Marco Integral de Madurez para la Respuesta de Ciberincidentes Nacionales

Mesa 3 sobre Ciberresiliencia y Gestión de Riesgos

Jornadas de Investigación “Ciberseguridad y resiliencia digital en tiempos contemporáneos”, 10-12 noviembre 2025/PROSIC-UCR

JMF JORGE MORA FLORES

Jorge Mora-Flores

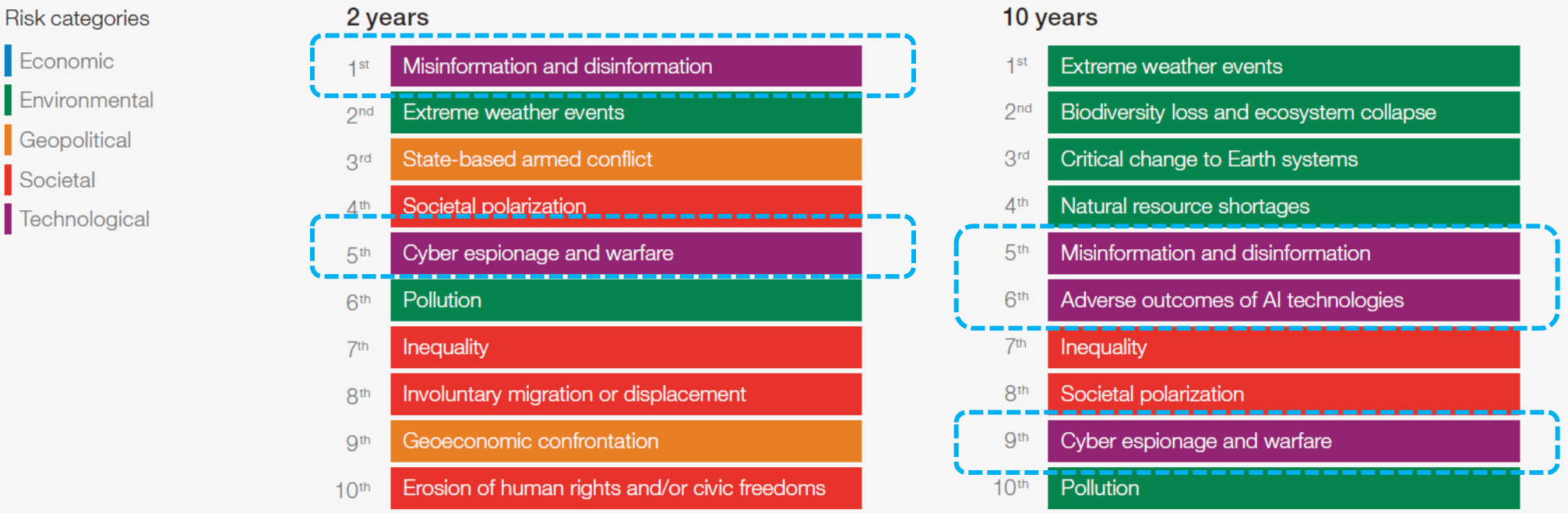
- Ingeniero en Computación, Máster en Innovación para el Desarrollo y Máster en Ciberseguridad.
- Candidato a la Especialización en Ciberseguridad Industrial.
- Consultor en Ciberseguridad y Desarrollo Digital en el **Banco Mundial** y el **Banco Interamericano de Desarrollo (BID)**.
- Parte del pool de expertos de **EU Cybernet**, **LAC4,** del proyecto **EU-LAC Digital Alliance** y la **OEA|CICTE**.
- Consultor en Ciberseguridad y Transformación Digital.
- LATAM Account Manager de **DeepSeas**.
- Ex director de Gobernanza Digital de Costa Rica.
- Coordinó a nivel técnico la atención del ciberataque nacional de Costa Rica sufrido en abril 2022 con su equipo del CSIRT-CR.

Complejidad de la ciberseguridad

Fuentes:

- World Economic Forum. (2025). Global cybersecurity outlook 2025. WEF.

Riesgos globales por severidad



Source

World Economic Forum Global Risks Perception Survey 2024-2025.

Ransomware


continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion/KrJjyE75_For_Costa_Rica
"FOR COSTA RICA"
https://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr
It takes about 2-3 days to download the rest of the information, after that if they don't get in touch with us, we will proceed to the next part, you po
orly understand your country is one big botnet
We want to say once again: we work exclusively for $$$. We do not pursue other goals
It takes about 2-3 days to download the rest of the information, after that if they don't get in touch with us, we will proceed to the next part, you poorly understand your country is one big botnet We want to say once again: we work exclusively for $$$. We do not pursue other goals
PUBLISHED 84%
4/28/2022
22299
52 [661.28 GB]
/ ROOT
(mtss desaf)2021.rar
1.94 GB
2.zip
252.40 MB
2022.rar
42.94 MB

