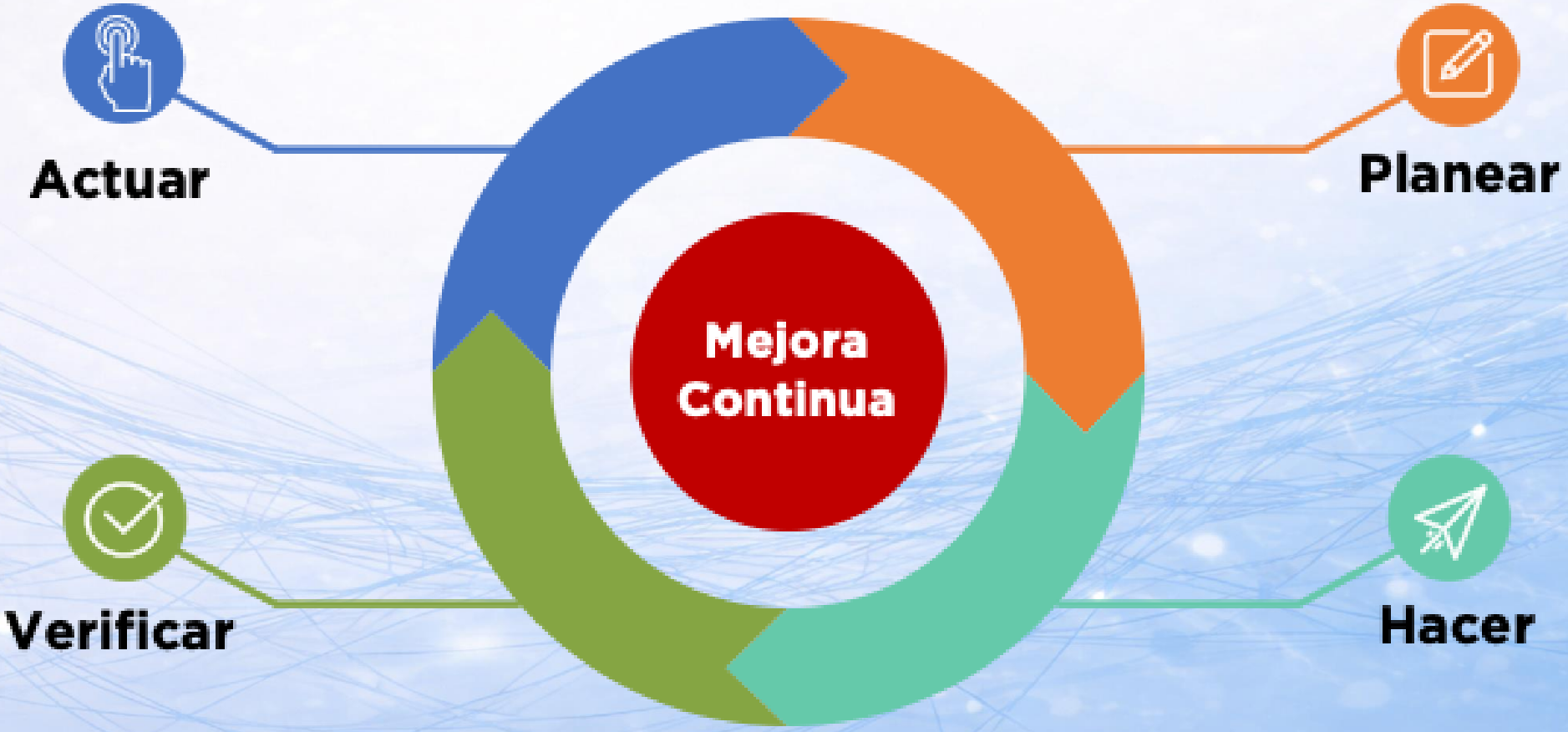
CIS Controls

Estategias de Ciberseguridad

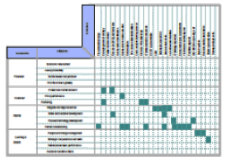
-De la Visión a la Acción-

Estrategia de Ciberseguridad

La Estrategia NO es un Estado, es un Proceso que debe cumplir el **ciclo de la mejora contínua**, pilar de los sistemas de gestión.



