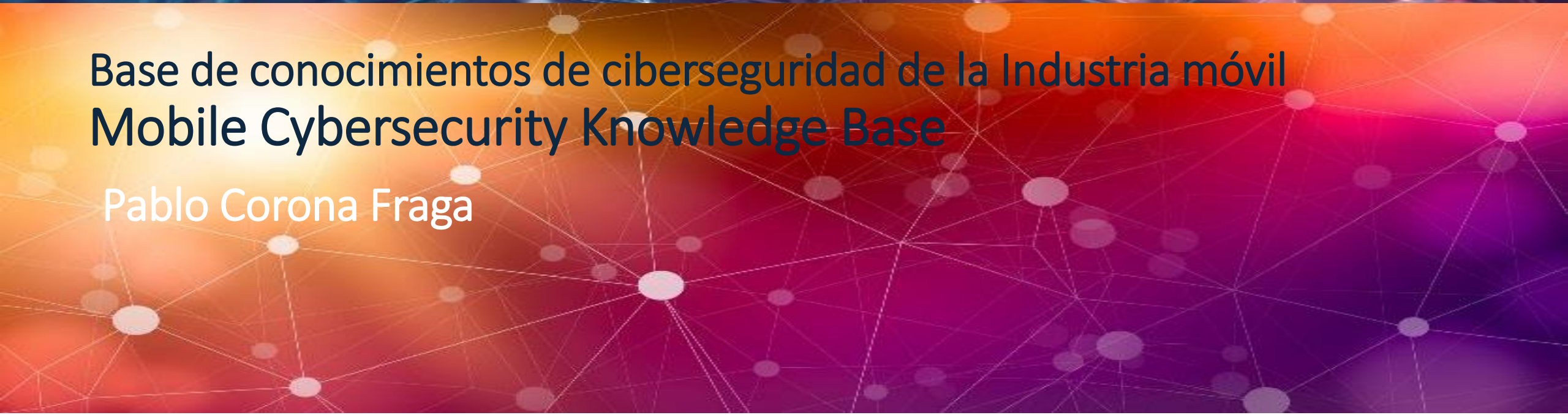




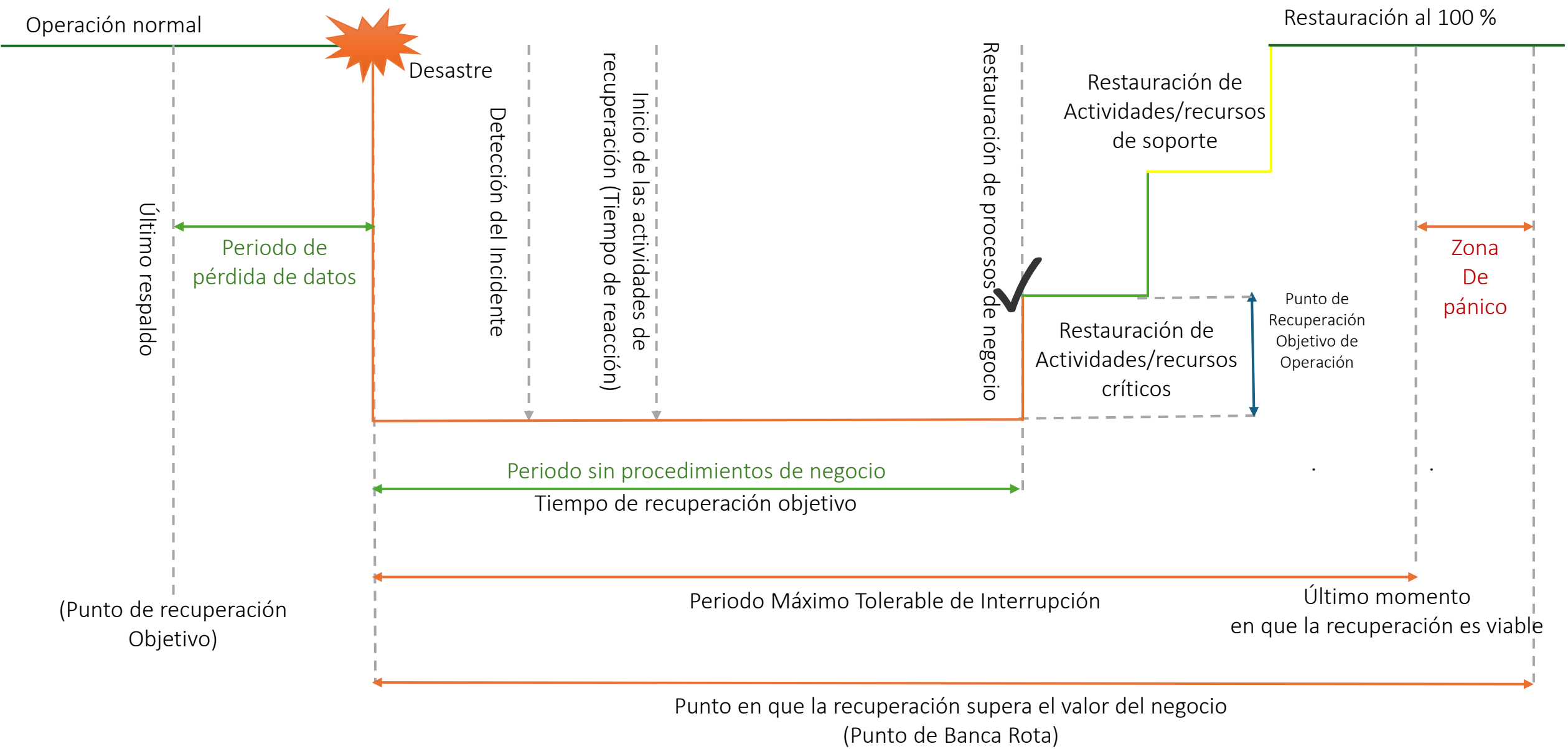
Mejores prácticas y resiliencia

Base de conocimientos de ciberseguridad de la Industria móvil
Mobile Cybersecurity Knowledge Base