Costa Rica: El despertar nacional

Abril 17

Primer ataque detectado - El comienzo del ciberataque nacional

$125M

Pérdidas en las primeras 48 horas

Mayo 8

Estado de emergencia - Decisión sin precedentes

$38M

Pérdidas diarias reportadas por el sector de importación y exportación

Mayo 31

Segundo ataque - El sistema de salud colapsa

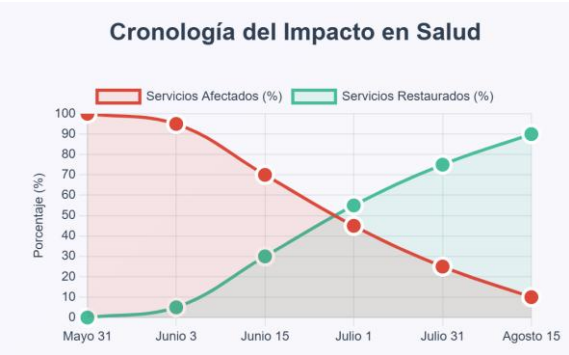
Noviembre

Recuperación para funcionar con normalidad, pero no completa - 7 meses después

$1.44B

Impacto Total

2.4% del PIB nacional
Equivalente al 50% del presupuesto anual de educación

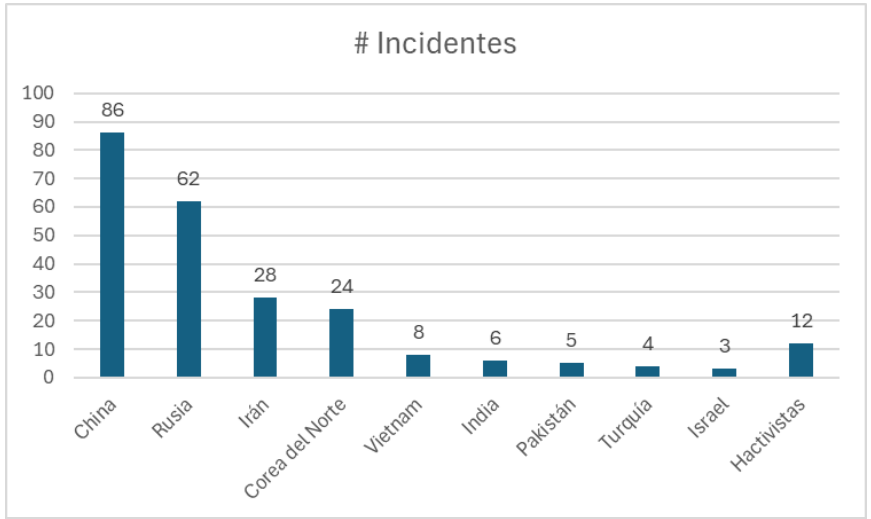


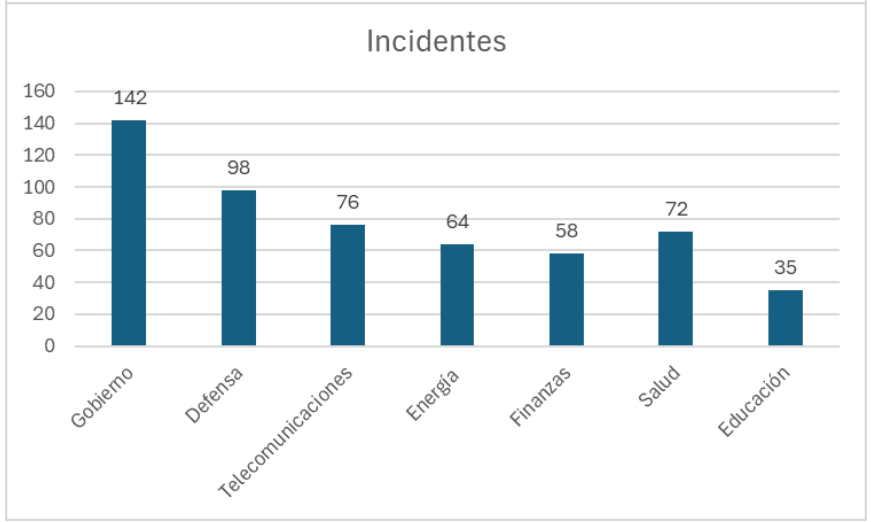
Fuentes:

- Vergara Cobos, E., Qiang, C. Z., & Straub, S. (2024). Economía de la ciberseguridad para los mercados emergentes. Banco Mundial.
- Mora-Flores, J. (2025). Presentación Cyber SBC 2025. NIMBUS-Cyber.

Ciberincidentes Globales

De 25 incidentes (2006-2010) a 142 incidentes (2021-2025)





CHINA 2024

+150%

Aumento ataques

ROBO CRIPTO

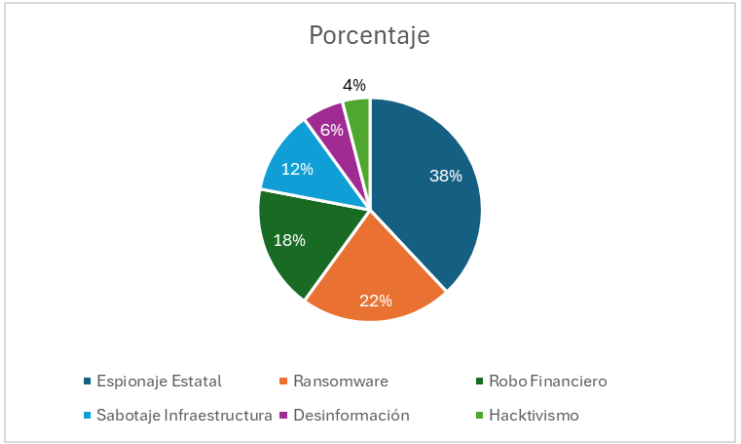
$1.5B

Corea Norte

SALT TYPHOON

20+

Países afectados



Latinoamérica: Incidentes Clave

2025 - Regional
- Malware chino detectado
- Operaciones USCYBERCOM

2023 - Costa Rica
- 12 servidores cifrados

2022 - Costa Rica
- Emergencia nacional
- $20M ransomware

2022 - México
- 6TB robados Defensa

2019 - Chile
- Red bancaria atacada

2018 - México
- $20M robados SWIFT

Fuente: Center for Strategic and International Studies (CSIS). (2025). Significant Cyber Incidents Since 2006. Washington, D.C.: CSIS.

Política pública en ciberseguridad

- "Una política pública de ciberseguridad es el **conjunto de estrategias**, **normas** y **acciones** coordinadas por el Estado para proteger el ciberespacio nacional y garantizar la seguridad digital de sus ciudadanos, instituciones y sectores clave.“
- (Basado en la lectura de UIT, 2021. National Cybersecurity Strategy Guide)
- Actores:
  - Gobierno
  - Sector privado
  - Academia
  - Ciudadanos

NIMBUS-Cyber

- NIMBUS (National Incident Maturity Baseline Unified System) es **una propuesta** de un marco integral de madurez específicamente diseñado para que los formuladores de políticas públicas (Policy Makers) puedan desarrollar, implementar y evaluar las capacidades nacionales de respuesta a ciberincidentes de manera sistemática y progresiva.

Dimensiones

Participación Democrática

Involucrar al ciudadano en las decisiones de ciberseguridad

Gobernanza Política

Estableciendo políticas y estrategias para la ciberseguridad

Dimensiones Transversales

Integrando la ciberseguridad en todas las áreas

Marco Legal

Creando leyes y regulaciones para la ciberseguridad

Coordinación Sectorial

Alineando esfuerzos entre diferentes sectores para la ciberseguridad

Capacidades Técnicas

Desarrollando habilidades y herramientas para la ciberseguridad

Modelo de Madurez (CMM)

5 **Liderazgo Adaptativo**

Liderar con flexibilidad y visión en un entorno global.

4 **Gestión Cuantitativa**

Utilizar datos y métricas para mejorar la toma de decisiones.

3 **Procesos Definidos**

Implementar procedimientos estandarizados para operaciones.