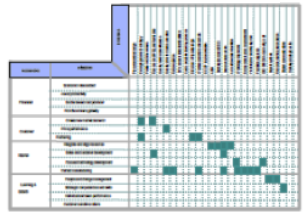
Estrategia de Ciberseguridad

ESTRATEGIA	ENFOQUE	SEGUIMIENTO	ACCIÓN
PLANEACIÓN ESTRATÉGICA • MIVIVA, Entorno, Tendencias, Riesgos, Objetivos	Mapa Estratégico  • Representación visual de la estrategia	Balanced Scorecard/ Metas  • Medición del cumplimiento de la estrategia y definición del nivel de mejora esperado	Iniciativas  • Programas de acción claves para alcanzar los objetivos

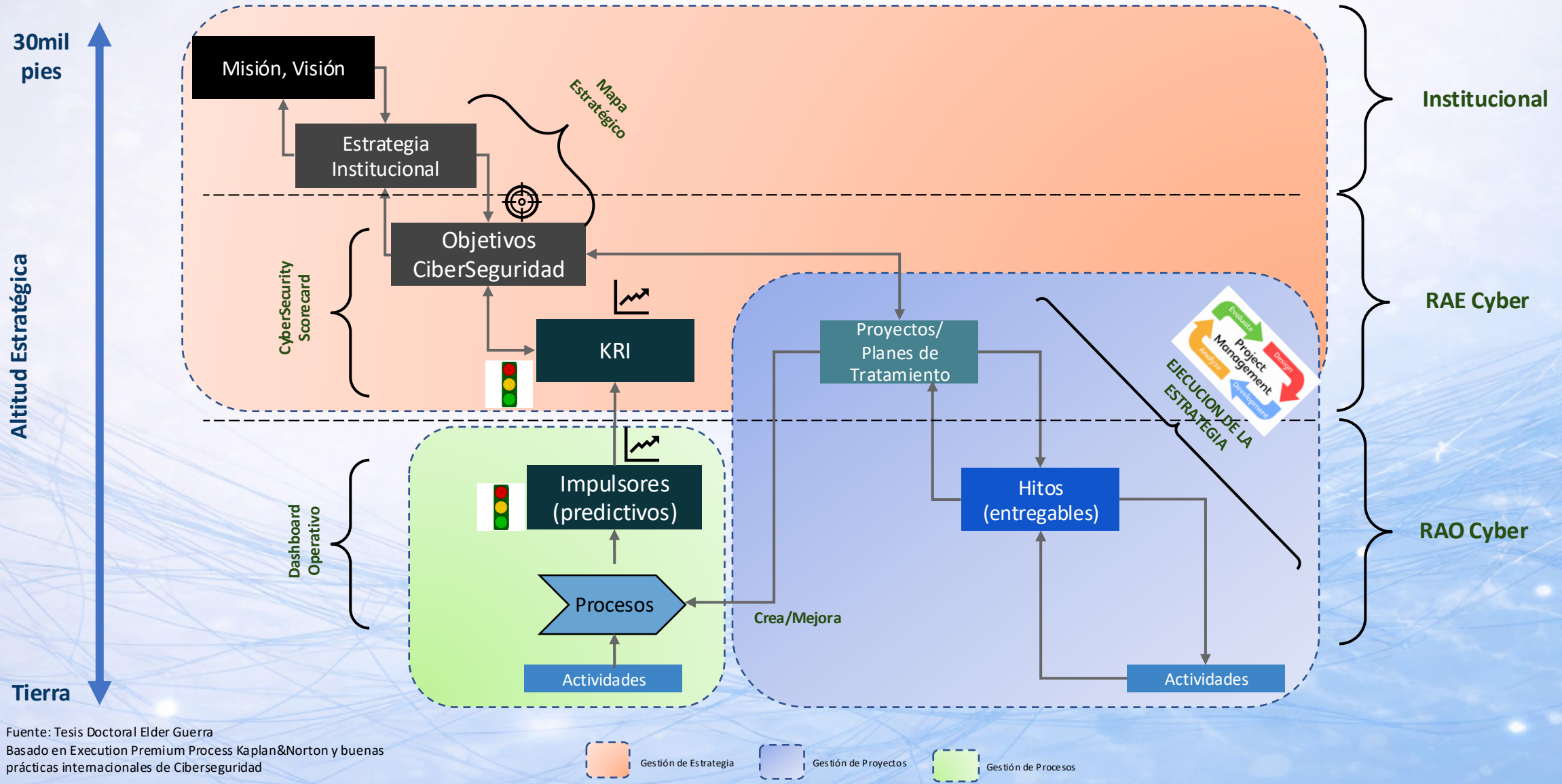
Estrategia del Negocio

Alineación

Estrategia de Ciberseguridad

ENFOQUE	SEGUIMIENTO	ACCIÓN
Mapa Estratégico  Objetivos	Scorecard  • Medición del cumplimiento de la estrategia y definición del nivel de mejora esperado	Proyecto/Plan  • Programas de acción claves para alcanzar los objetivos

