TrendAI™ · Mérida 2026

Del inventario de vulnerabilidades a la gestión del riesgo

Johnny Trujillo

Enterprise Regional Accoun Manager

TrendAI™ · **Agosto 2026**

TrendAI

63 días → -7 días

El tiempo promedio para explotar una vulnerabilidad pasó de 63 días en 2018 a aproximadamente -7 días en 2025.

Fuente: Mandiant M-Trends 2026

TrendAI

El dato detrás del dato

Un valor negativo significa que ya no hay ventana de reacción

Mandiant y Google Threat Intelligence reportan que el Mean Time to Exploit pasó de 63 días en 2018, a -1 día en 2024, y aproximadamente -7 días en 2025. Un valor negativo significa que, en promedio, la explotación ocurrió antes de que hubiera un parche disponible.

El atacante puede explotar una vulnerabilidad antes de que exista el parche. Un ciclo tradicional de vulnerability management, basado en escaneo periódico y severidad, ya no alcanza.

Fuente: Mandiant M-Trends 2026

Antes el modelo podía ser:
Vulnerabilidad → se publica → fabricante desarrolla parche → empresa escanea → prioriza → parchea → atacante intenta explotarla.

Ahora puede ser:
Vulnerabilidad → atacante la explota → pasan días → aparece el parche → empresa apenas empieza a evaluar qué hacer.

La explotación de vulnerabilidades sigue siendo la puerta de entrada número uno

Mandiant señala que los exploits siguen siendo el vector inicial más común por sexto año consecutivo.

Además advierte que un acceso aparentemente menor puede transferirse a otro actor que ejecuta ransomware en menos de 30 segundos, haciendo que una alerta considerada de baja prioridad pueda convertirse rápidamente en un compromiso significativo.

> El riesgo no necesariamente está en la vulnerabilidad con el CVSS más alto. Está en la exposición que el atacante realmente puede utilizar para llegar a un activo crítico.

Fuente: Mandiant M-Trends 2026

Si no puedo parchear todo, ¿cómo sé qué debo atender primero?

El atacante ya no necesita vulnerarte desde cero, puede comprar el acceso.

Infostealers → credenciales expuestas → mercados clandestinos → Initial Access Brokers → hand-off

01

INFOSTEALERS

16M+

dispositivos infectados observados en 2025

Roban credenciales, cookies de sesión y otros datos que después pueden utilizarse para obtener acceso.

IBM X-Force — Cloud attacks are evolving (2026)

02

DARK WEB

+12%

credenciales de infostealers a la venta (2024)

Los cinco principales infostealers generaron más de 8M de anuncios; cada anuncio puede contener cientos de credenciales.

IBM X-Force Threat Intelligence Index 2025

03

INITIAL ACCESS BROKERS

22 s

mediana de hand-off en 2025

Los brokers pueden monetizar accesos corporativos. Mandiant observa que un segundo grupo puede recibir acceso al entorno casi inmediatamente.

Mandiant — M-Trends 2026, p. 55 + IBM X-Force

El riesgo ya tiene una cadena de suministro: robar identidad → monetizar acceso → transferirlo a otro atacante.

¿Qué activos, identidades y credenciales de tu organización ya están expuestos antes de que alguien los compre?

Fuentes: IBM X-Force, “Cloud attacks are evolving: What 2025 trends mean for defenders in 2026” (16M+ dispositivos; accesos corporativos de alto valor e IAB). IBM X-Force Threat Intelligence Index 2025 (+12% en credenciales de infostealers a la venta; >8M anuncios). Mandiant, M-Trends 2026, p. 55 (22 s de mediana entre acceso inicial y hand-off a un segundo grupo).

No estamos entrando en un periodo de incertidumbre. Estamos entrando en un nuevo entorno operativo definido por la incertidumbre.

En este entorno, la ciber resiliencia ya no es solo una capacidad defensiva. Es el resultado de la gestión continua del ciber riesgo, permitiendo a las organizaciones operar con confianza, incluso en condiciones de incertidumbre.

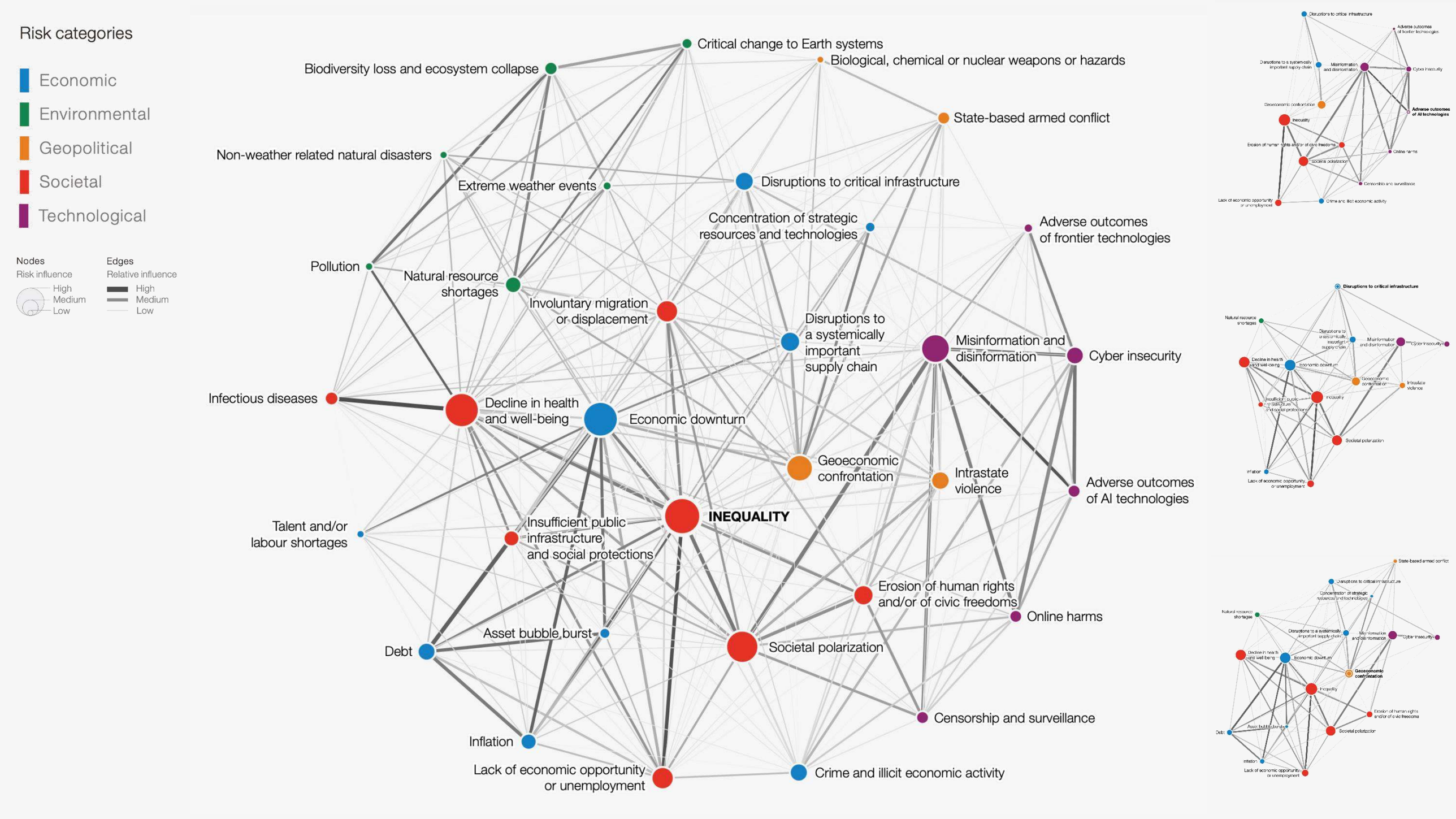
WORLD ECONOMIC FORUM

TrendAI™

Tenemos que aprender a dejar de hablar solo de amenazas y de eventos, para complementarlo con la parte de gestión de riegos.