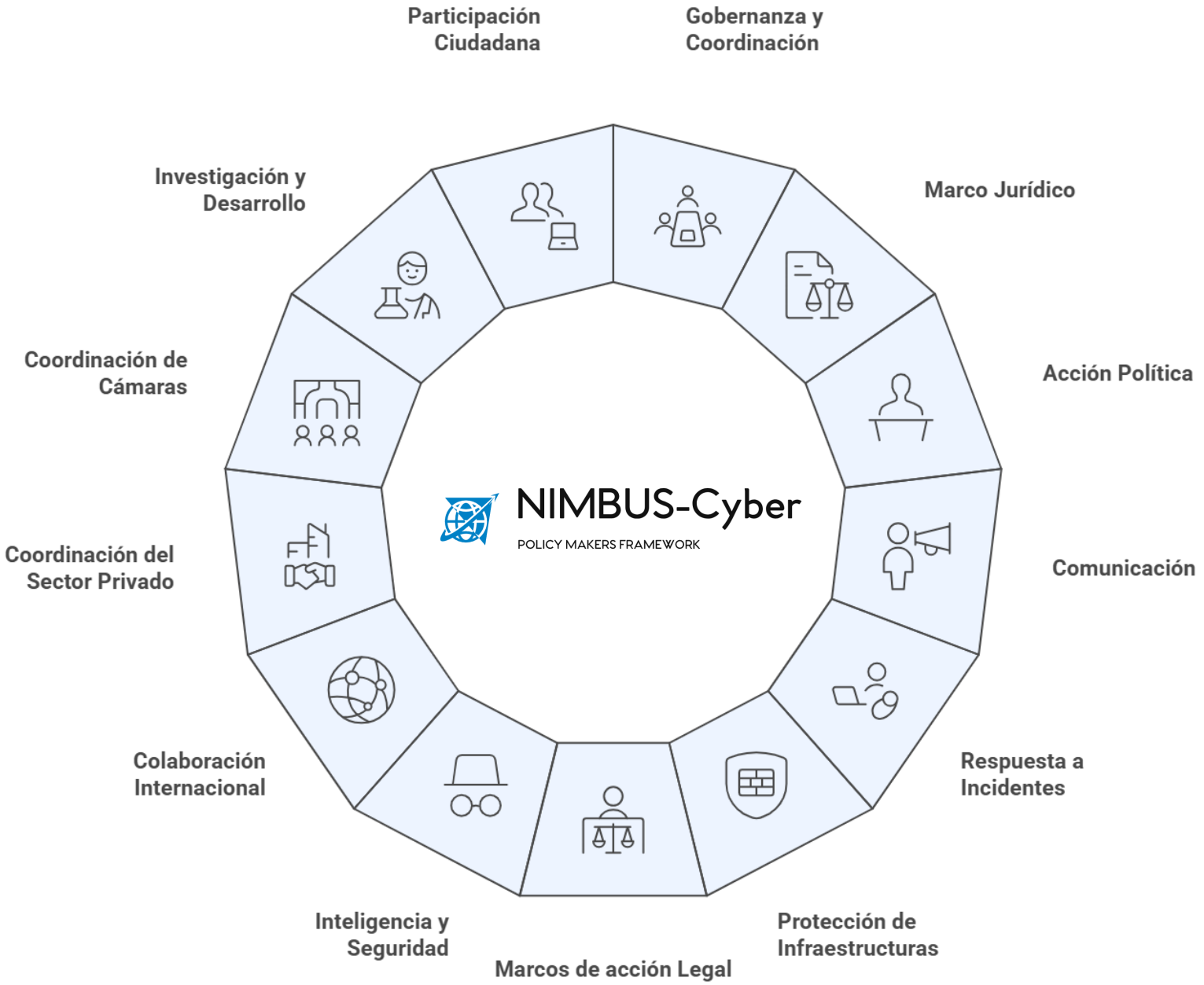
2 **Estructura Básica**

Establecer una organización fundamental y jerarquía.

1 **Respuesta Reactiva**

Abordar problemas a medida que surgen sin planificación proactiva.

Pilares


Participación Ciudadana
Gobernanza y Coordinación
Marco Jurídico
Acción Política
Comunicación
Respuesta a Incidentes
Protección de Infraestructuras
Marcos de acción Legal
Inteligencia y Seguridad
Colaboración Internacional
Coordinación del Sector Privado
Coordinación de Cámaras
Investigación y Desarrollo
NIMBUS-Cyber
POLICY MAKERS FRAMEWORK