Pablo Corona Fraga



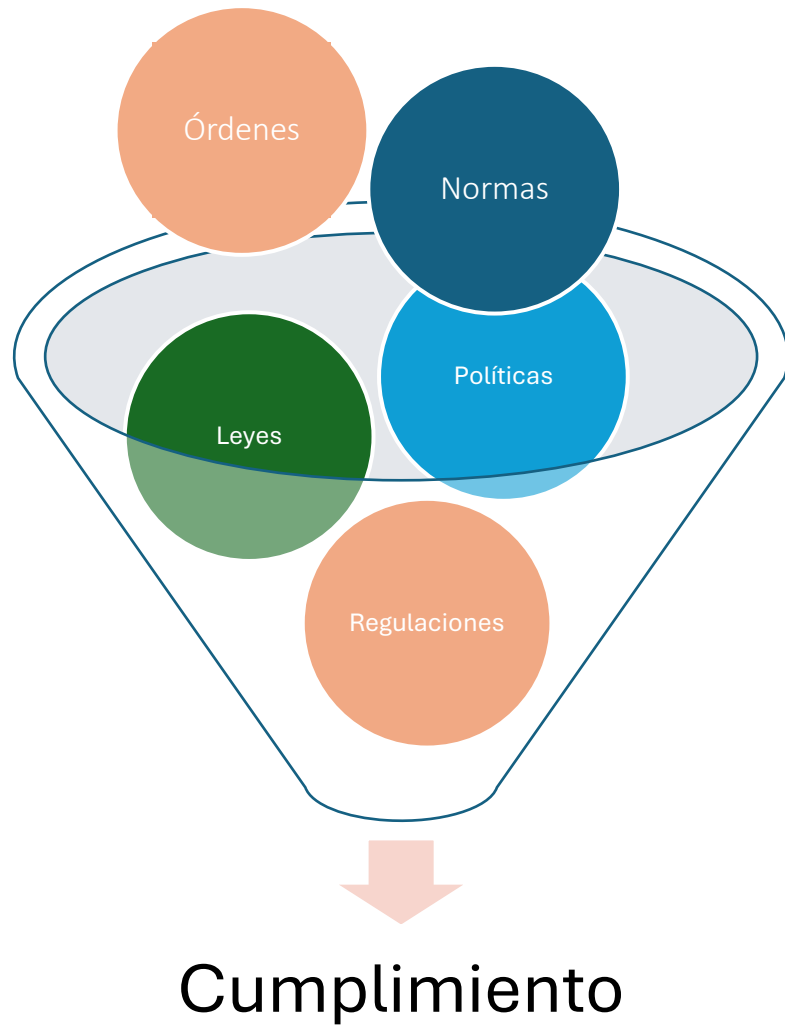
Resiliencia



Entidades globales y maduras

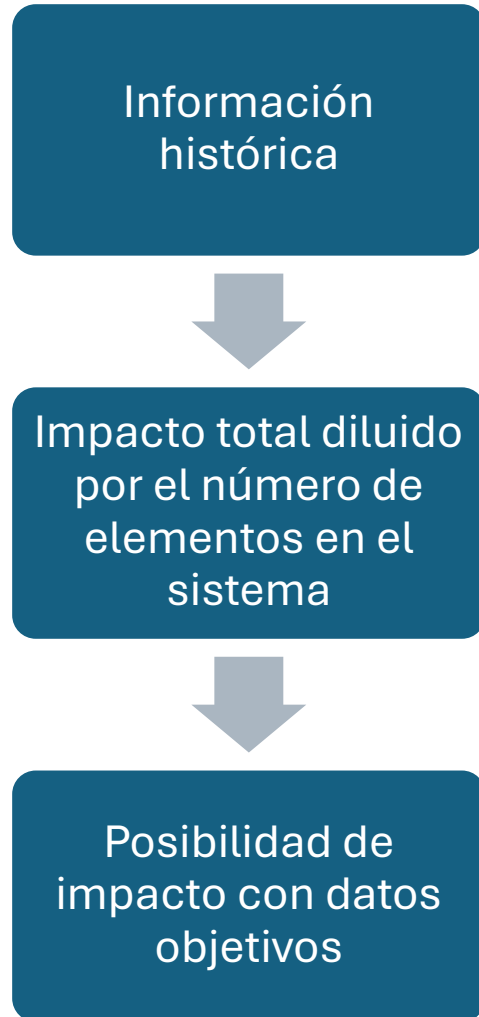


Armonizar elementos

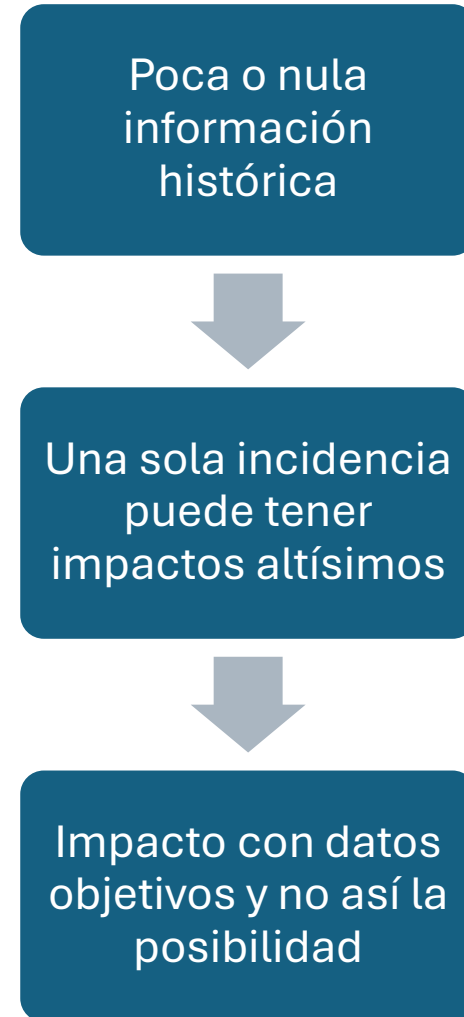


Tipos de riesgos

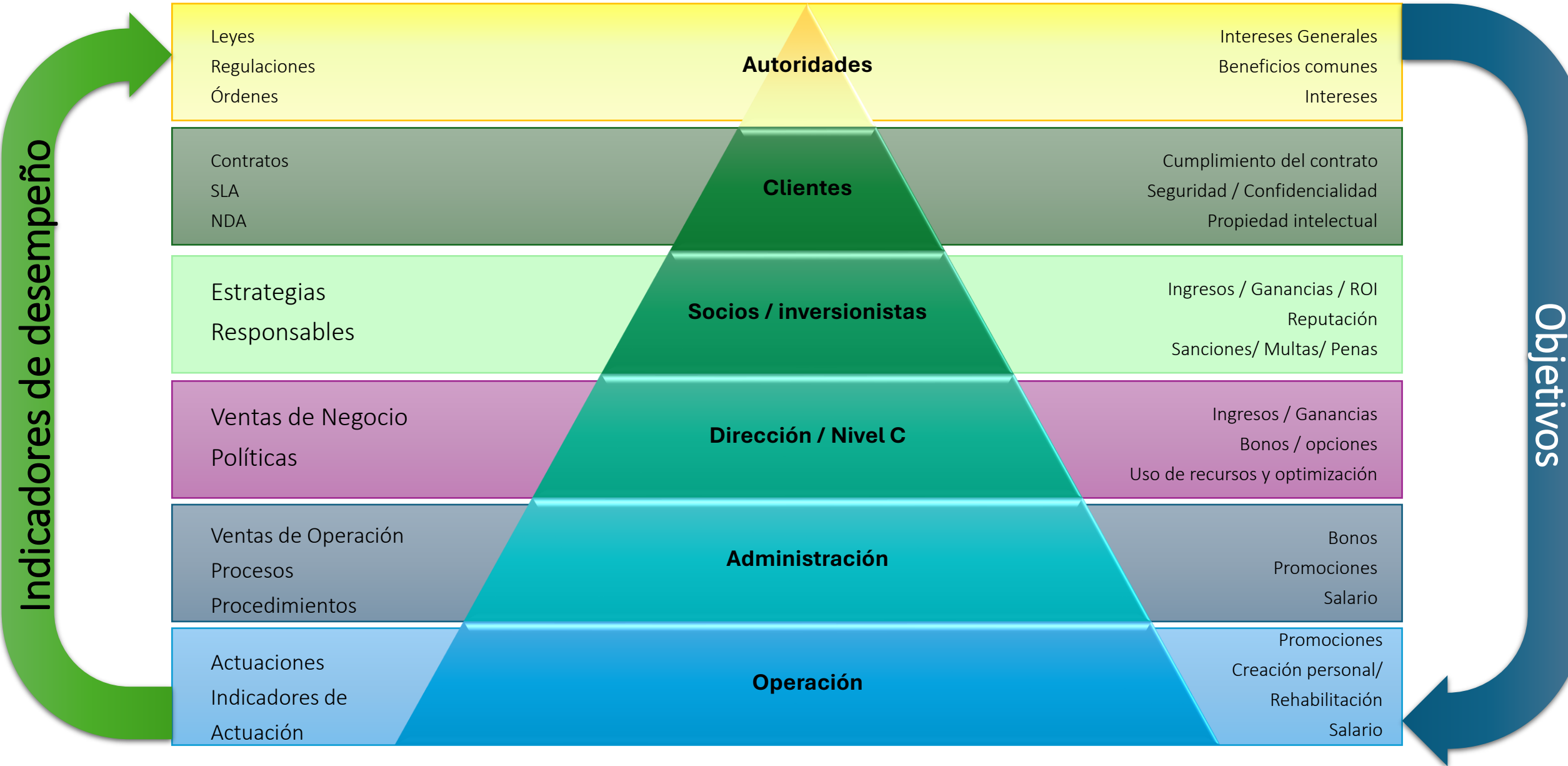
Promediables



No promediables