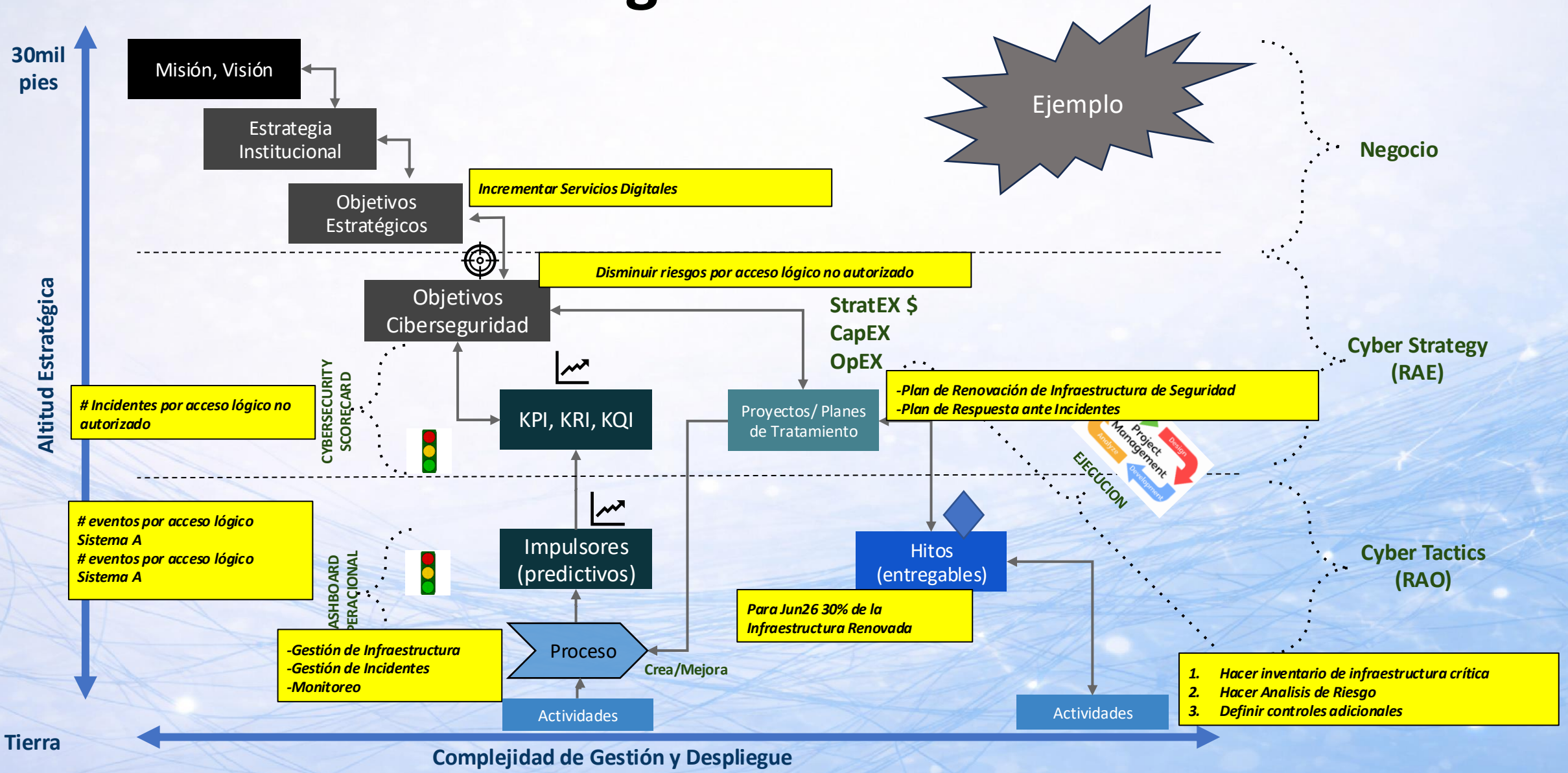
De la Estrategia a la Táctica en Ciberseguridad