1. Gobernanza y coordinación con el ecosistema

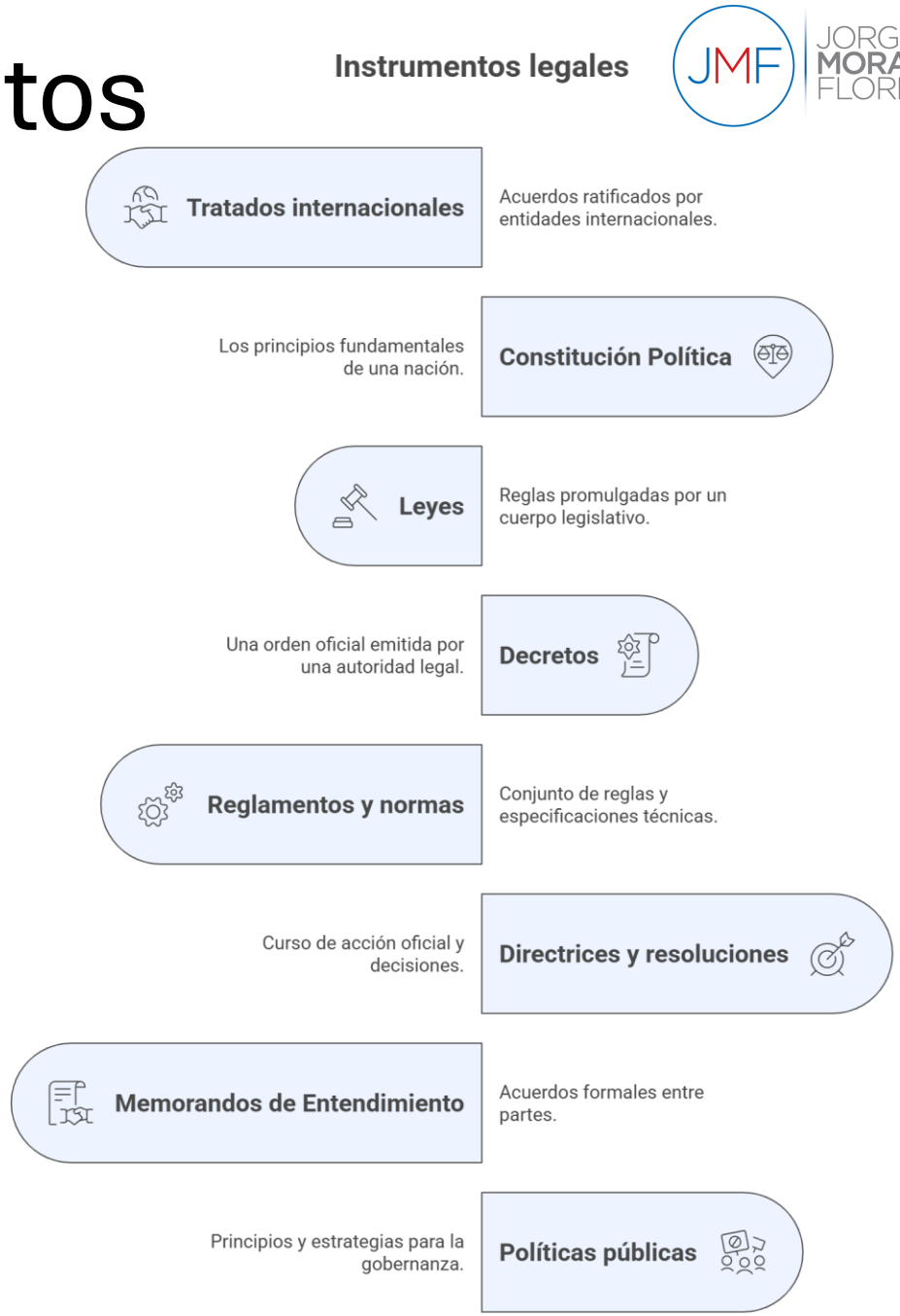
Propósito

Establecer estructuras de gobernanza efectivas que permitan la coordinación estratégica y operativa de todos los actores del ecosistema nacional de ciberseguridad.

2. Marco jurídico e instrumentos legales existentes

Propósito

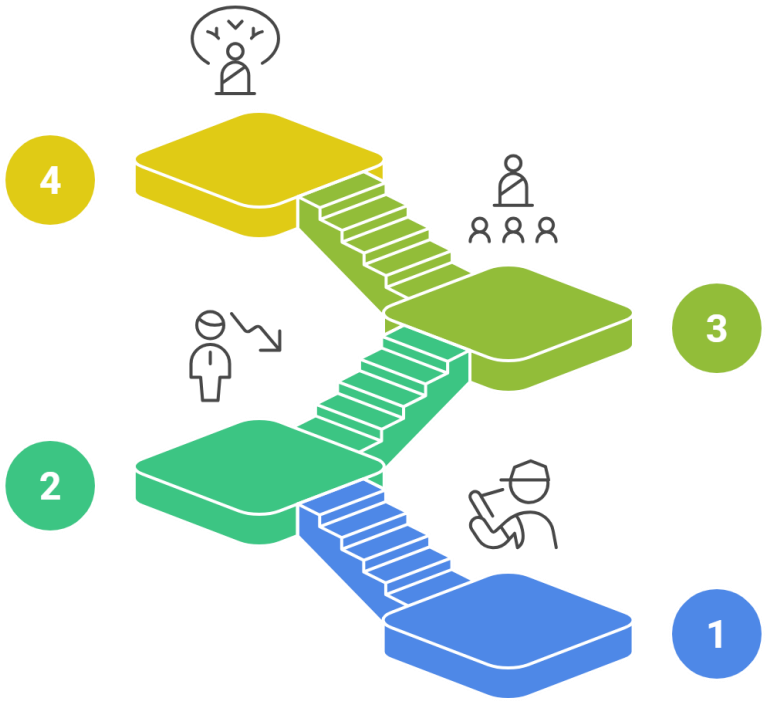
Desarrollar y utilizar marcos jurídicos robustos e instrumentos legales efectivos que habiliten y respalden todas las acciones de ciberseguridad nacional, incluyendo la planificación estratégica.



3. Acción política y coordinación institucional

Propósito

Asegurar el apoyo y liderazgo político al más alto nivel para la implementación efectiva de políticas de ciberseguridad nacional, especialmente para la coordinación interinstitucional durante ciberincidentes nacionales.



Crisis Nacional

El presidente lidera la respuesta a una crisis nacional.

4

Crisis Sectorial

Un ministro gestiona una crisis que afecta a un sector.

2

3

Crisis Mayor

Un consejo coordina la respuesta a una crisis mayor.

1

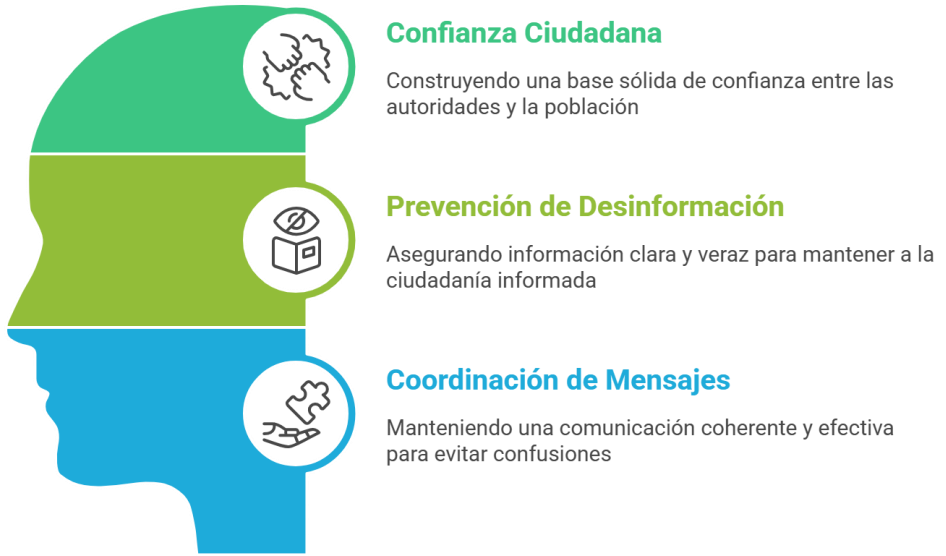
Incidente Menor

Un equipo técnico aborda un problema menor (SOC + CERT/CSIRT Nacional).