Estructura del Ecosistema con objetivos y KPIs



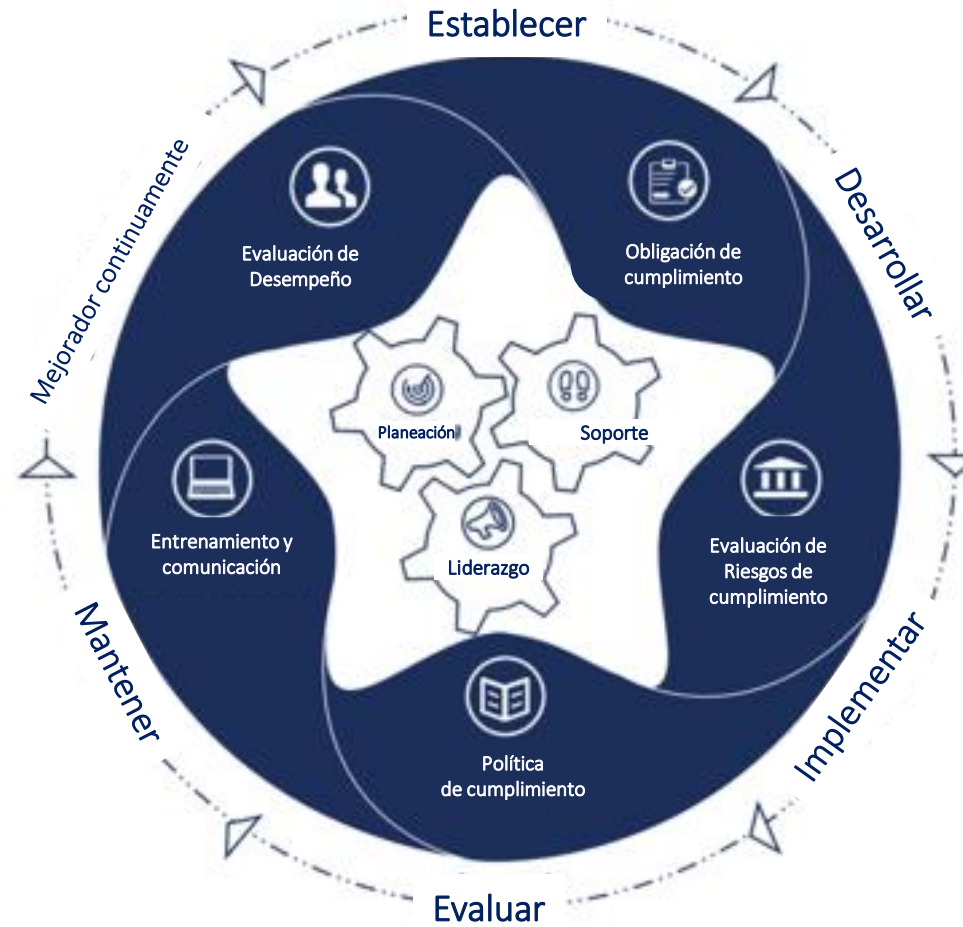
Impacto



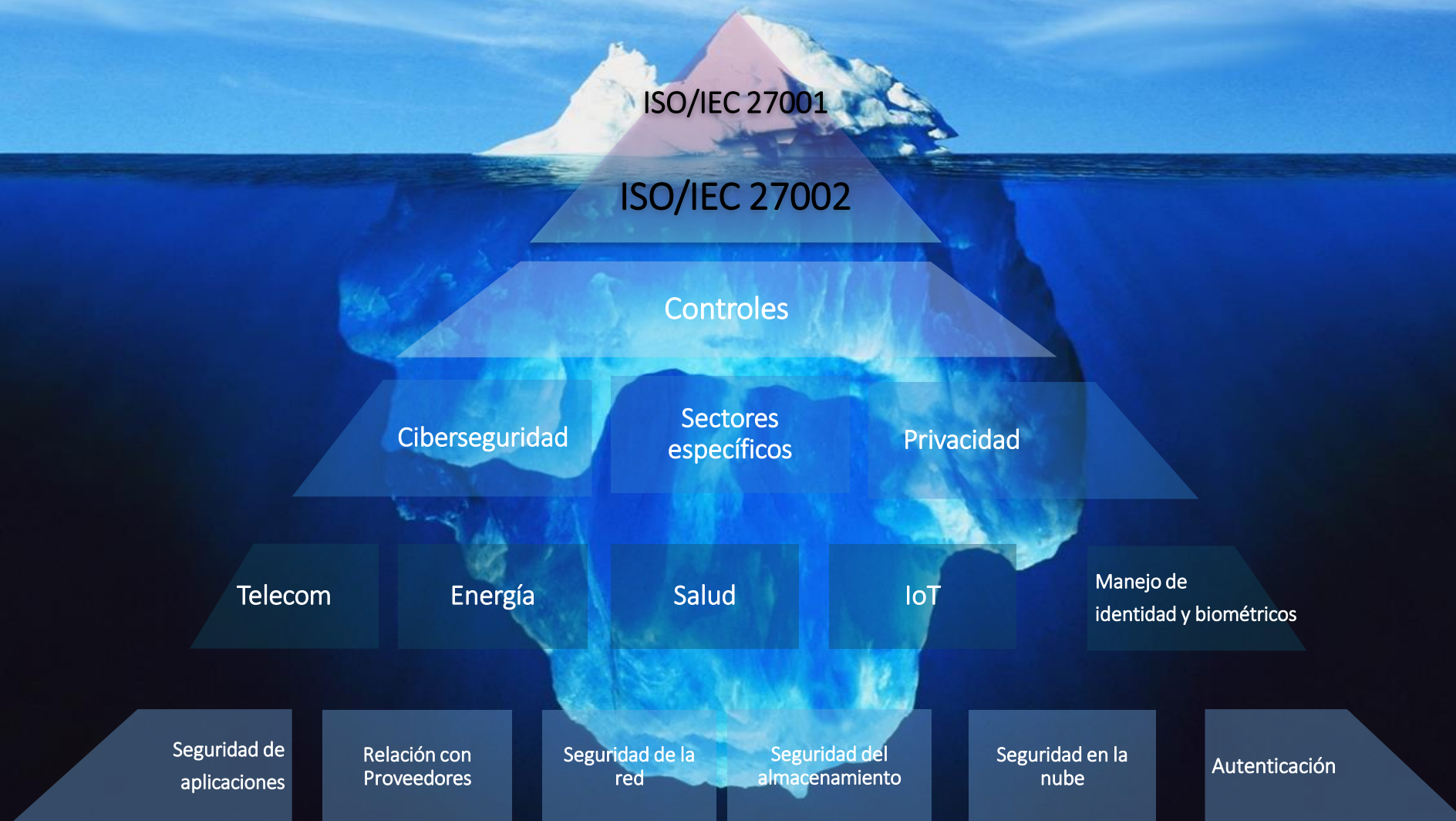
Gráfico 1. Beneficios para las empresas derivados de la adherencia a estándares internacionales de ciberseguridad. Elaboración propia.

Marcos de referencia para cumplimiento

Contexto de la Organización