WORLD ECONOMIC FORUM

TrendAI™

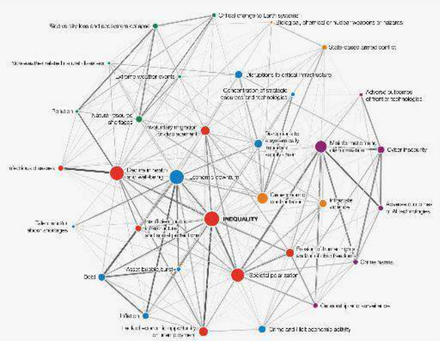

Risk categories
Economic
Environmental
Geopolitical
Societal
Technological
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Critical change to Earth systems
Biodiversity loss and ecosystem collapse
Biological, chemical or nuclear weapons or hazards
State-based armed conflict
Non-weather related natural disasters
Extreme weather events
Disruptions to critical infrastructure
Concentration of strategic resources and technologies
Adverse outcomes of frontier technologies
Pollution
Natural resource shortages
Involuntary migration or displacement
Disruptions to a systemically important supply chain
Misinformation and disinformation
Cyber insecurity
Infectious diseases
Decline in health and well-being
Economic downturn
Geoeconomic confrontation
Intrastate violence
Adverse outcomes of AI technologies
Talent and/or labour shortages
Insufficient public infrastructure and social protections
INEQUALITY
Erosion of human rights and/or of civic freedoms
Online harms
Asset bubble burst
Debt
Societal polarization
Censorship and surveillance
Inflation
Lack of economic opportunity or unemployment
Crime and illicit economic activity

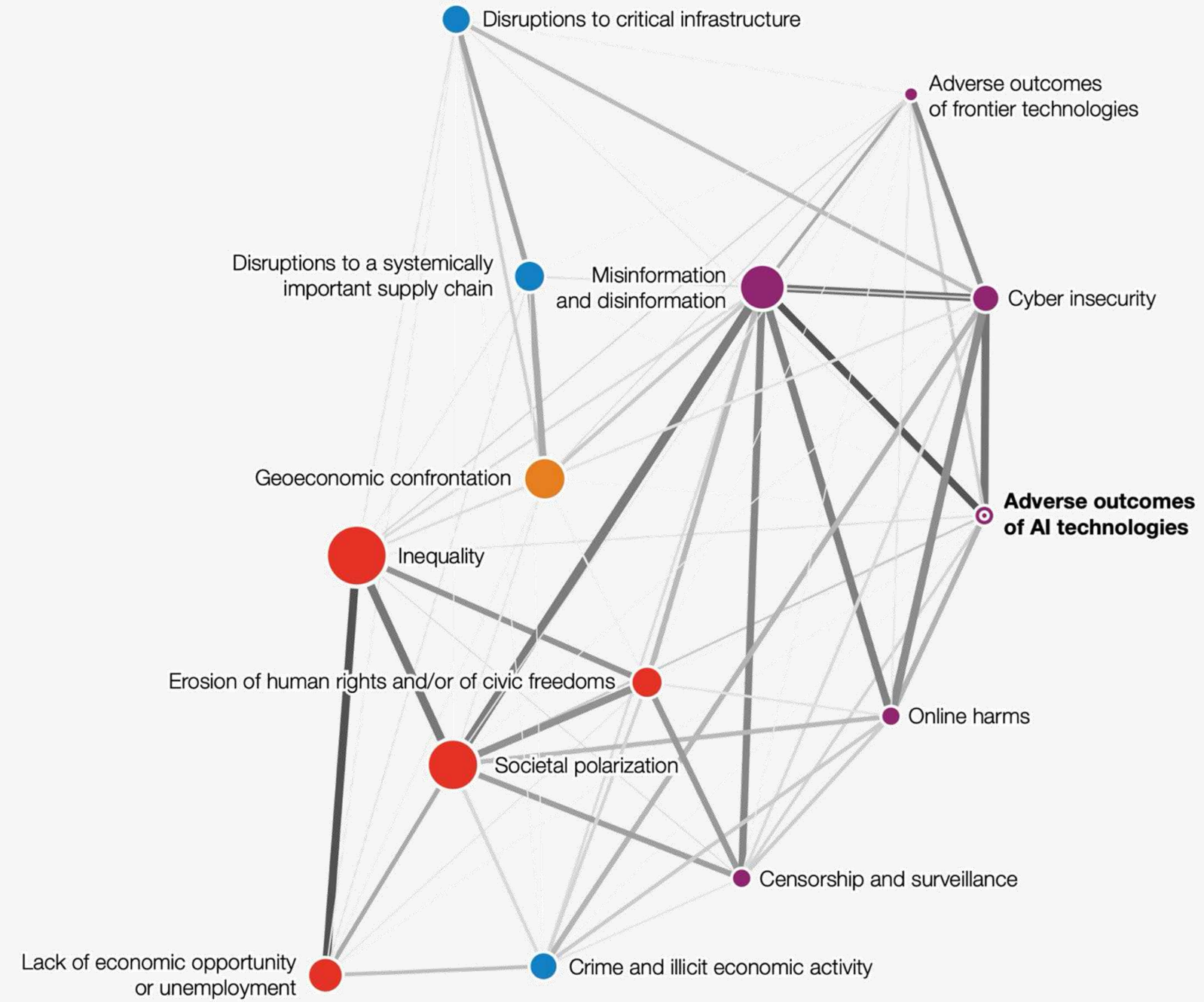
Risk categories

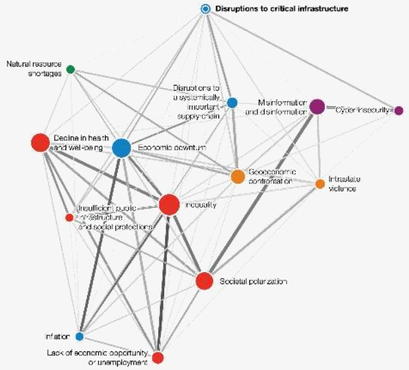
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