4. Comunicación gestionada y coordinada

Propósito

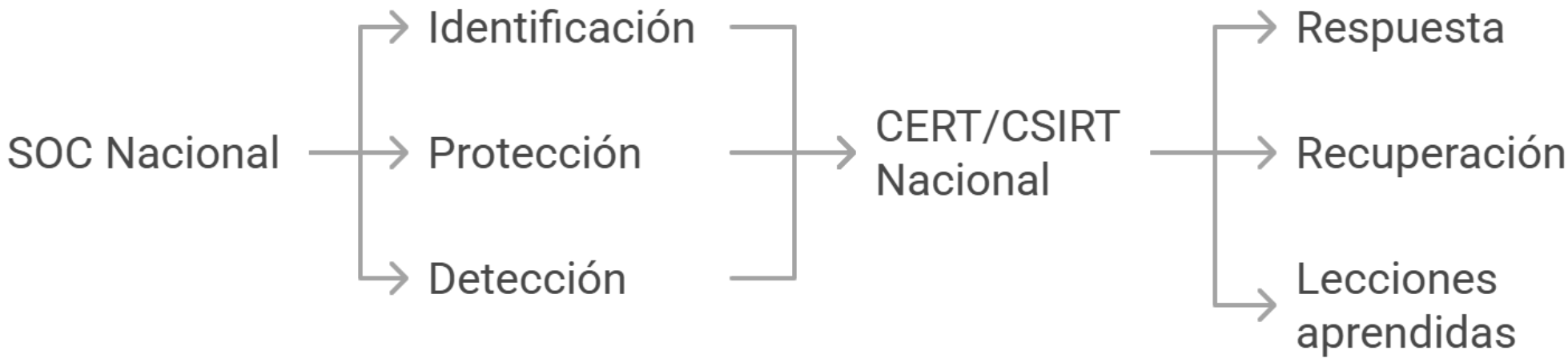
Establecer capacidades de comunicación estratégica y coordinada para gestionar la información pública durante ciberincidentes, mantener la confianza ciudadana y coordinar mensajes institucionales.



5. Coordinación técnica y respuesta al incidente

Propósito

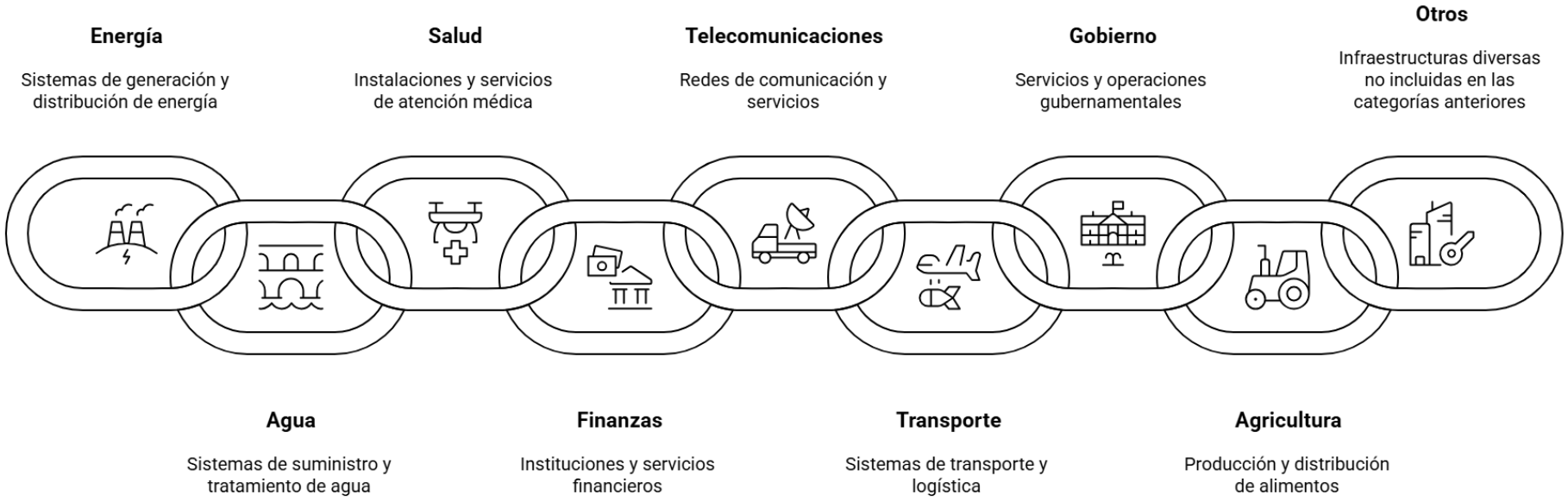
Desarrollar y mantener capacidades técnicas centrales de respuesta a ciberincidentes a través de un SOC y CERT/CSIRT Nacional maduro, validado y bien coordinado internacionalmente.



6. Protección de infraestructuras críticas y servicios esenciales

Propósito

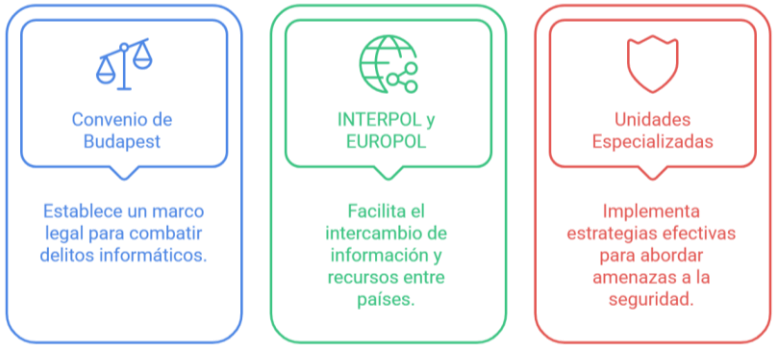
Desarrollar capacidades especializadas para proteger las infraestructuras que son esenciales para el funcionamiento de la sociedad y la economía nacional.