Fuente: Tesis Doctoral Elder Guerra
Basado en Execution Premium Process Kaplan&Norton y buenas prácticas internacionales de Ciberseguridad

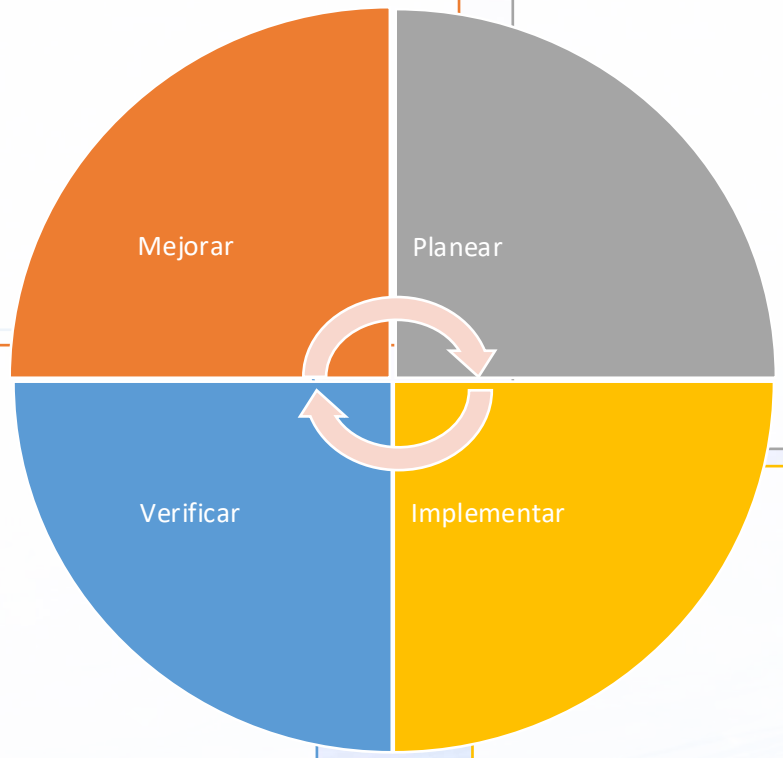
VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA
CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

De la Estrategia a la Táctica en Ciberseguridad



Sistema de Gestión – Estrategia Cyber

- Formular la Estrategia de Ciberseguridad alineada a la Estrategia Institucional y su contexto
- Cybersecurity Strategy Map
- Cybersecurity Scorecard
- Cybersecurity Portfolio
- Cybersecurity StratEX
- Políticas, Procedimientos, Registros
- Análisis & Tratamiento de Riesgos
- Roles, Responsabilidades, Autoridad