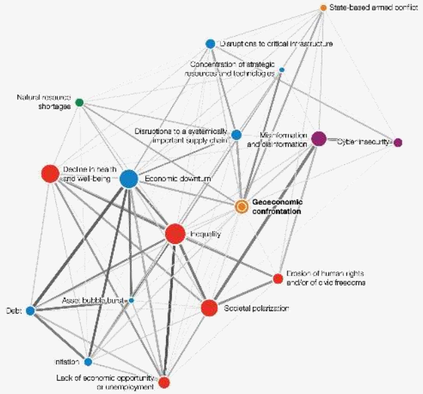
Nodes
Risk influence
High
Medium
Low

Edges
Relative influence
High
Medium
Low







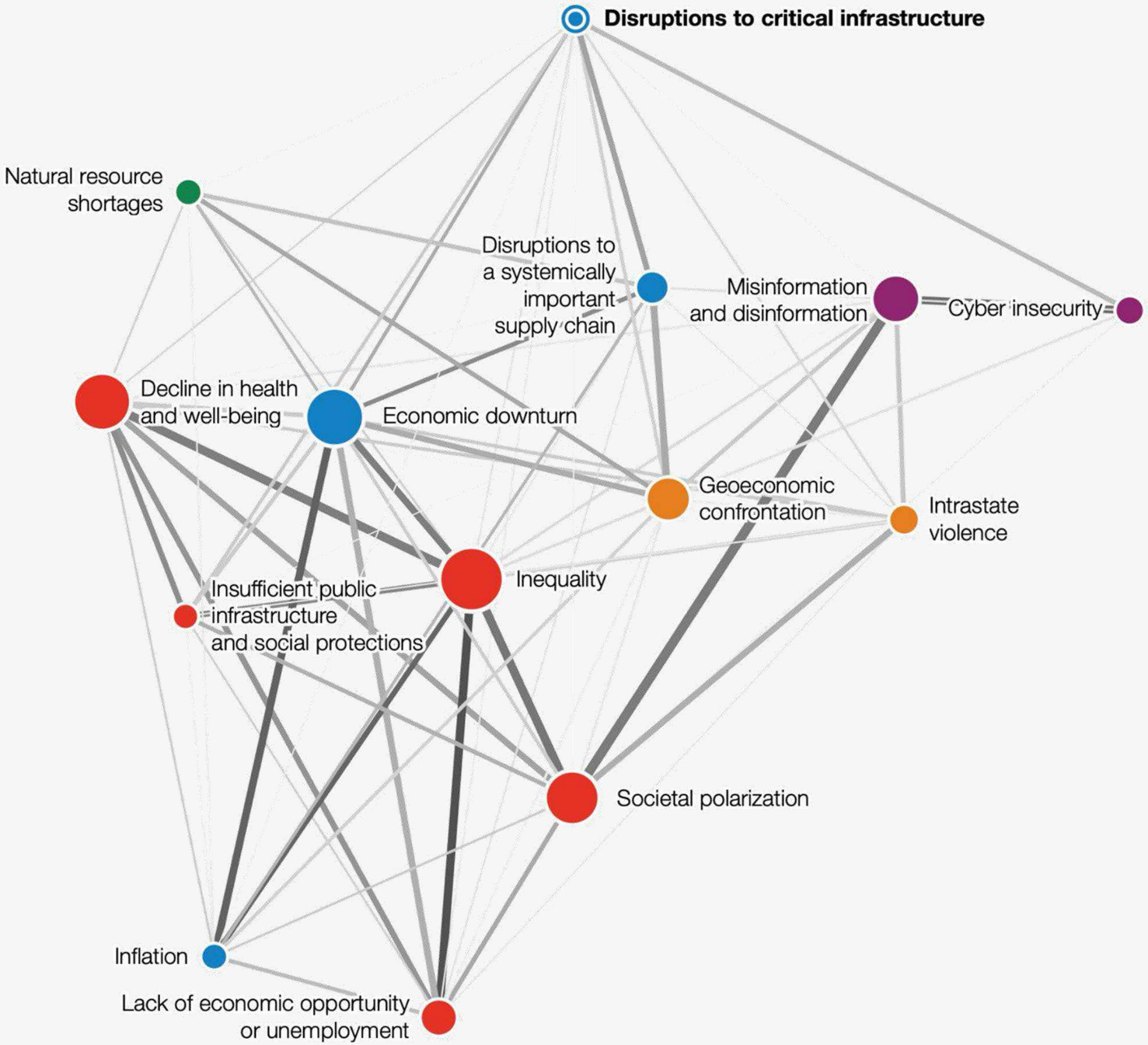


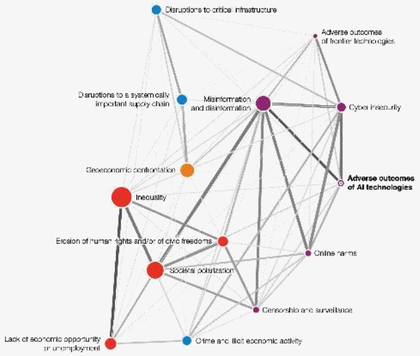
Risk categories

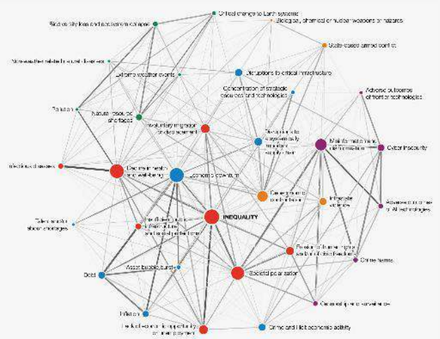
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

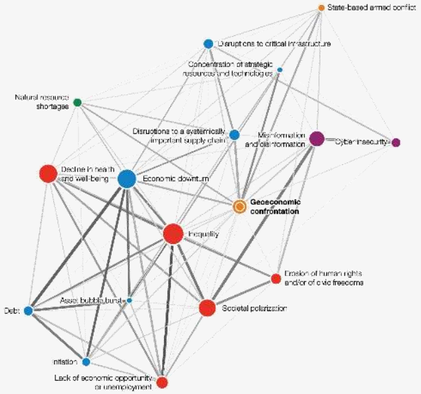
Nodes
Risk influence
High
Medium
Low

Edges
Relative influence
High
Medium
Low







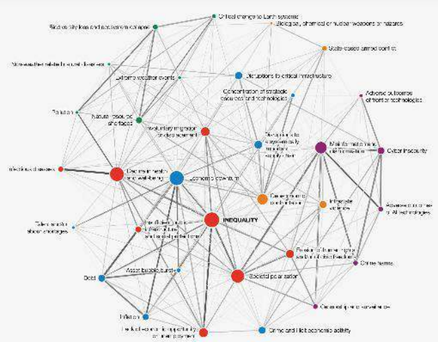


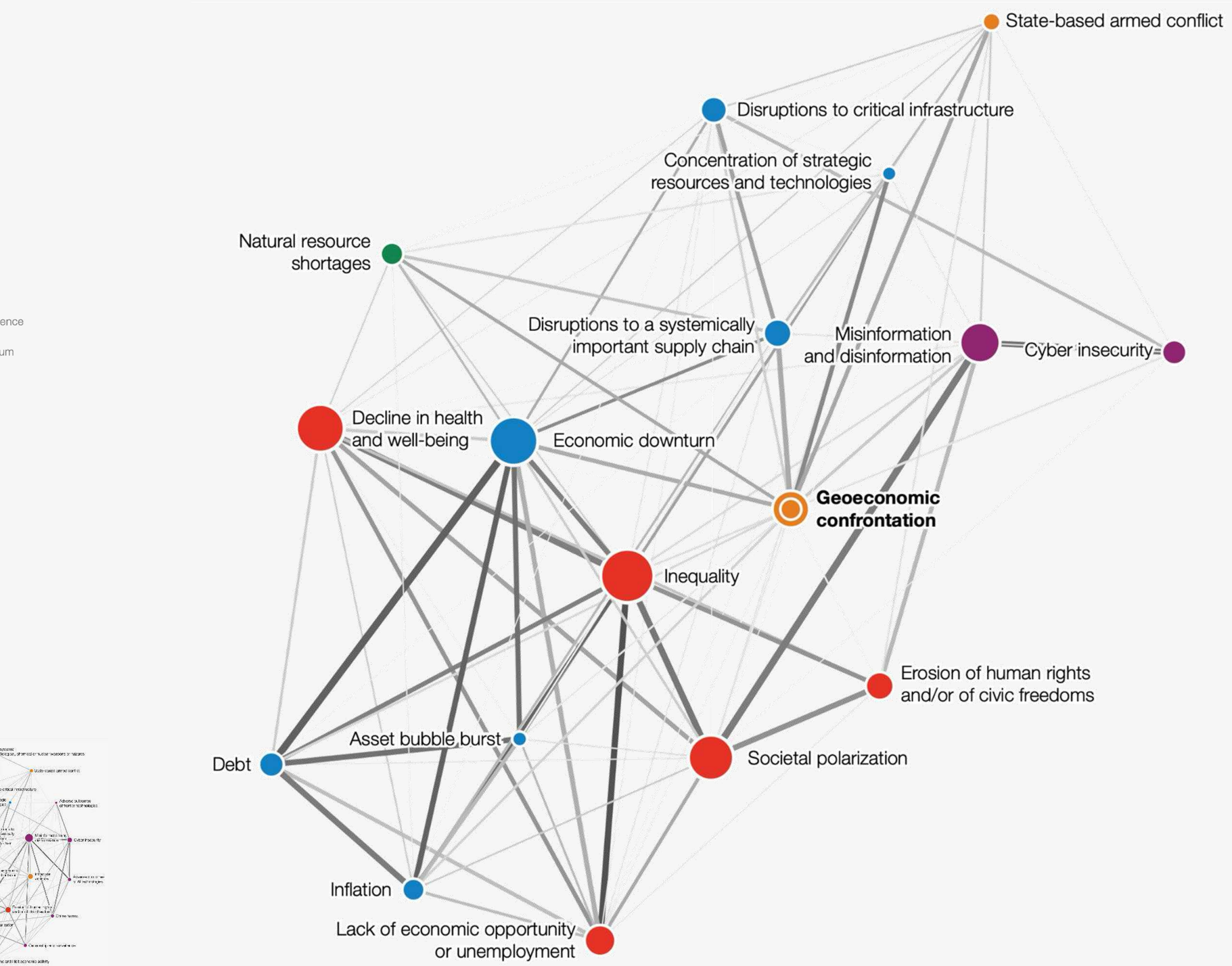
Risk categories

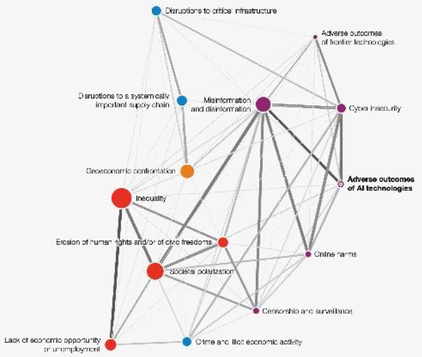
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

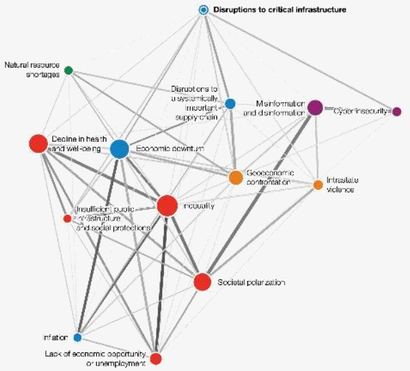
Nodes
Risk influence
High
Medium
Low

Edges
Relative influence
High
Medium
Low





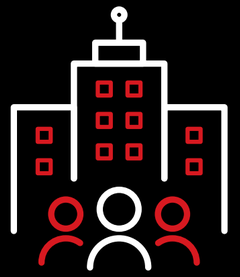




“Se prevé que la IA sea el factor de cambio más significativo en la ciberseguridad durante este año”