Diferencia entre el Qué y el Cómo



¿Probabilidad? Posibilidad? Verosimilitud?

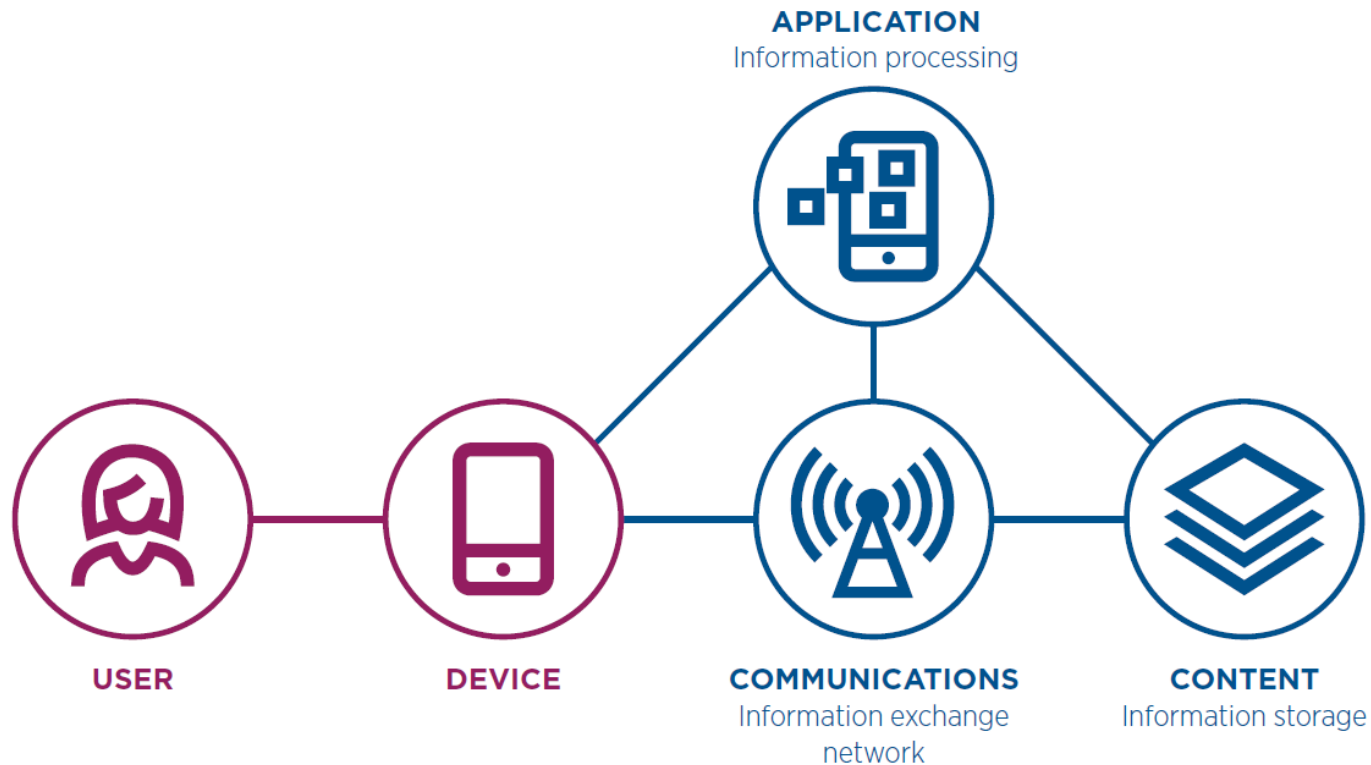
		Impacto				
		Despreciable	Marginal	Moderado	Crítico	Catastrófico
Verosimilitud	Certidumbre	5	6	7	8	9
	Probable	4	5	6	7	8
	Posible	3	4	5	6	7
	Improbable	2	3	4	5	6
	Excepcional	1	2	3	4	5