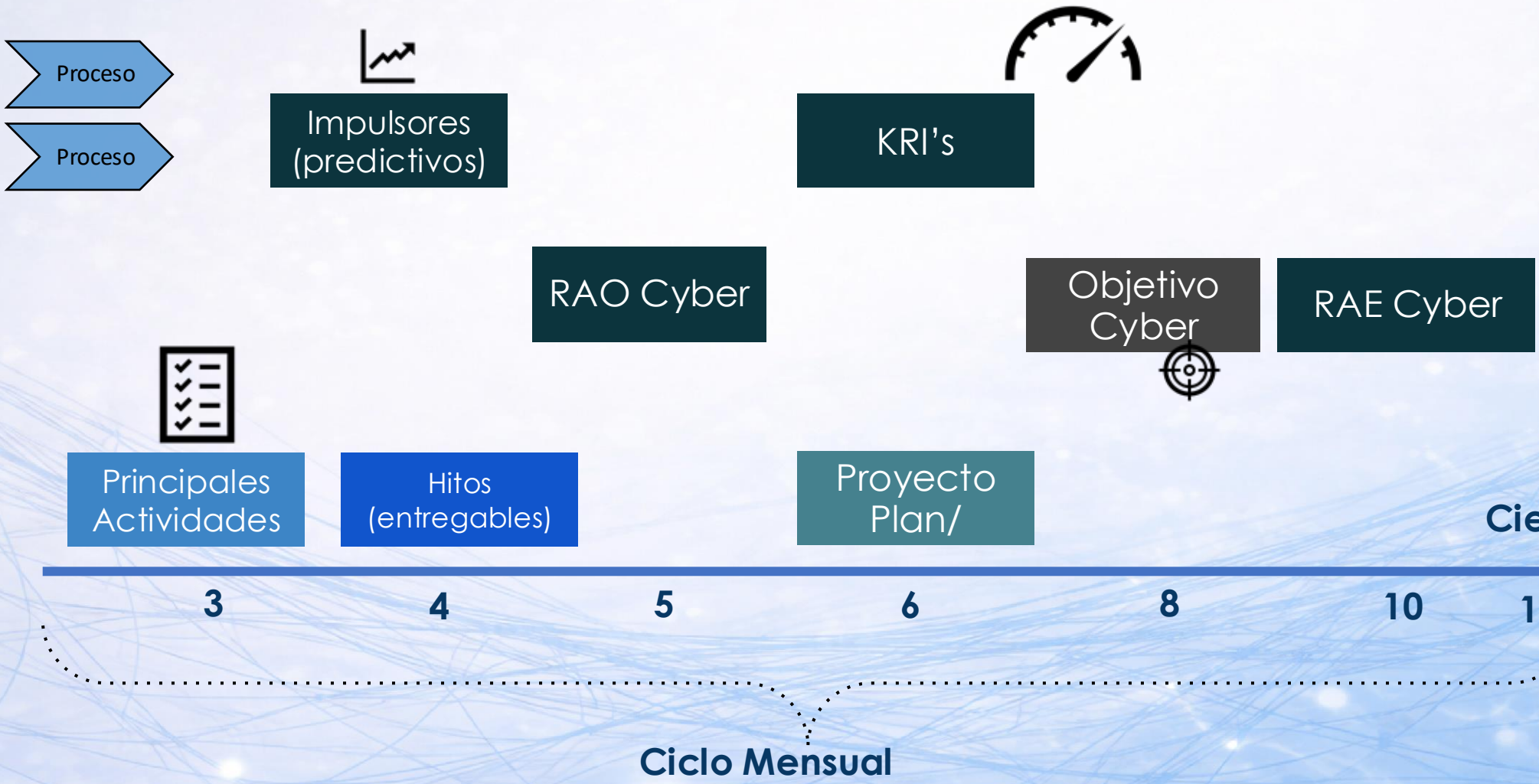


- Implementar el Portafolio de Proyectos Estratégicos y Planes de Tratamiento
- Implementar Controles
- Ejecutar Cyber CApEX, OpEX

- Reuniones de Análisis Operativo (RAO Cyber)
- Reuniones de Análisis Estratégico (RAE Cyber)
- Analisis de Datos, Auditorías Internas y Externas, Revisiones por Dirección

- Implementar Acciones Correctivas
- Implementar Acciones de Mejora

Rendición de Cuentas – Ciclo mensual - ejemplo



Flujo de Información Reporte/Seguimiento/Mejora de la Estrategia

NOTA: Para cada elemento debe reportarse con evidencia (foto, lista de asistencia, video, etc –media-)