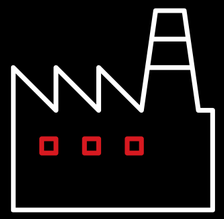
“La adopción gener… …xpande nu… …tradicionales … para gestionar”

“La … …transformando la ciberseguridad en ambos lados: fortaleciendo la defensa y, al mismo tiempo, habilitando ataques más sofisticados”



IA

está acelerando todo, en todas partes, al mismo tiempo



El problema no es solamente las vulnerabilidades

PERSONAS

- Identidades y privilegios
- Usuarios de riesgo
- Phishing / comportamiento

ACTIVOS

- Endpoints y servidores
- Aplicaciones
- OT e IoT

CLOUD

- Workloads y SaaS
- Configuraciones
- Identidades cloud

EXPOSICIÓN EXTERNA

- Dominios e IPs
- Servicios publicados
- Shadow IT

VULNERABILIDADES

- CVEs y software vulnerable
- Misconfigurations
- Exploits / exposición

AI

- Shadow AI
- Aplicaciones y modelos AI
- Datos y uso no autorizado

correlacionar señales + contexto + criticidad + rutas de ataque

NO ES: “¿Cuántas vulnerabilidades tengo?”

¿Dónde está realmente mi riesgo?

Priorizar lo explotable, expuesto y crítico para el negocio.

El costo de llegar tarde

Estamos usando IA demasiado tarde

50% de las organizaciones comprometidas ya utiliza agentes de IA dentro del SOC.

18% los aplica a vulnerability scanning y vulnerability management.

Estamos usando IA para detectar, investigar y responder. Todavía muy poco para identificar exposición, contextualizar, priorizar y prevenir.

Fuente: IBM Cost of a Data Breach 2026

El siguiente paso de la ciberseguridad no es generar más alertas. Es usar inteligencia, contexto de negocio e IA para decidir qué riesgo importa realmente.

TrendAI

De vulnerabilidad a riesgo de negocio

TrendAI

¿Qué debo corregir primero?

Vulnerabilidad → Explotabilidad → Exposición → Criticidad del activo → Threat intelligence → Impacto en el negocio

↓

Priorización basada en Riesgo y contexto

Mandiant recomienda que vulnerability management no priorice únicamente por severidad, sino que los datos se analicen con contexto de negocio, considerando el valor del activo y su impacto sobre las operaciones.

TrendAI™

¿ESPERARÍAS A TENER UN INFARTO PARA REVISAR TU SALUD?

¿Se puede conocer la salud observando un solo signo vital?

SALUD DE UNA PERSONA

Un wearable correlaciona

- 💗 Frecuencia cardíaca
- 🩸 Presión arterial
- 🌡️ Temperatura
- 🫁 Saturación O_2
- 😴 Calidad sueño
- 🧠 Estrés

Frecuencia elevada **aislada** ≠ diabetes?

Frecuencia + presión + baja O_2 + Azúcar en sangre + glucosa = **riesgo real**.

Ciber Riesgo

- Visivilidad
- Contexto
- Correlación
- Prioridad

RISK PRIORITY

SALUD DE CIBERSEGURIDAD

Cyber Risk correlaciona

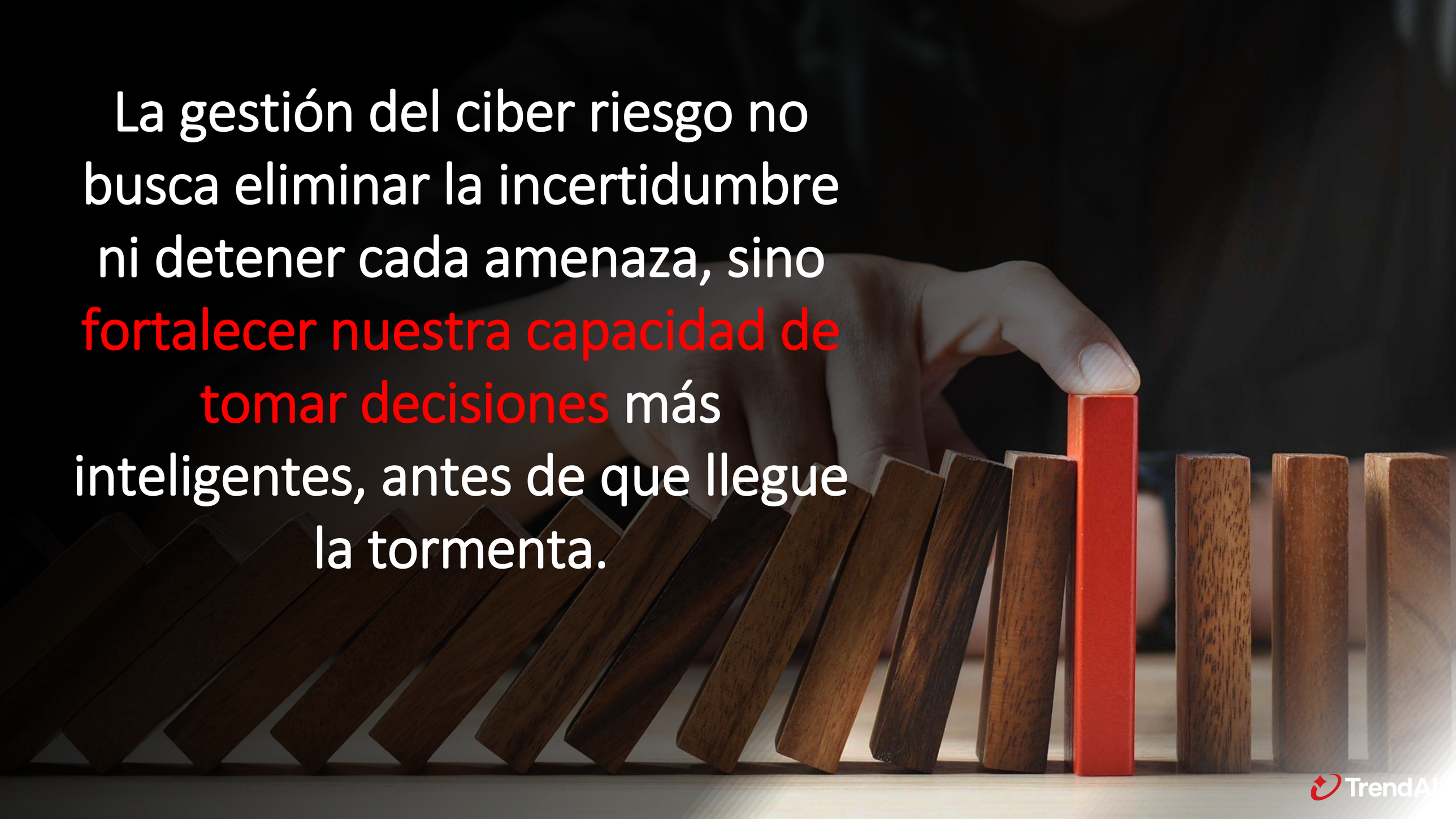
- 💻 Endpoints
- 👤 Identidades
- ☁️ Cloud
- 🌍 Attack surface
- 🕳️ Vulnerabilidades
- ⚠️ Amenazas

Crítica **aislada** = cierto riesgo.