Verde: Aceptable
 Amarillo: Podría ser aceptable
 Naranja: Debe ser atendido, prioridad baja

Rojo: Debe ser atendido, prioridad alta
 Marrón: Debe ser atendido y prioridad muy alta
 Morado: Debe ser atendido, negocio en peligro inminente

Es una cadena de valor con muchas partes interesadas

MODULES IN A DIGITAL SERVICE

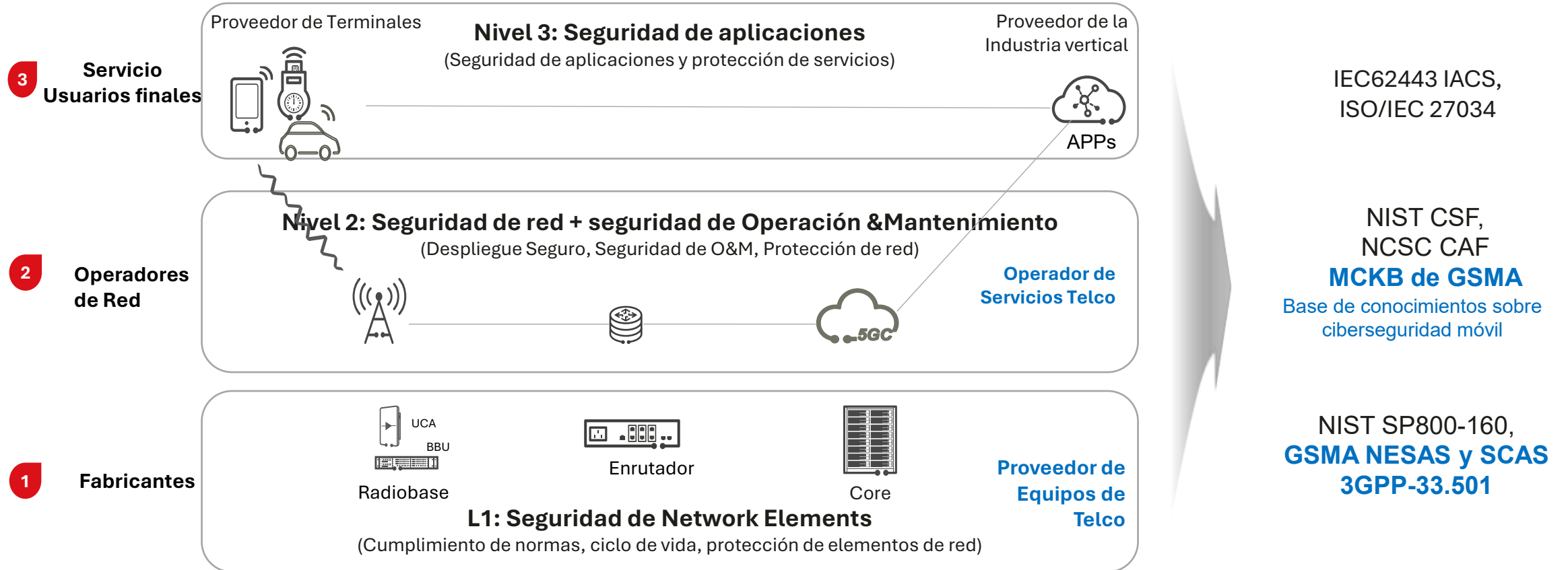


La ciberseguridad es una responsabilidad de todos los actores de la cadena de valor

Creación de resiliencia de seguridad

Promueve la co-construcción de la ciberseguridad móvil global.

Referencias de la Industria



El modelo de seguridad de 3 capas es ampliamente aceptado en la industria de las telecomunicaciones.

La seguridad requiere una "responsabilidad compartida" entre las partes interesadas.

Alcance de la base de conocimientos de ciberseguridad

- Librería de artículos para ayudar a los operadores a identificar y mitigar riesgos



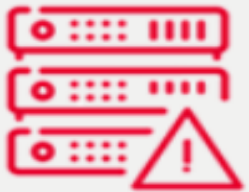
Gestión de Riesgos



**Seguridad del
Dispositivo**



Seguridad de red móvil



Seguridad de red IP



**Seguridad de
interconexión**

Alcance de la base de conocimientos de ciberseguridad

Seguridad de dispositivos 	SMS Blasters (FS.67) / Anti-Theft (FS.25)			IoT Security (FS.60)	
	Software Updates (FS.25) / Mobile Malware (SG.19)				
	(e)UICC Profiles (FS.27)		IMEI Security		
	Cryptographic Algorithms (FS.35)				

Seguridad de red móvil 	Voicemail Services (SG.20)				
	Voice Calling VoLTE (FS.22)				
	Exchange of Subscriber Credentials (FS.28) / Credentials Storage				
	Network Function Virtualization (FS.33) / Micro-segmentation (FS.61)				

Seguridad de Interconexión 	SIM Box Fraud (FS.01) / SMS Fraud (FF.09) / Binary SMS (FS.42)						
	SS7 (FS.07, FS.11, FS.52)		Diameter (FS.19)	GTP-C (FS.20)	GTP-U (FS.37)	5G (FS.36)	SIP (FS.38)
					Key Management (FS.34)		
	Interconnect Signalling (FS.21) / Interconnect Testing (FS.26)						

Gestión de riesgos			
MoTIF Framework (FS.57/FS.58)			
Controls Testing Methodology			
Baseline Controls (FS.31)			
5G Fraud (FS.39)		5G Security (FS.40)	
Fraud Manual (FF.21)		Security Manual (FS.30)	
Vulnerability Disclosure (FS.23)			
Post Quantum Crypto (PQ.1, PQ.2)			

Seguridad en red IP privada		
DNS Encryption (IG.10)		
IP Exchange Network (IR.34, IR.77)		

MCKB ayuda a identificar, mapear y mitigar

MCKB propone documentación relativa a:

Controles de seguridad de línea de base (FS.31); Controles de amenazas (FS. 30); y soluciones de seguridad clave (FS.34, FS.36, FS.35).