Integrar la Estrategia de IA a la Estrategia Institucional

-Perspectiva Ejecutiva-

ISO/IEC 42001:2023

INTERNATIONAL STANDARD

ISO/IEC 42001

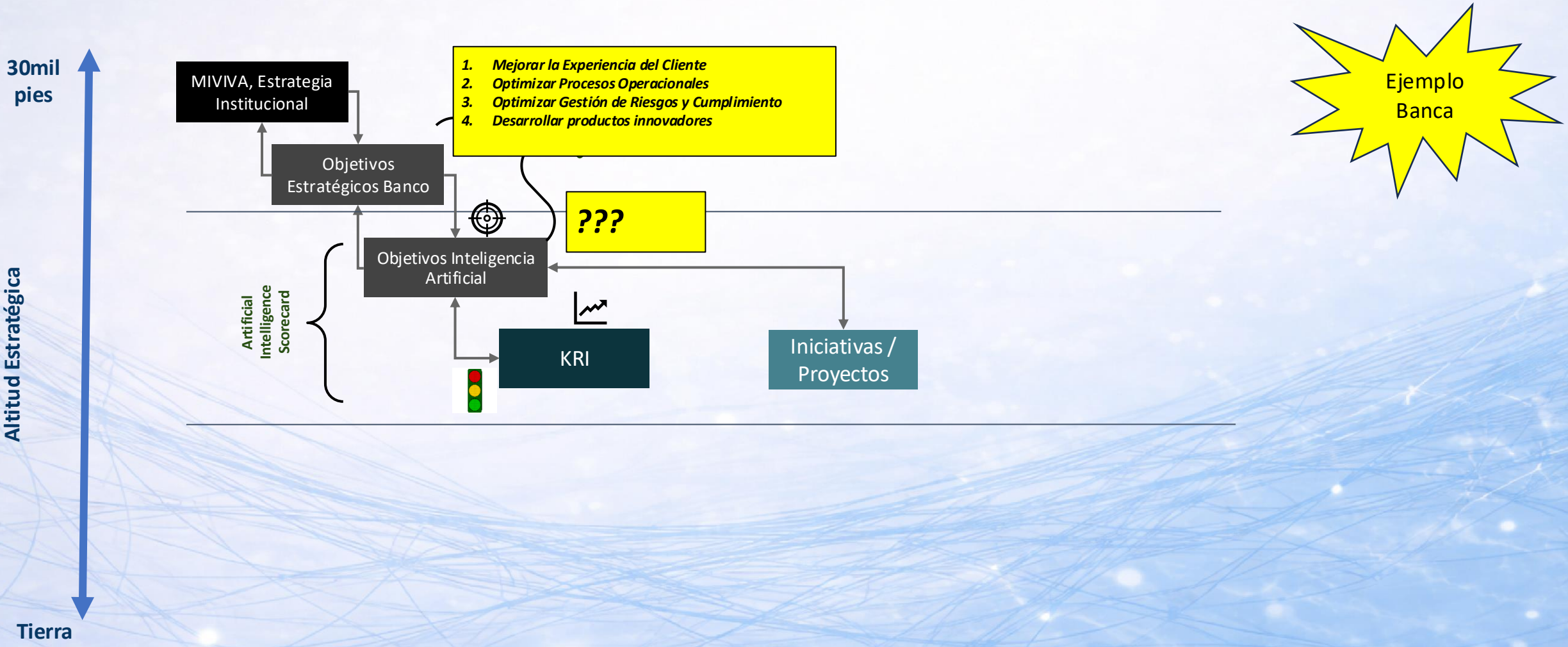
First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Contents

De la Estrategia a la Táctica en IA – ISO/IEC 42001



Fuente: Tesis Doctoral Elder Guerra
Basado en Execution Premium Process Kaplan&Norton y buenas prácticas internacionales de Ciberseguridad, Continuidad, IA

Objetivos Estratégicos relacionados a IA – Banca

Mejora de la Experiencia del Cliente

- **Objetivo de IA:** Implementar un sistema de recomendación personalizado utilizando aprendizaje automático para ofrecer productos y servicios financieros adaptados a las necesidades y comportamientos de cada cliente.
- **Resultado**: Mejorar la satisfacción y lealtad del cliente al proporcionar ofertas personalizadas

- **Objetivo de IA:** Desarrollar e integrar asistentes virtuales y chatbots basados en IA para ofrecer soporte al cliente 24/7.
- **Resultado**: Aumentar la disponibilidad y calidad del servicio al cliente, mejorando la experiencia del cliente.

2. Optimización de Procesos Operacionales

- **Objetivo de IA:** Automatizar el proceso de revisión y aprobación de solicitudes de préstamos mediante modelos de IA que evalúen el riesgo crediticio en tiempo real.
- **Resultado:** Reducir el tiempo de procesamiento y los costos operativos, mejorando la eficiencia.

- **Objetivo de IA**: Implementar sistemas de detección de fraudes basados en IA para monitorear y analizar transacciones en tiempo real.
- **Resultado:** Incrementar la seguridad y reducir las pérdidas por fraude, optimizando la operación bancaria

Ejemplo Banca

Objetivos Estratégicos relacionados a IA – Banca

3. Gestión de Riesgos y Cumplimiento

- **Objetivo de IA:** Utilizar análisis predictivo para identificar y gestionar riesgos financieros potenciales antes de que ocurran.
- **Resultado**: Mejorar la toma de decisiones en cuanto a inversiones y préstamos, mitigando riesgos financieros

- **Objetivo de IA:** Desarrollar sistemas de monitoreo continúo basados en IA para asegurar el cumplimiento de las normativas financieras
- **Resultado**: Reducir el riesgo de sanciones y multas, asegurando que el banco cumpla con las regulaciones aplicables