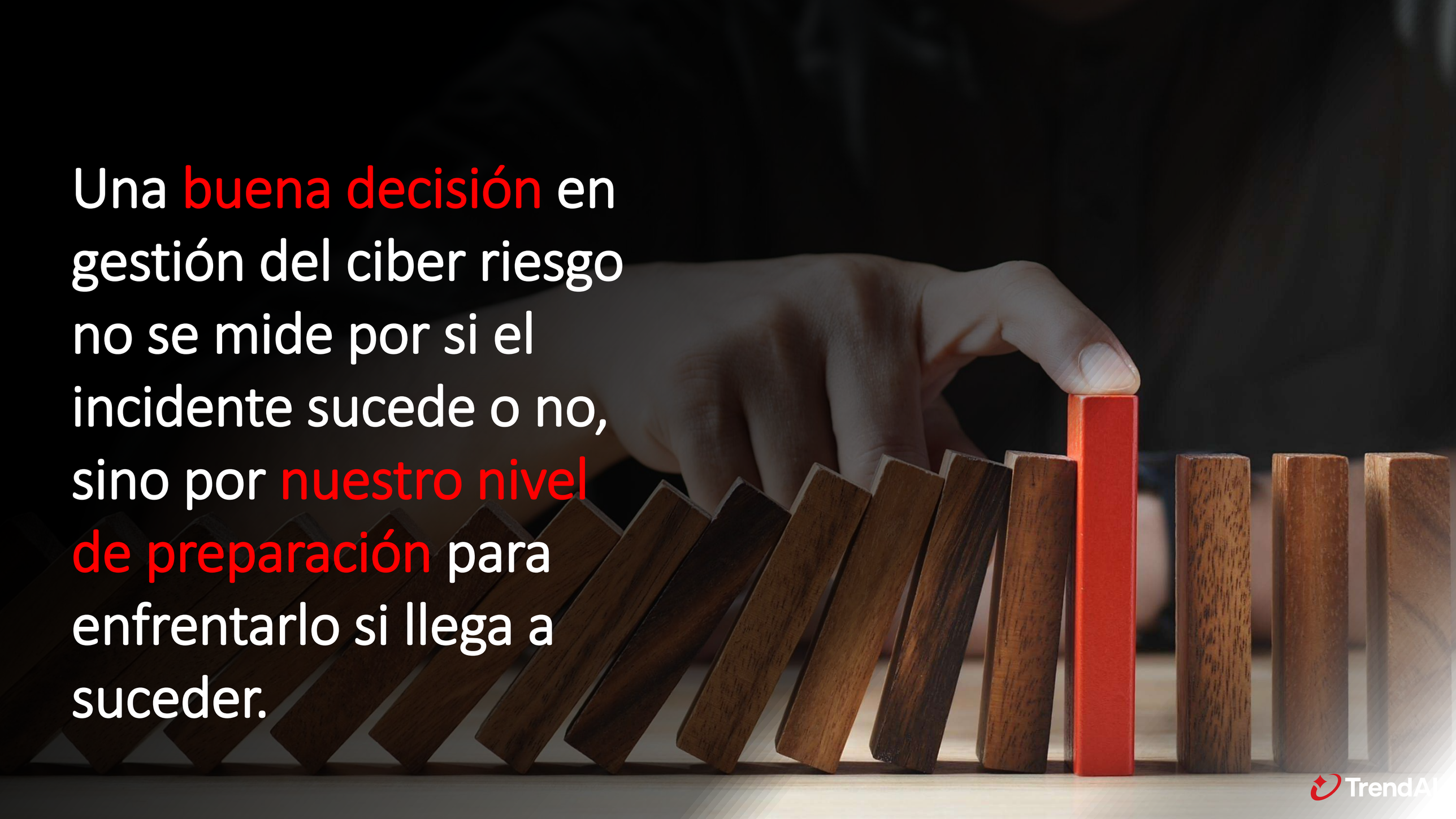
Crítica + expuesta + exploit + activo crítico = **máxima prioridad**.

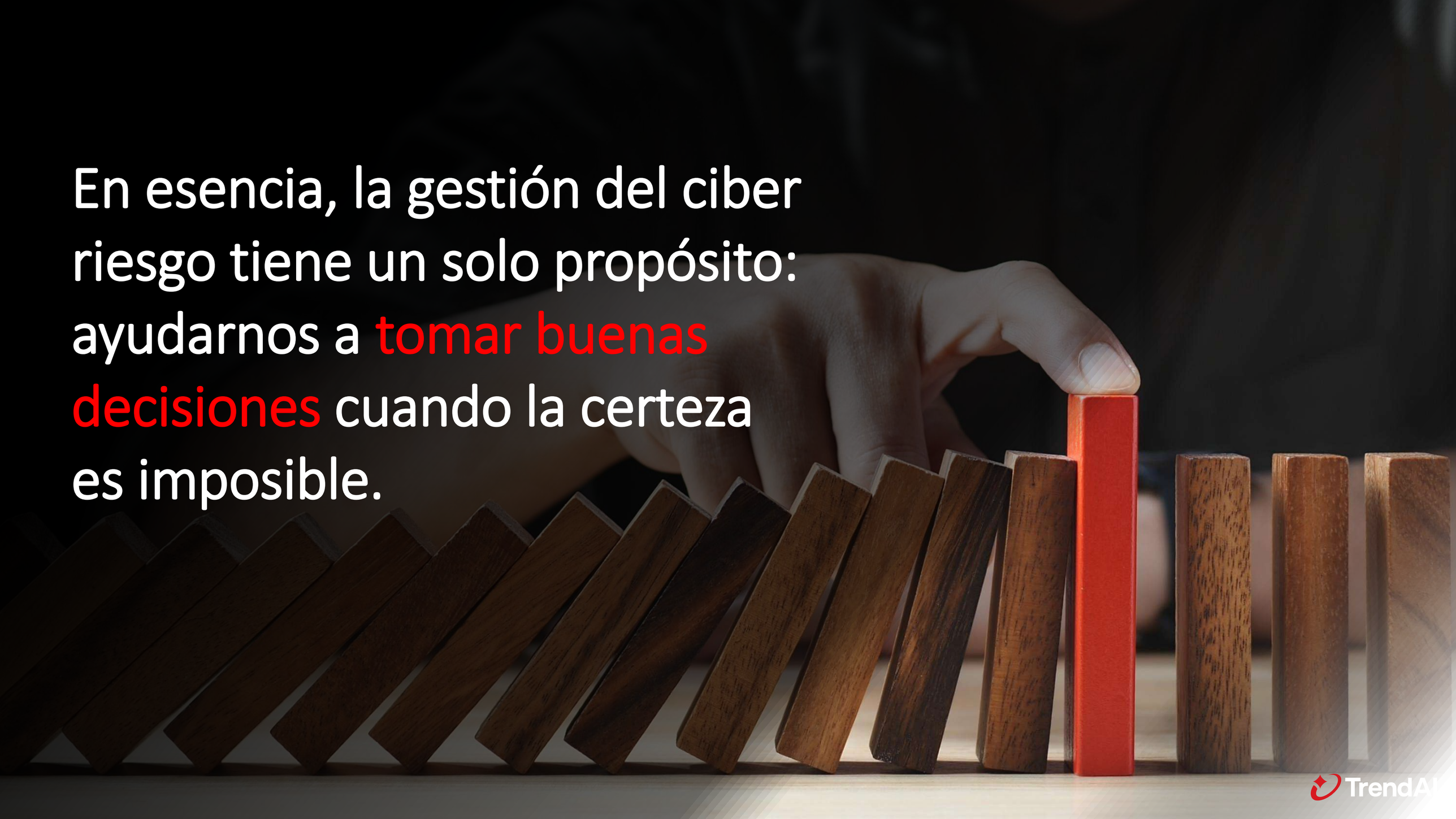
En el Ciber Riesgo no mide un solo signo vital. Correlaciona toda la exposición para identificar qué es un riesgo real para el negocio.

“La probabilidad de éxito de los atacantes aumenta cuando las organizaciones **no tienen la capacidad de tomar decisiones proactivas** basadas en el ciber riesgo.


La gestión del ciber riesgo no busca eliminar la incertidumbre ni detener cada amenaza, sino fortalecer nuestra capacidad de tomar decisiones más inteligentes, antes de que llegue la tormenta.

Una buena decisión en gestión del ciber riesgo no se mide por si el incidente sucede o no, sino por nuestro nivel de preparación para enfrentarlo si llega a suceder.




En esencia, la gestión del ciber riesgo tiene un solo propósito: ayudarnos a tomar buenas decisiones cuando la certeza es imposible.

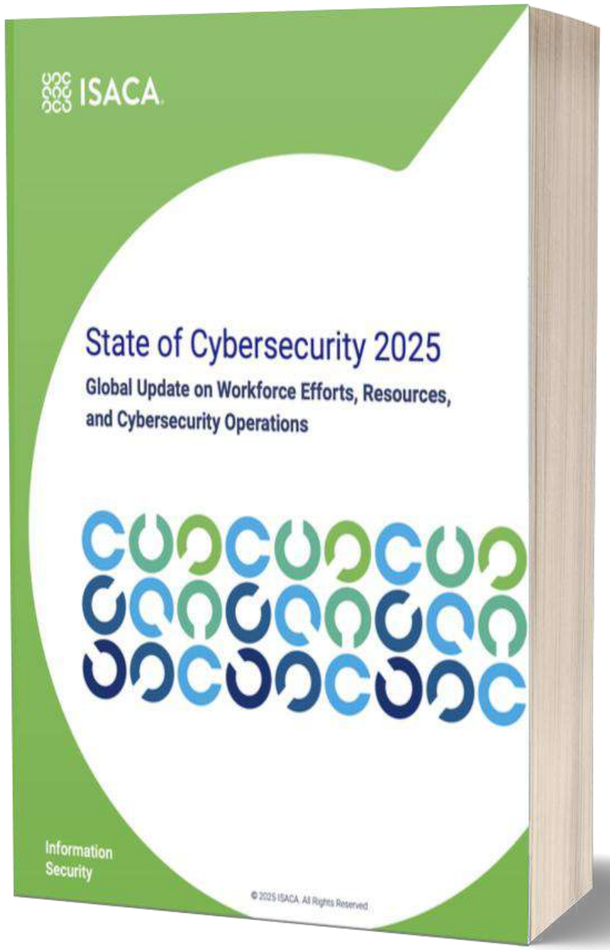
El propósito de la gestión del ciber riesgo es sencillo: ayudar a los líderes a tomar mejores decisiones, no garantizar resultados perfectos.