7. Marcos y acciones legales

Propósito

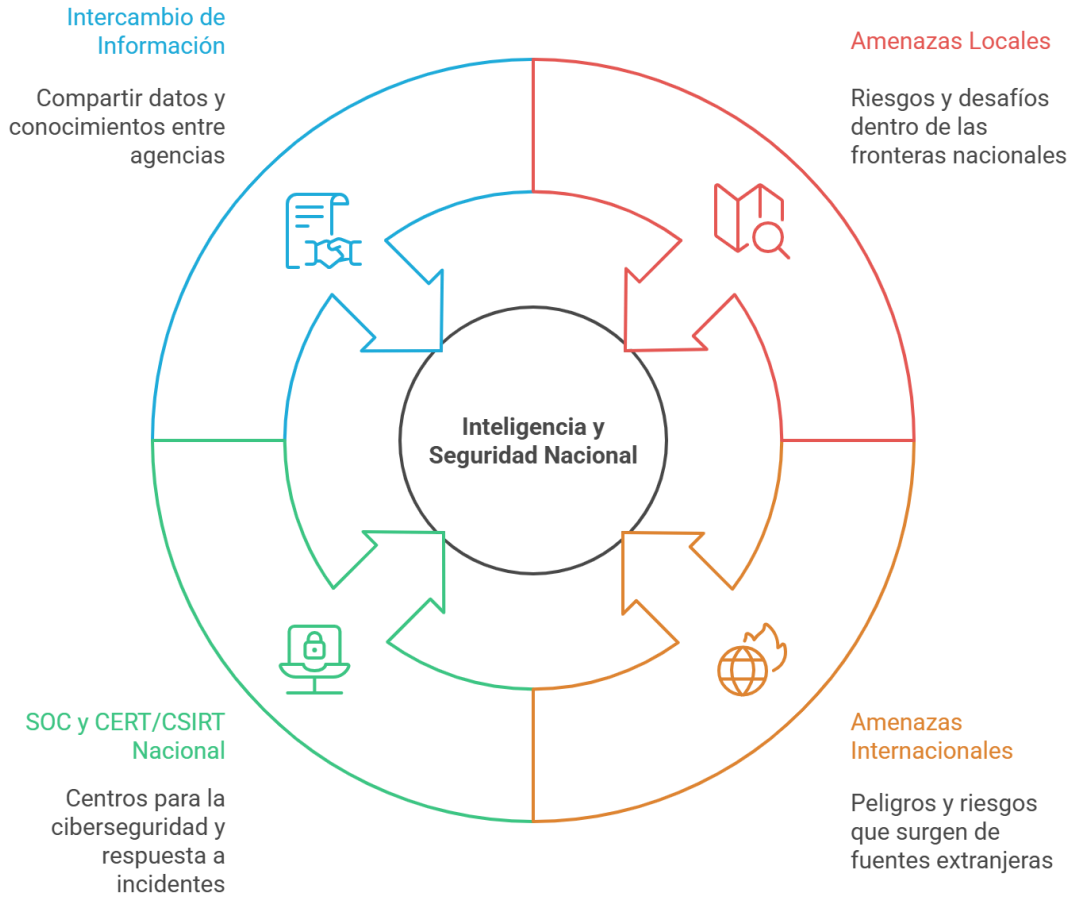
Desarrollar capacidades de coordinación efectiva entre autoridades de ciberseguridad, sistema judicial y fuerzas del orden para la investigación y persecución del cibercrimen, **respetando la separación de poderes**.



8. Inteligencia y Seguridad Nacional

Propósito

Integrar capacidades de inteligencia cibernética con la arquitectura de seguridad nacional para detectar, analizar y responder a amenazas cibernéticas de actores estatales y no estatales sofisticados.

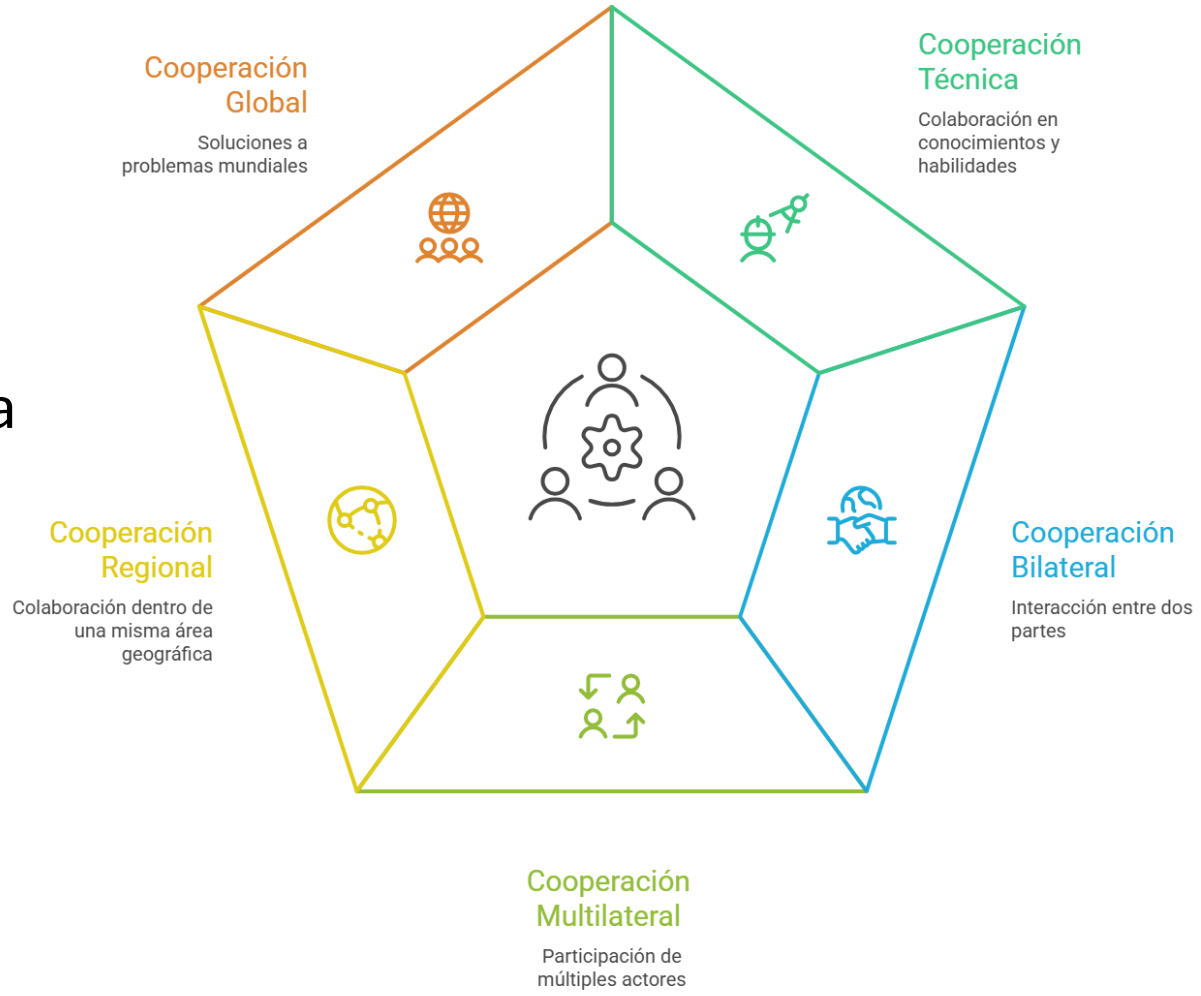


9. Colaboración internacional

Propósito

Desarrollar capacidades robustas de cooperación internacional en ciberseguridad para el intercambio de información, desarrollo conjunto de capacidades y respuesta coordinada a amenazas transfronterizas.