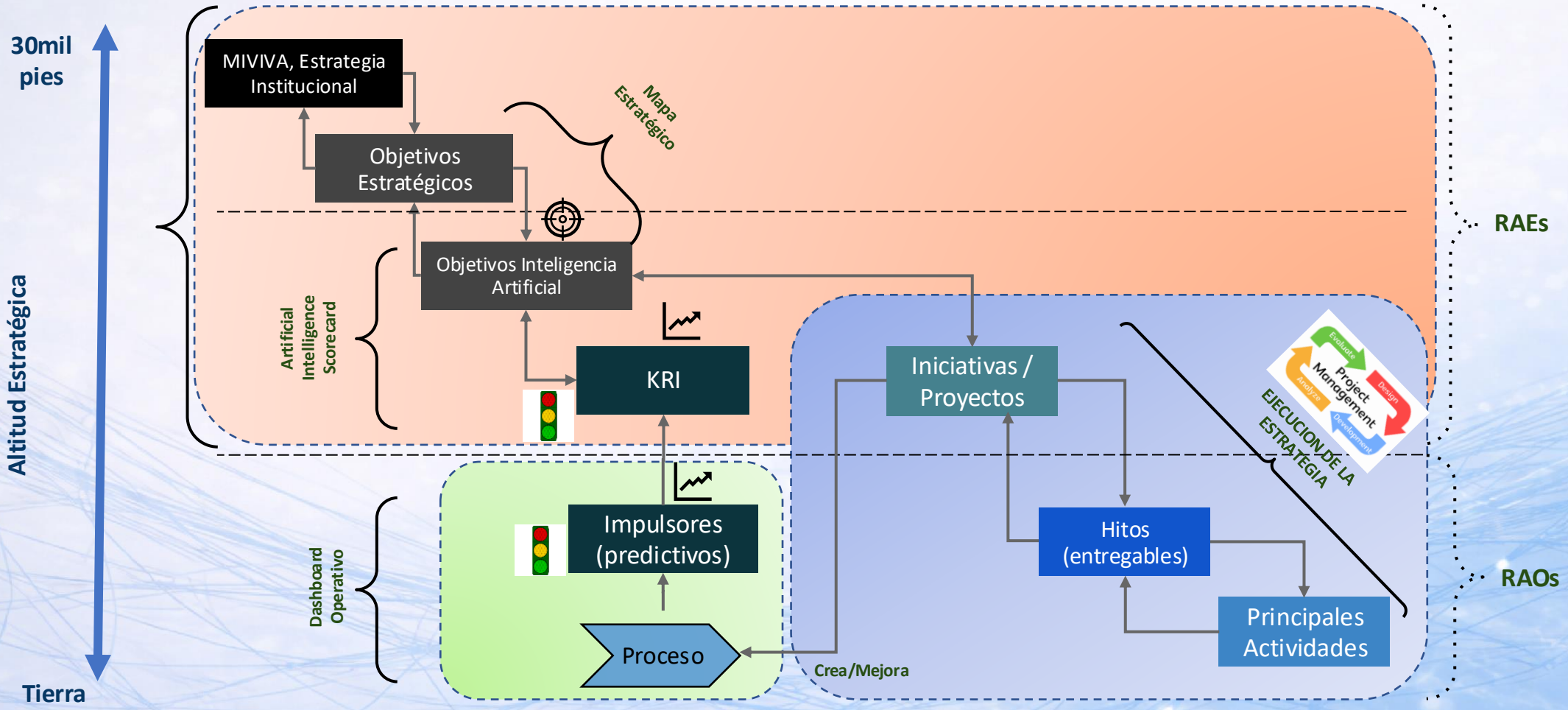
4. Desarrollo de Productos Innovadores

- **Objetivo de IA:** Crear un sistema de recomendación de inversiones automatizado (robo-advisor) que ofrezca asesoría personalizada basada en datos de mercado y perfil del cliente.
- **Resultado**: Productos financieros innovadores y personalizados, aumentando la competitividad del banco

- **Objetivo de IA:** Desarrollar productos financieros basados en análisis de datos, como seguros dinámicos que ajustan las primas en función del comportamiento del cliente.
- **Resultado**: Innovación en productos financieros, atrayendo a nuevos clientes y reteniendo a los existentes