La gestión del ciber riesgo no promete seguridad garantiza que tomemos las decisiones correctas antes de que sea demasiado tarde.

Gestión de Amenazas	Gestión del Ciber Riesgo
Inmediata, táctica, enfocada en lo que está ocurriendo ahora	Estratégica, predictiva, enfocada en lo que podría ocurrir
Requiere precisión y velocidad	Requiere juicio y priorización
Responde a: ¿Está lloviendo? ¿Dónde? ¿Cómo respondemos?	**Responde a:** ¿Podría llover? ¿Cuánto importaría si sucede? ¿Cómo nos preparamos?

Hablar de Ciber Riesgo es difícil porque:	
Las amenazas son tangibles	El ciber riesgo es hipotético
Las amenazas activan alertas	El ciber riesgo requiere imaginar escenarios futuros
Las amenazas exigen acción inmediata	El ciber riesgo requiere decisiones reflexivas
El éxito es visible: un ataque fue detenido	El éxito es invisible: nada ocurre porque actuamos a tiempo y correctamente
Se basa en la certeza y la evidencia	Se basa en la probabilidad, el impacto y la anticipación

Tipo de Ciber Riesgo	Lo que Representa
Ciber Riesgo Inherente	El nivel de ciber riesgo al que se enfrenta la organización antes de implementar cualquier medida de seguridad. Sin firewalls, sin SOC, sin controles de identidad, sin respaldos: solo exposición pura. Refleja el peligro de operar en un entorno digital sin protección.
Ciber Riesgo Residual	El nivel de ciber riesgo que permanece después de aplicar los controles y defensas existentes: monitoreo SOC, MFA, EDR, respaldos, segmentación, configuraciones en la nube, políticas de proveedores, etc. Es el riesgo que aún persiste, incluso con todas las protecciones actuales en funcionamiento.
Apetito de Ciber Riesgo	El nivel de ciber riesgo que la organización está dispuesta a aceptar según sus prioridades de negocio, requisitos regulatorios y apetito de riesgo. Representa el equilibrio entre protección, costo y necesidades operativas — no riesgo cero, sino el nivel adecuado de riesgo.



How often is a cyberrisk assessment performed on your organization?

Never	2%
Monthly	11%
Every 1-6 months	20%
Every 7-12 months	9%
Annually	40%
Every 1-2 years	4%
2 years or longer	3%
Don't know	12%

61%

0% 10% 20% 30% 40% 50%


Después de una Brecha
Antes de una Brecha
Durante una Brecha
Ciber Resiliencia
Gestión del Ciber Riesgo
Detección y Respuesta
Personas
Tecnología
Procesos

TrendAI™

Operación Normal

Metas y objetivos
en cumplimiento

Aprender y adaptarse

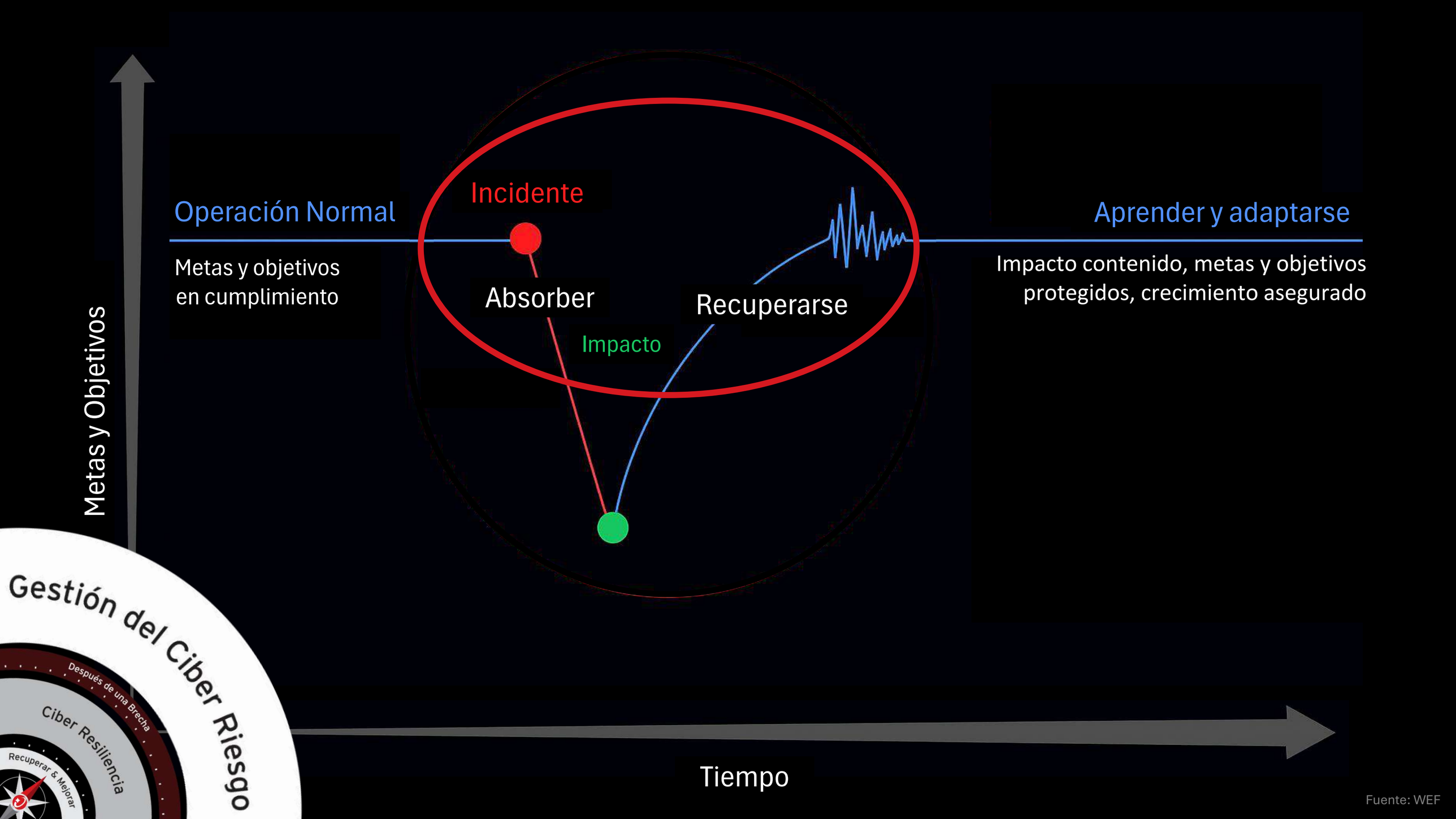
Impacto contenido, metas y objetivos
protegidos, crecimiento asegurado