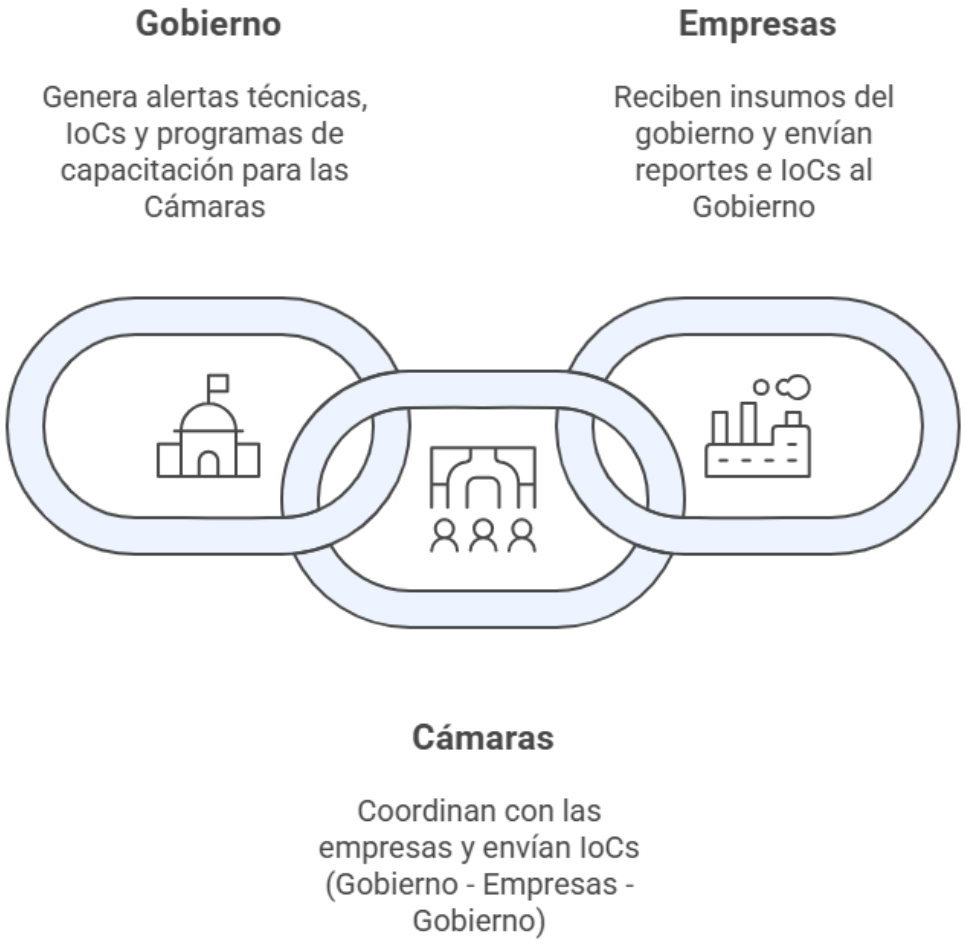
- **Ejemplos**
  - FIRST
  - CSIRT Americas (OEA/CICTE)
  - ENISA
  - OTAN
  - Red Gealc



10. Coordinación con el sector privado y productivo

Propósito

Establecer mecanismos efectivos de coordinación con el sector privado general y productivo para proteger la economía nacional y facilitar intercambio de información sobre amenazas que afectan la competitividad económica.



11. Coordinación con cámaras sectoriales claves

Propósito

Desarrollar coordinación especializada con sectores tecnológicos críticos que tienen capacidades únicas para la ciberseguridad nacional, incluyendo telecomunicaciones, TIC, financiero y clústeres especializados.

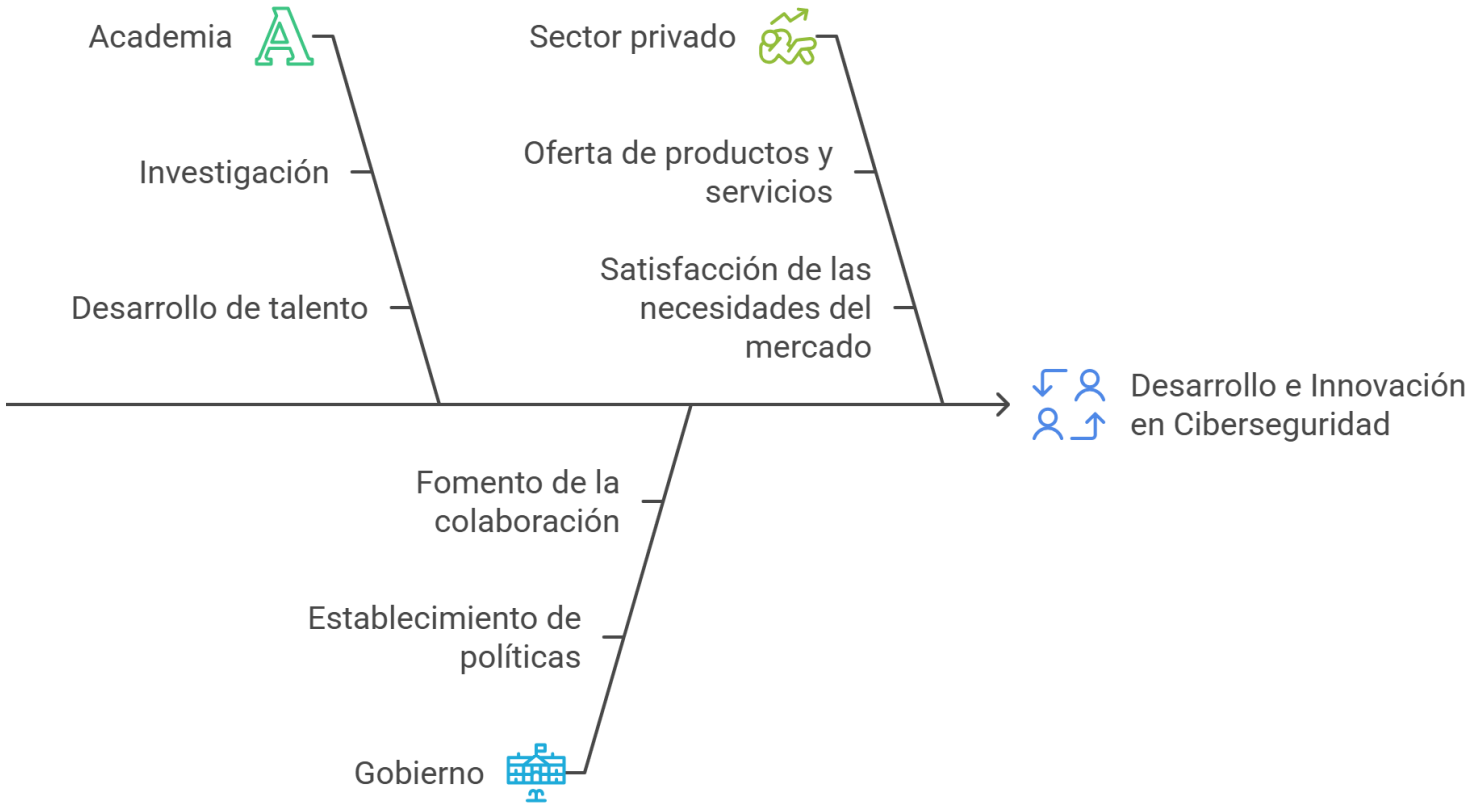
12. Investigación, desarrollo e innovación