Ejemplo Banca

De la Estrategia a la Táctica en IA – ISO/IEC 42001

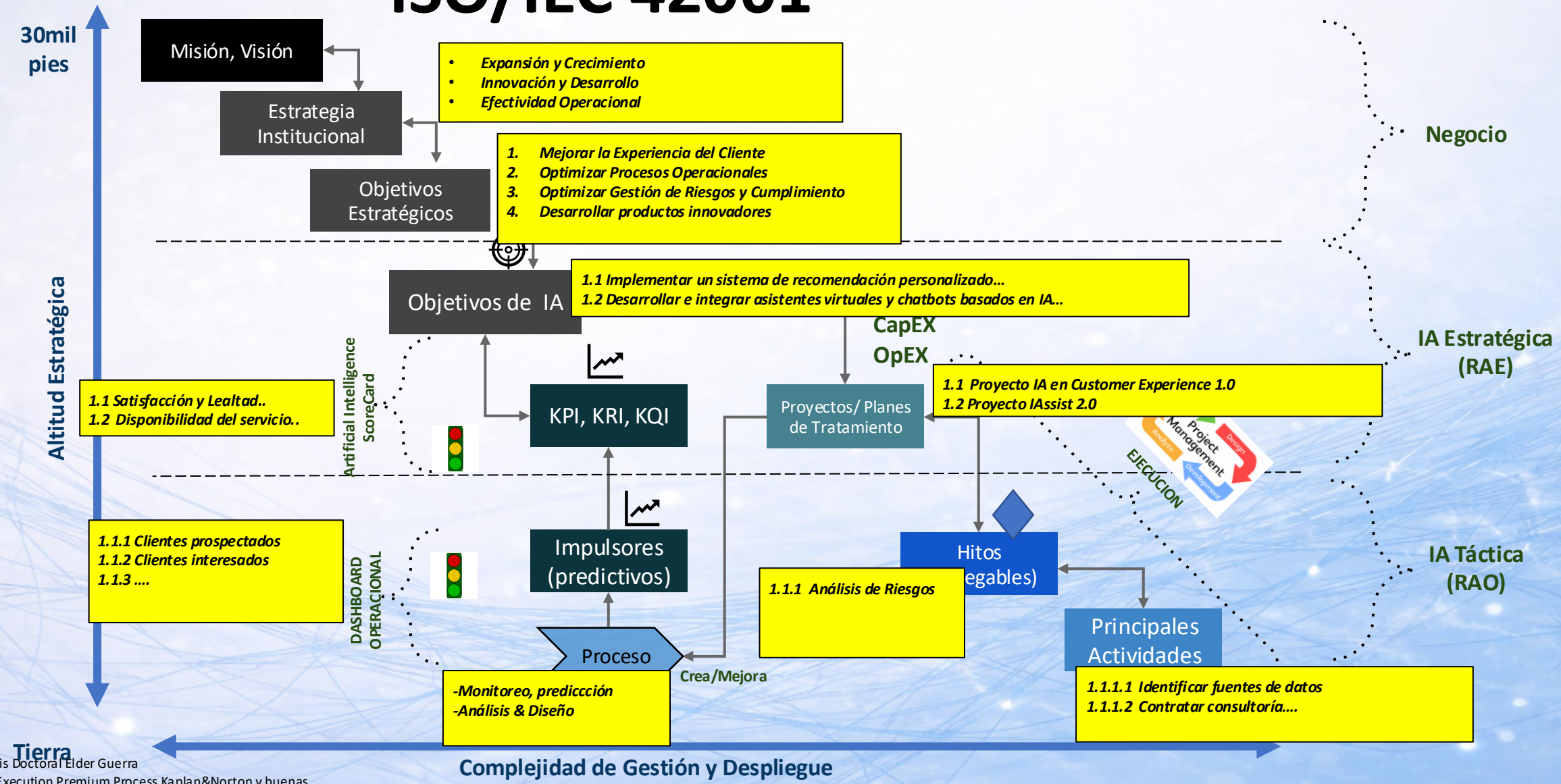


Fuente: Tesis Doctoral Elder Guerra
Basado en Execution Premium Process Kaplan&Norton y buenas prácticas internacionales de Ciberseguridad, Continuidad, IA

Gestión de Estrategia
Gestión de Proyectos
Gestión de Procesos

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA
CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

De la Estrategia a la Táctica en IA – ISO/IEC 42001



Fuente: Tesis Doctoral Elder Guerra
Basado en Execution Premium Process Kaplan&Norton y buenas prácticas internacionales de Ciberseguridad, Continuidad, IA

Estrategias de Ciberseguridad + IA
De la Visión a la Acción

-Perspectiva Ejecutiva-

Elder Guerra

Co-Founder & Consulting Services Director

ES Consulting

+502 5978 2846

eguerra@es.consulting

www.es.consulting

www.linkedin.com/in/elder-guerra-villagran/

www.facebook.com/estrategiayseguridad

Gracias¡