Metas y Objetivos

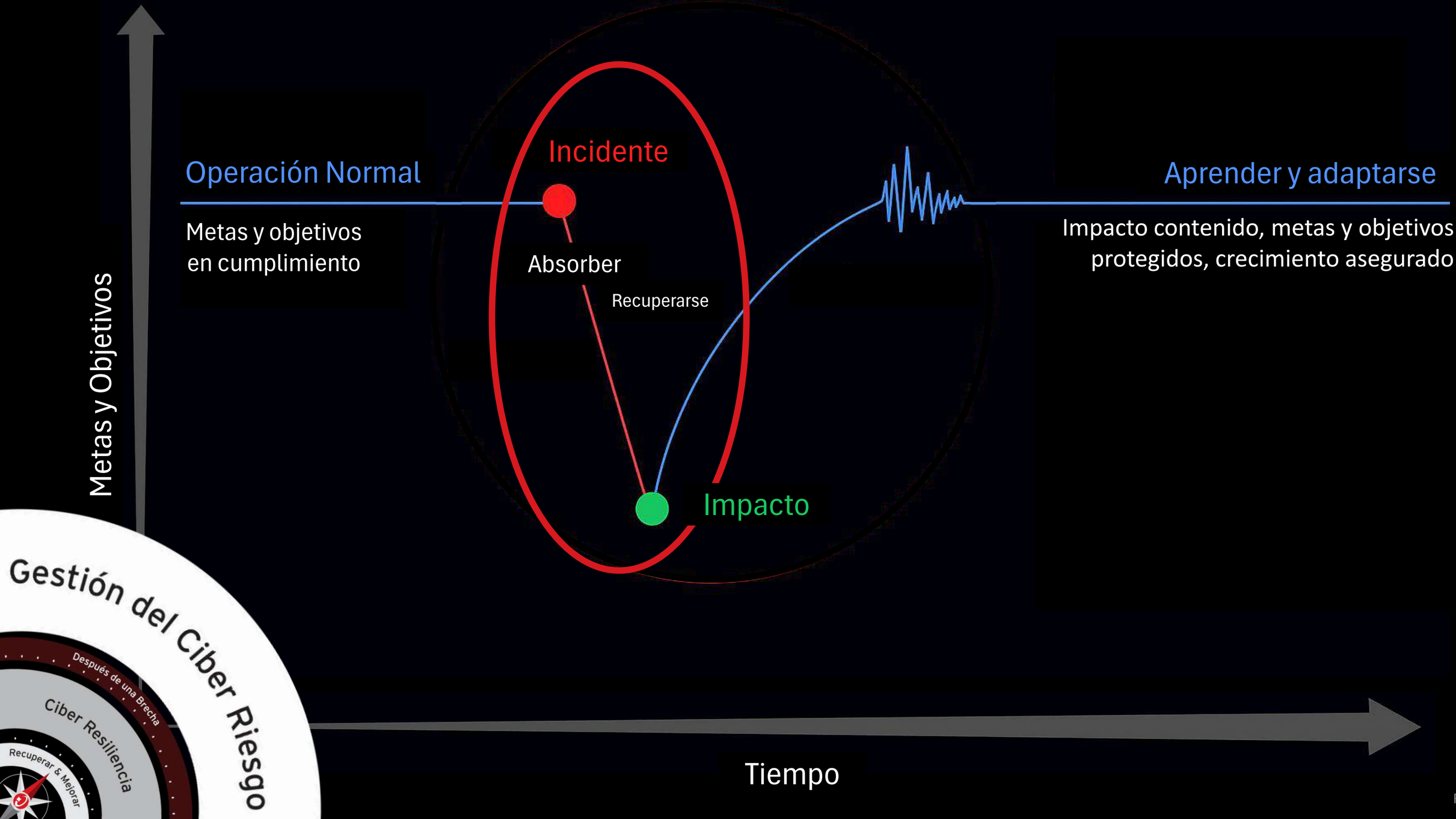
Impacto

Tiempo

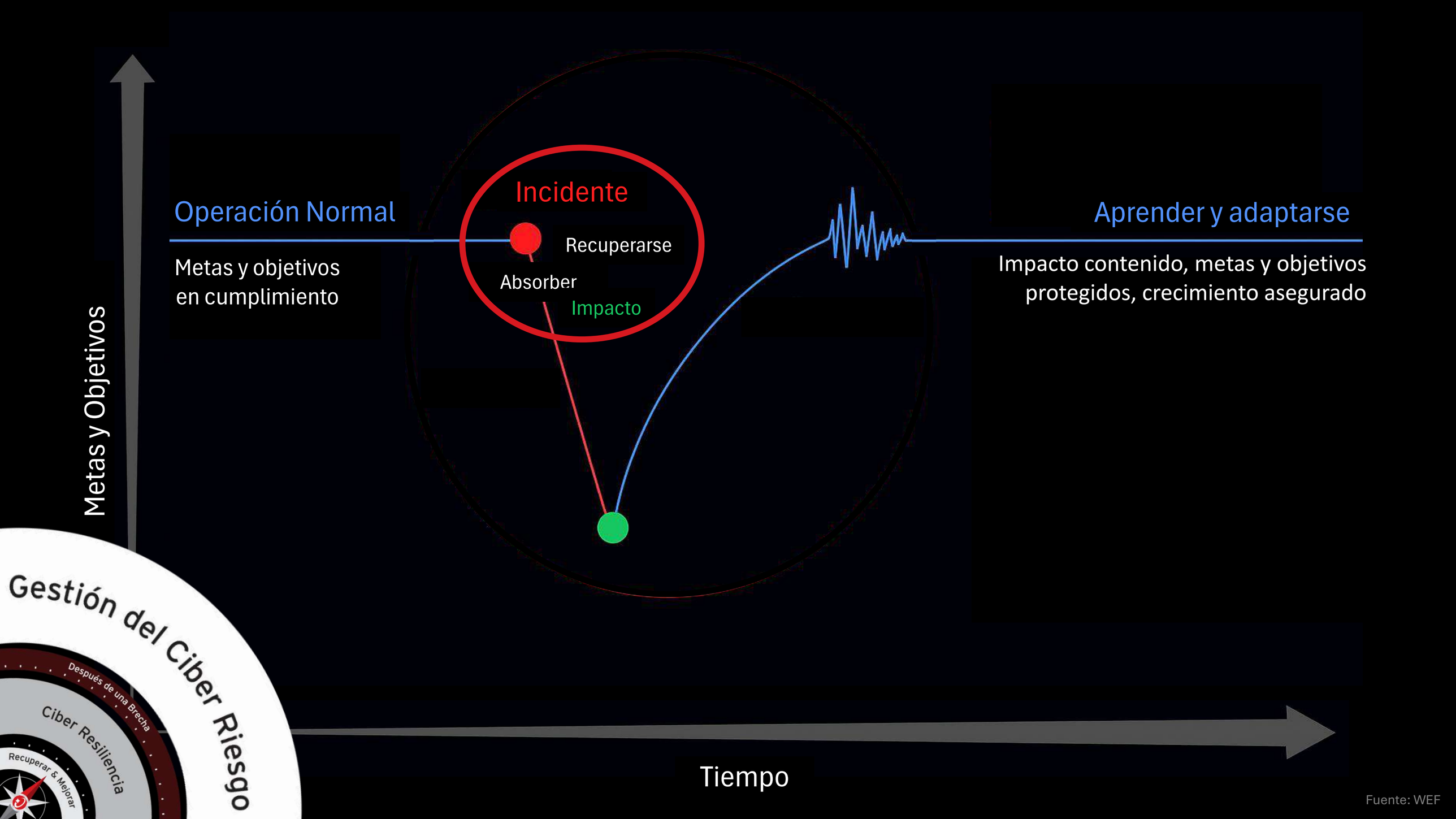
Fuente: WEF


Metas y Objetivos
Operación Normal
Metas y objetivos
en cumplimiento
Incidente
Absorber
Impacto
Recuperarse
Aprender y adaptarse
Impacto contenido, metas y objetivos
protegidos, crecimiento asegurado
Tiempo
Gestión del Ciber Riesgo
Después de una Brecha
Ciber Resiliencia
Recuperar & Mejorar

Fuente: WEF


Operación Normal
Metas y objetivos en cumplimiento
Incidente
Absorber
Recuperarse
Impacto
Aprender y adaptarse
Impacto contenido, metas y objetivos protegidos, crecimiento asegurado
Metas y Objetivos
Tiempo
Gestión del Ciber Riesgo
Después de una Brecha
Ciber Resiliencia
Recuperar & Mejorar

Fuente: WEF


Metas y Objetivos
Operación Normal
Metas y objetivos
en cumplimiento
Incidente
Recuperarse
Absorber
Impacto
Aprender y adaptarse
Impacto contenido, metas y objetivos
protegidos, crecimiento asegurado
Tiempo
Gestión del Ciber Riesgo
Después de una Brecha
Ciber Resiliencia
Recuperar & Mejorar