❑ Solución de seguridad móvil de extremo a extremo

- Planificación, construcción, mantenimiento, optimización y funcionamiento de la red del operador.

❑ Guía práctica de seguridad móvil

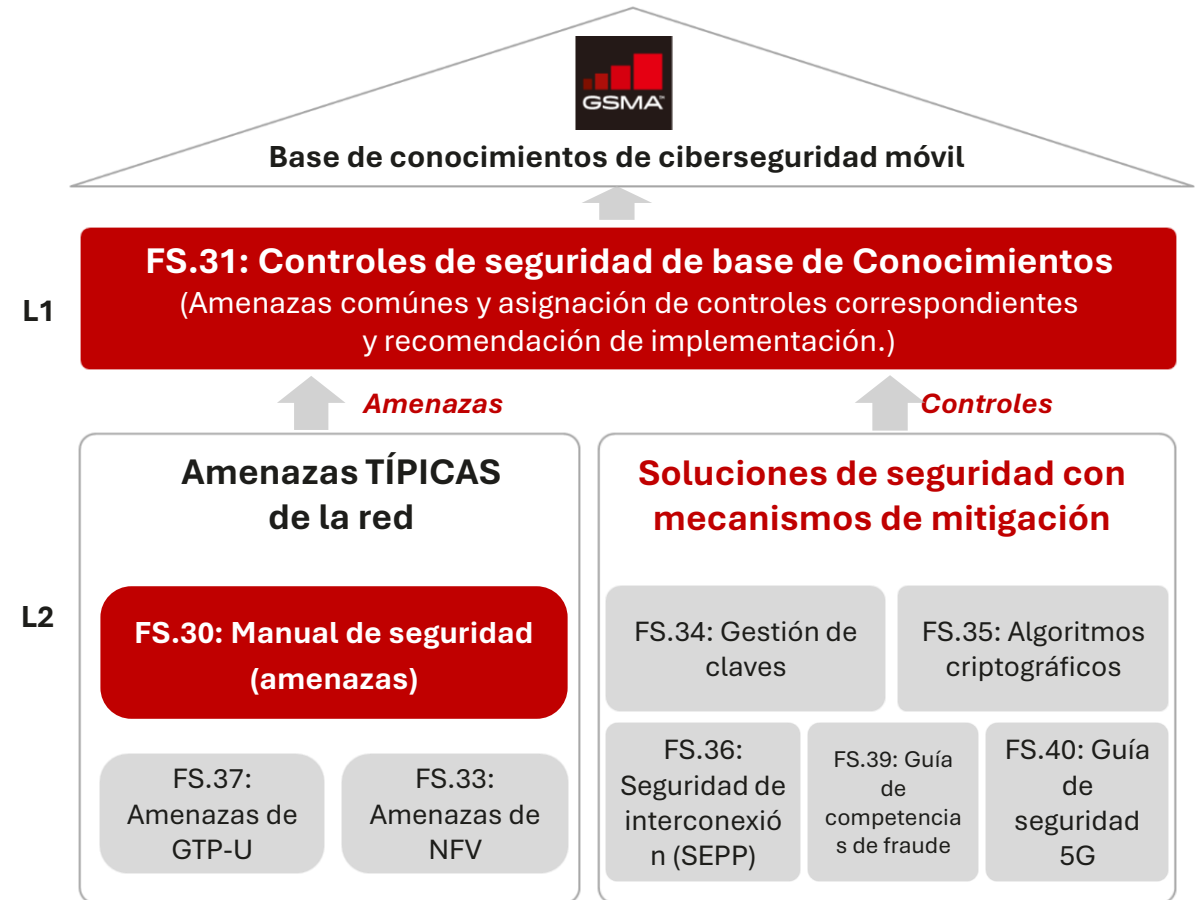
- Una referencia y una base estratégica para mejorar la seguridad de la red Móvil

❑ Colaboración con todas las partes

- Los Proveedores de equipos comparten información acerca de vulnerabilidades de equipos, los Operadores de Servicios lo hacen respecto a amenazas comunes de las redes, mitigando riesgos de los elementos de la red y remediando vulnerabilidades. Los Proveedores de Aplicaciones y Servicios de Industrias verticales protegen la información sensible del mercado y datos de usuarios. Las Agencias especializadas generan y comparten conocimiento, mejores prácticas, al mismo tiempo que analizan incidentes típicos de industria.

❑ Evaluación de seguridad

- Medidas de control de seguridad en función a la base de conocimientos y realizar evaluaciones periódicas basadas en el modelo de madurez de seguridad GSMA