Propósito

Desarrollar capacidades nacionales de investigación e innovación en ciberseguridad que contribuyan a la soberanía tecnológica, competitividad económica y liderazgo internacional.

Ejemplos

- Laboratorios forenses
- Centro Nacional de I+D+i
- Publicación de Papers conjuntos



13. Ciudadanía digital y participación ciudadana

Propósito

Desarrollar una ciudadanía digitalmente alfabetizada y participativa que contribuya activamente a la ciberseguridad nacional, incluyendo la protección y transparencia de procesos electorales democráticos.

Concientización

Educación

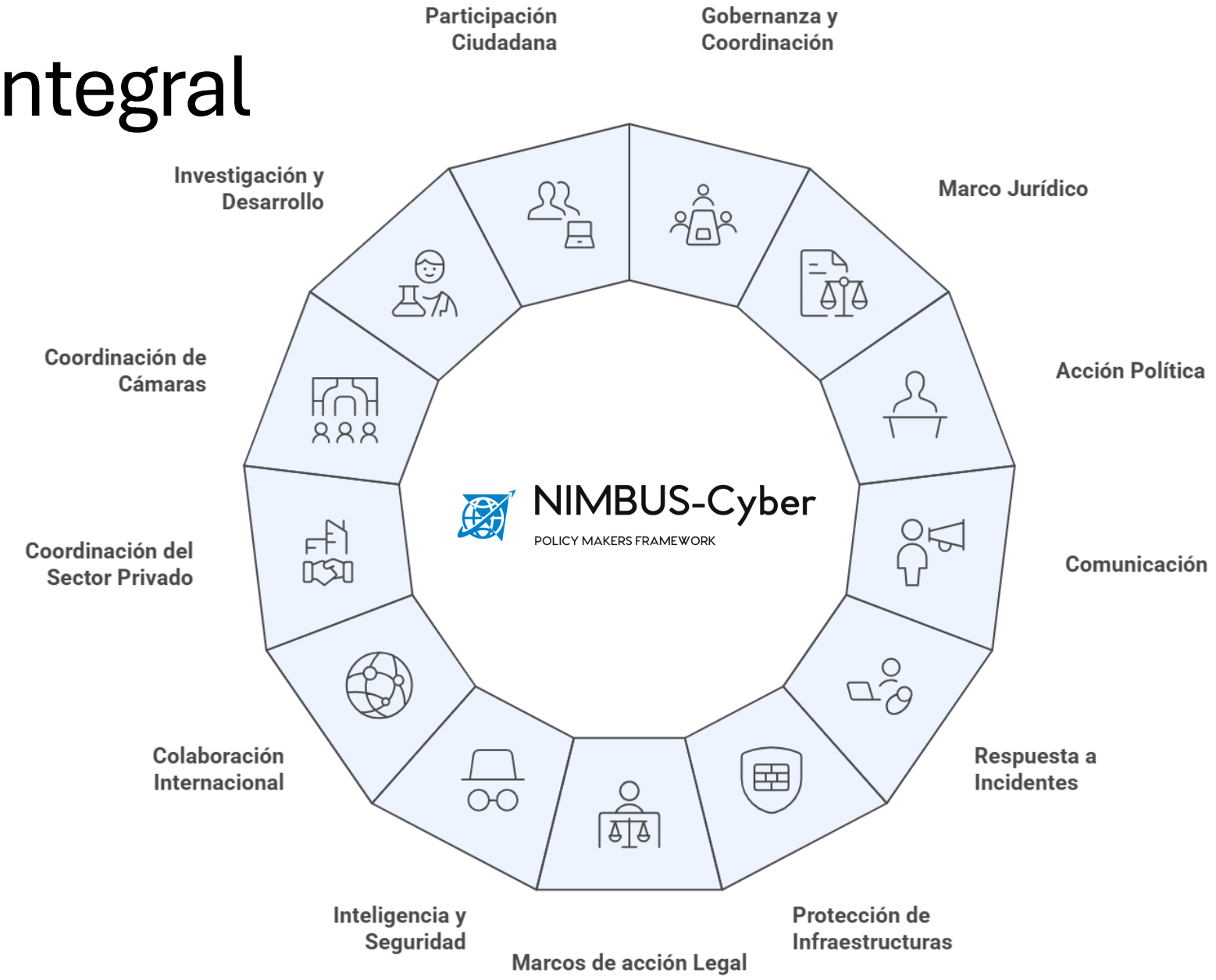
Participación

Voluntariado

Gobierno Abierto

Transparencia Electoral

Marco Integral



JMF | JORGE MORA FLORES

¡Gracias!

jorge@moraflores.com