Fuente: WEF

SOC

SecOps

XDR & ASIEM

CROC

CyberRiskOps

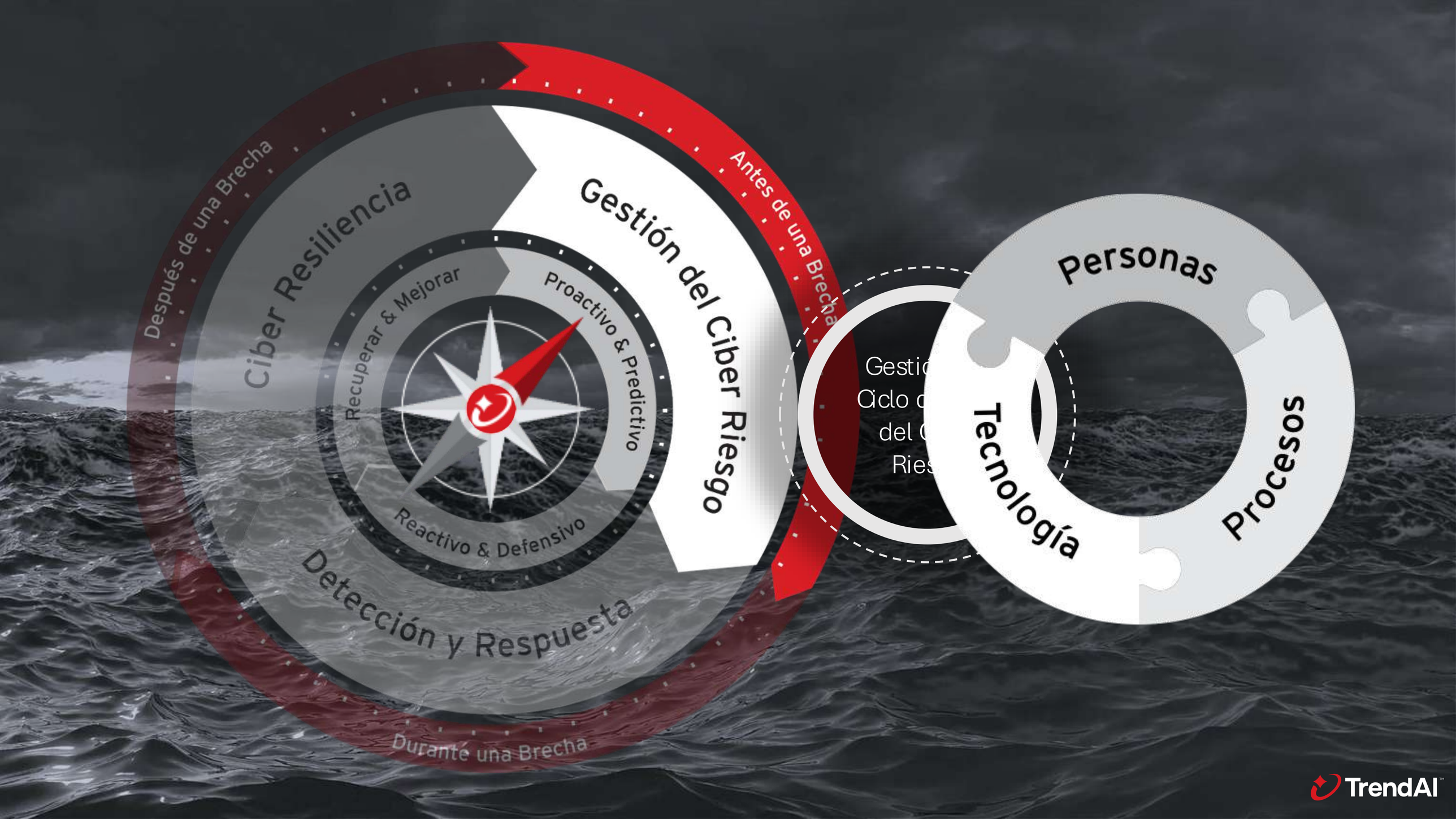
CREM

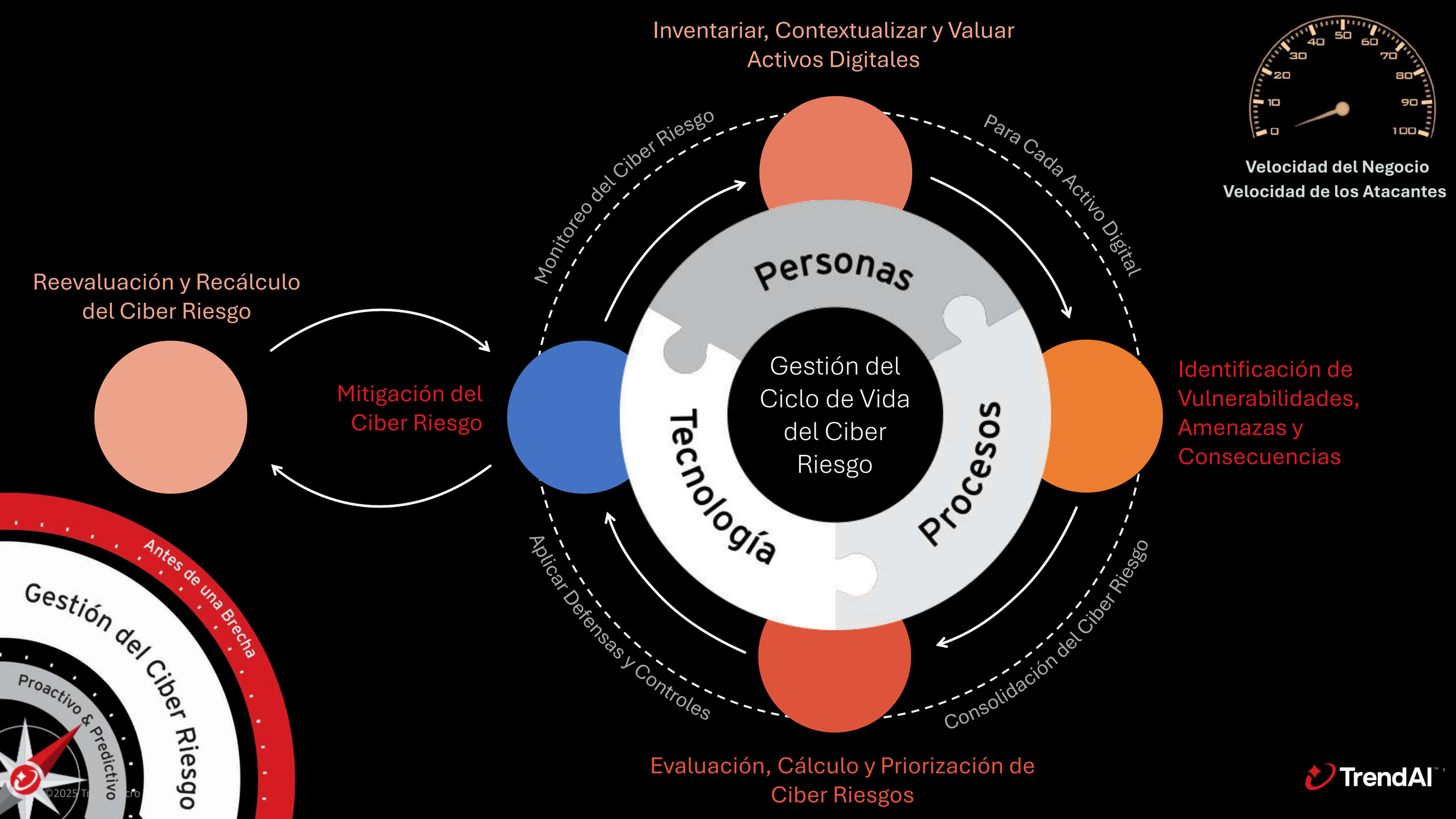
TrendAI™

Cada ciber riesgo. Cada señal. Defensa continua.

La exposición y los ciber riesgos informan la priorización de las detecciones

Los incidentes e investigaciones repriorizan las exposiciones y las medidas de prevención


Después de una Brecha
Ciber Resiliencia
Recuperar & Mejorar
Gestión del Ciber Riesgo
Antes de una Brecha
Proactivo & Predictivo
Reactivo & Defensivo
Detección y Respuesta
Durante una Brecha
Personas
Tecnología
Procesos
TrendAI


Inventariar, Contextualizar y Valuar Activos Digitales
Velocidad del Negocio
Velocidad de los Atacantes
Monitoreo del Ciber Riesgo
Para Cada Activo Digital
Reevaluación y Recálculo del Ciber Riesgo
Mitigación del Ciber Riesgo
Personas
Tecnología
Procesos
Gestión del Ciclo de Vida del Ciber Riesgo
Identificación de Vulnerabilidades, Amenazas y Consecuencias
Aplicar Defensas y Controles
Consolidación del Ciber Riesgo
Evaluación, Cálculo y Priorización de Ciber Riesgos
Gestión del Ciber Riesgo
Antes de una Brecha
Proactivo & Predictivo
TrendAI

Identificación de Vulnerabilidades, Amenazas y Consecuencias

“Lo que no se define
no se puede medir.
Lo que no se mide
no se puede mejorar.
Lo que no se mejora
se degrada siempre”

 ©2025 Trend Micro Inc.

Gracias

TrendAI™. AI Fearlessly.

Mérida 2026 ·

TrendAI