Elementos clasificados de controles de seguridad



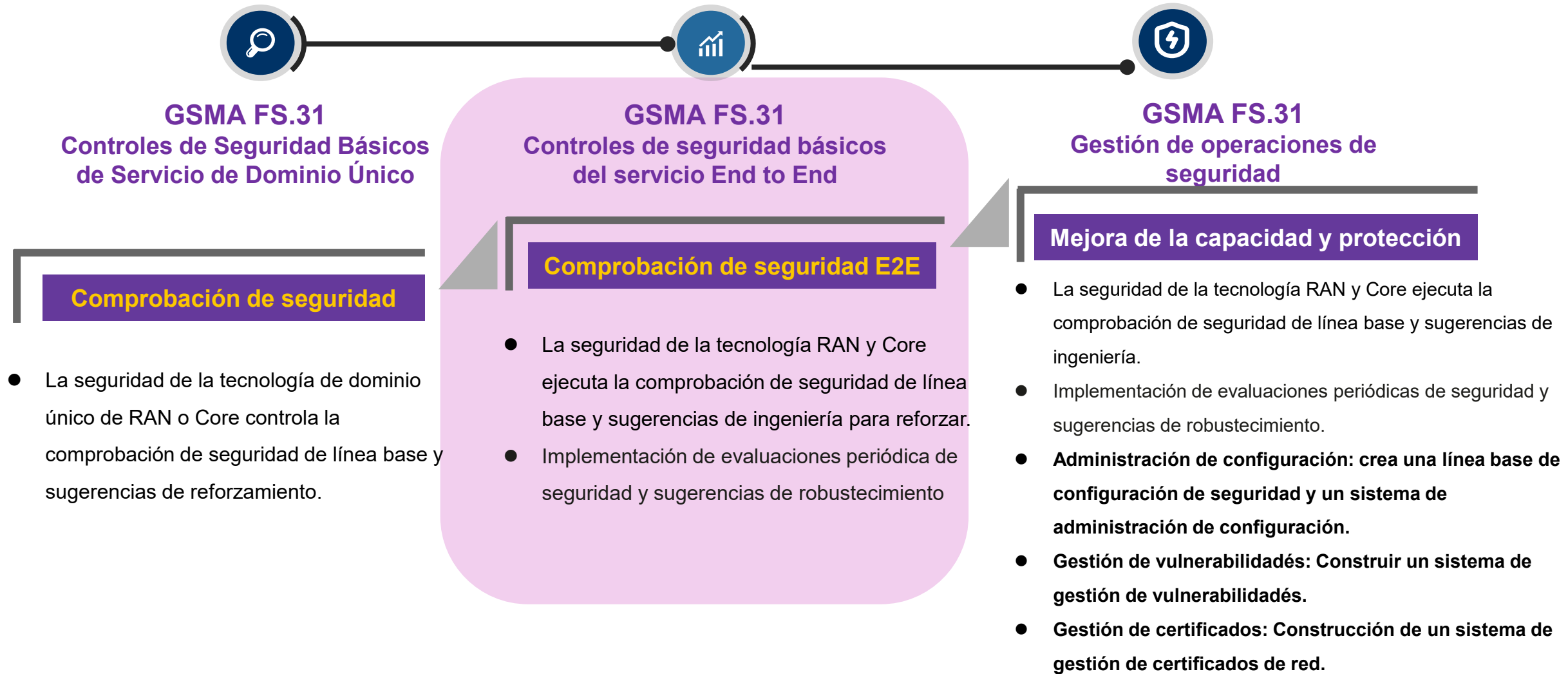
Lo hace a través de controles técnicos y controles de Negocio.

Controles de equipos de usuario y equipos móviles
Controles de gestión de la UICC
Controles de Internet de las cosas
Controles de radio
Controles de la arquitectura de red
Controles de infraestructura de red
Controles de servicios de red
Controles de gestión de la red core
Controles de operaciones de red
Orquestación y controles de seguridad NFV
Controles de operaciones de seguridad
Controles de roaming e interconexión



BC-001	Compromiso a nivel de progreso
BC-002	rol que reconoce formalmente la seguridad
BC-003	Políticas de la administración
BC-004	GRC (gobernanza, riesgo y cumplimiento)
BC-005	Seguro por diseño
BC-006	Protección de datos/privacidad
BC-007	Ciclo de vida de desarrollo de software seguro (SDLC)
BC-008	Administración de Continuidad del Negocio (BCM)
BC-009	Controles de seguridad física
BC-010	Manchas de adquisición
BC-011	instrucciones de externalización
BC-012	Retirada del servicio de equipos
BC-013	Los productos (HW/SW) protegidos
BC-014	Estrategias de ciber y regímenes de cumplimiento
BC-015	definir objetivos estratégico claros de ciberresiliencia

Alcance progresivo de MCKB



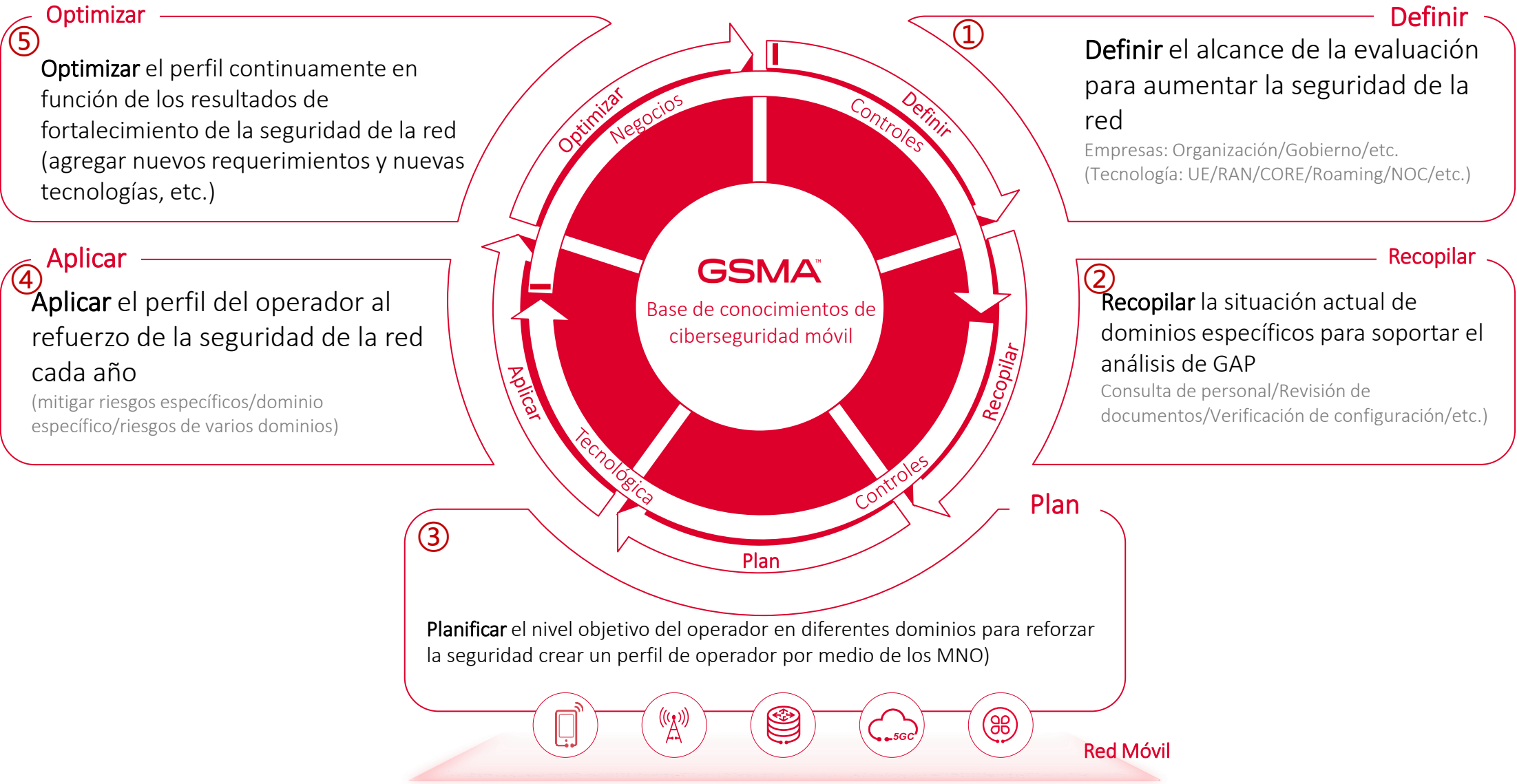
Seguridad E2E (End to End), de extremo a extremo.

Modelo de madurez de MCKB

- L5** Optimizar continuamente el proceso y el procedimiento de seguridad de los operadores en función de las actualizaciones de software de los proveedores y los nuevos riesgos o requisitos reglamentarios
- L4** Desarrollar y rastrear los KPI de refuerzo de seguridad y la implementación de los operadores
- L3** Crear estándares de seguridad de dominio específico de la empresa
- L2** Crear/ejecutar/verificar una tarea de seguridad de dominio específico de rutina (como: verificación de acceso a la red)
- L1** Modificación temporal de la configuración de seguridad de dominio específico o procesamiento de eventos
- L0** Sin consideración de seguridad de dominio específico



GSMA MCKB permite la mejora de la red móvil en cinco pasos



Seguridad por Diseño – NESAS (Network Equipment Security Assurance)

NESAS de la GSMA facilita mejoras en los niveles de seguridad de los equipos de red en toda la industria móvil, proporcionando un marco de aseguramiento con alcance inclusivo y global.

Security

> Home

GSMA Network Equipment Security Assurance Scheme

- Network Equipment Vendors
- Mobile Operator Benefits
- Conformance Results
- Authorised Test Laboratories
- Appointed Auditors
- Government & National Authority Benefits
- Documentation
- Contact Us
- < GSMA Services
- < Back to Home

GSMA Network Equipment Security Assurance Scheme (NESAS)

What is the GSMA Network Equipment Security Assurance Scheme (NESAS)?

The GSMA Network Equipment Security Assurance Scheme (NESAS) is here to facilitate improvements in network equipment security levels, across the mobile industry. Providing one universal and global security assurance framework. Ultimately, raising confidence and trust in mobile network equipment.

Beneficios para la Industria

NESAS es de confianza en todo el mundo, desde el diseño del producto hasta la entrega final y el mantenimiento.

Los módulos y sus equipos son probados y auditados en relación con una línea de base de seguridad, definida por expertos de la industria a través de GSMA y 3GPP. Por lo tanto, refleja las necesidades de seguridad de todo el ecosistema, incluidos los reguladores, los operadores de redes móviles, los hiperescaladores y los proveedores de equipos.

Estándar universal de la Industria

El estándar evoluciona continuamente para satisfacer las necesidades de toda la industria, sobre la base de los estándares 3GPP + GSMA y evitando que los requerimientos de seguridad se **fragmenten** regionalmente.

Impulsa la mejora

Las auditorías y las evaluaciones brindan una oportunidad para que los expertos aporten comentarios y análisis en profundidad, lo que ayuda a los proveedores a mejorar sus procesos y productos, a la vez que mejoran la seguridad en toda la industria.

Sólida auditoría independiente

NESAS es un esquema **imparcial**. La GSMA trabaja con socios reconocidos internacionalmente para auditar y evaluar equipos de forma continua.

Simplificación del proceso

La lista de resultados de las evaluaciones proporciona una visibilidad casi en tiempo real del estado de la seguridad, lo que permite a los interesados la visualización de resultados y comparaciones con transparencia y claridad.

Beneficios para los reguladores

Aporta un sistema global transparente e independiente, que refleja las necesidades de seguridad de todo el ecosistema, brindando un sistema claro para la mitigación de riesgos y Seguridad de forma integral.

Beneficios para todos los miembros de la cadena de valor

Proveedores de equipos de red

NESAS está diseñado para ayudar a evaluar los niveles de seguridad, los equipos y las funciones definidas por 3GPP.

- *Demuestre a los clientes que sus productos cumplen con los estándares de seguridad universales en los que confía la industria global.*
- *Proporciona claridad a los clientes y reguladores, al tiempo que apoya el desarrollo del negocio.*
- *Una auditoría con alcance global: no es necesario repetir las pruebas de seguridad en múltiples mercados.*
- *Aprovechar la mejora continua de la seguridad con el consentimiento de los expertos y auditores.*

Operadores móviles

NESAS ayuda a garantizar la seguridad y la resiliencia de su red.

- *Confíe en su equipo de red gracias a la certificación del proveedor*
- *El único sistema de seguridad con el aval de los creadores del estándar en la industria Telecom (a través de GSMA y 3GPP), lo que garantiza que se mantenga al día con la identificación de nuevas amenazas y las mitigaciones.*
- *Optimice el análisis de la cadena de suministro, y la visibilidad instantánea de los niveles de seguridad*
- *Reduzca las pruebas de seguridad mediante la externalización de las pruebas de referencia a laboratorios de evaluación.*
- *Conformidad probada por auditores independientes y laboratorios certificados*

Hiperescaladores

Demostrar la conformidad con NESAS les permite liderar con el ejemplo y abogar por la seguridad más alta dentro de los servicios en la nube

- *Proporciona a los clientes la seguridad basada en su equipo de red, desde el desarrollo hasta la implementación.*
- *Fomenta la seguridad mediante la cultura de seguridad por diseño*
- *Haga que sus plataformas sean más atractivas para alojar aplicaciones sensibles, como las que manejan transacciones financieras o de industrias que demandan alta disponibilidad*

Conclusiones

Uso de Estándares globales

Evitar fragmentación, duplicidad y requerimientos adicionales de Ciberseguridad. Para ello considerar marcos de referencia maduros de la Industria como **GSMA Mobile Cybersecurity Knowledge Base**

Mejorar la cultura de la Ciberseguridad

Brindar planes de capacitación continua y adopción de nuevos conocimientos basados en la evolución de las tecnologías

Alentar la innovación

Mantener una gestión basada en riesgos que tengan por objetivo la mejora en la calidad de vida de las personas y aumento en la productividad, eficiencia de las organizaciones e Industrias

Identificar ciclo de vida

Incorporar los mecanismos de control para actualizar, modernizar y hacer uso de tecnologías emergentes para mejorar la seguridad de los productos/Servicios y mantenerlos vigentes

Las estrategias de Ciberseguridad deben considerarse de manera global y armonizadas, en lugar de acciones que deban llevarse a cabo solo de manera aislada.

Gracias

Pablo Corona Fraga

pcoronaf@nyce.org.mx

@pcoronaf

