

#STICPANAMÁ

V JORNADAS STIC & CONGRESO ROOTED_— CON

CAPÍTULO PANAMÁ

COMPROMISO
INTERNACIONAL POR LA
CIBERSEGURIDAD **GLOBAL**



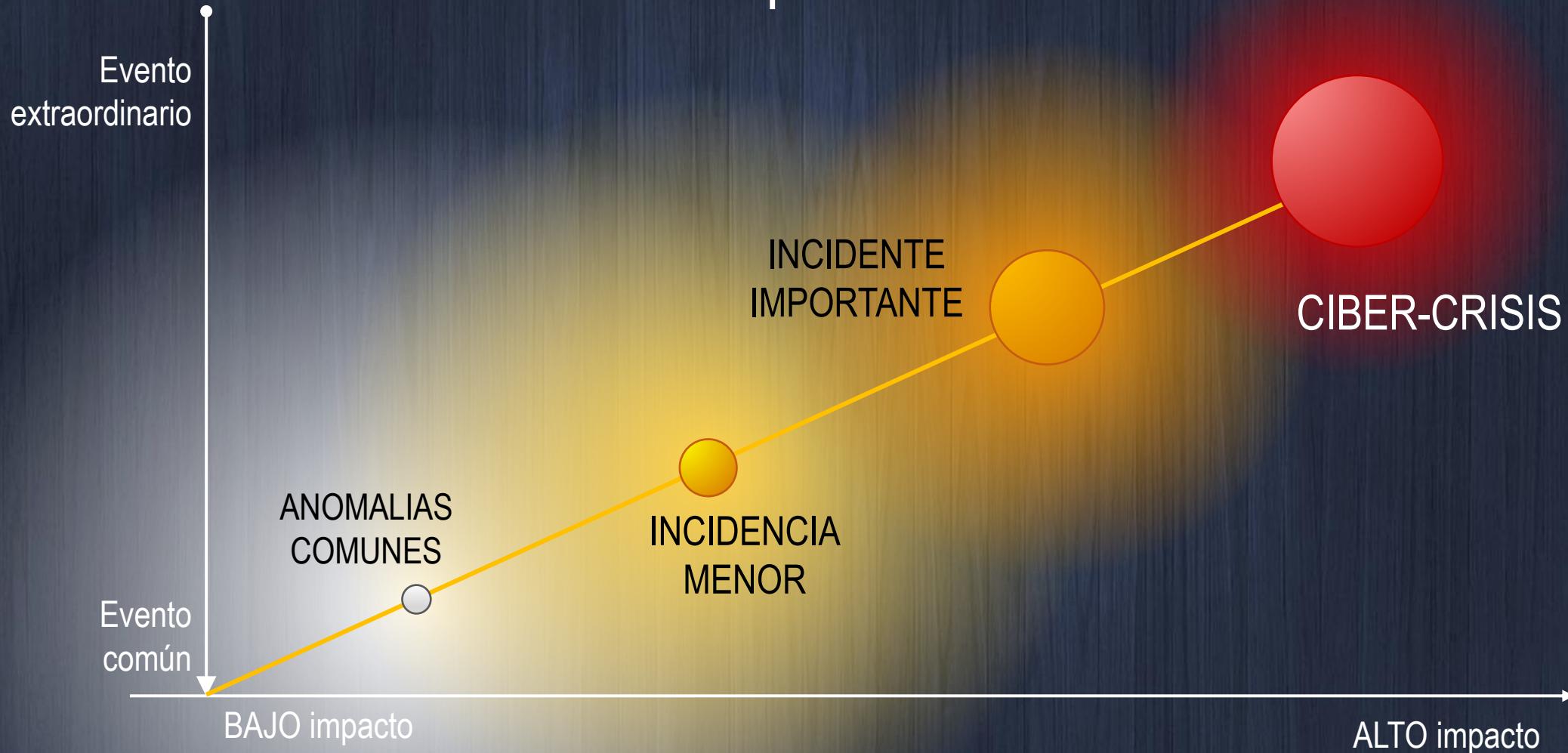
SHALL WE
PLAY A GAME,
JEFES?



trc



Roadmap to crisis



Una ciber crisis genera efectos ...



Bienes y Servicios



Reputación



Colectivos

ECONÓMICOS, financieros, profesionales, judiciales, organizativos, regulatorios, legales, **REPUTACIONALES**, de RRHH, **MEDIATICOS**, ... y también técnicos.

Las crisis afrontan riesgos ... del negocio
Requieren la implicación **de la directiva**



La gestión 'TRADICIONAL'



Del ransomware a la estafa del CEO



RESPONSABILIDADES de la DIRECTIVA

- Entender los riesgos
- Aprobar las medidas para la gestión de los ciber riesgos
- Supervisar que se apliquen correctamente
- Formación especializada en ciberseguridad (para la directiva y para los empleados)
- Asumir su responsabilidad al decidir la estrategia → definir su '**apetito de riesgo**'

CONSECUENCIAS en NIS2

- Responsabilidad personal por el incumplimiento
- Inhabilitación temporal para ejercer funciones directivas



- Hoy, la respuesta a una ciber-crisis requiere que el Equipo de respuesta a Incidentes (ERI) y la 'Suite-C' funcionen de forma coordinada y bien entrenada, **como un único equipo**.

Cometidos de la dirección



- **CEO**: Debe empujar estratégicamente y tener interlocución directa con el CISO (CRO, CSO, ...)
- **CHRO**: Debe contribuir a la formación y adopción de una cultura resiliente, con seguimientos constantes.
- **COO/CBO**: Deben ser supervisados de forma constante por su implicación directa en la seguridad corporativa.
- **CFO/CIAO/CLO**: Deben dotar del presupuesto adecuado y auditar el trabajo de las primeras líneas de defensa.
- **CIO/CTO**: Como primera línea de defensa, son responsables de la ciberseguridad de los sistemas que operan y deben tener una interlocución constante (y amistosa) con ciberseguridad.
- **CISO**: Debe diseñar, supervisar y, en muchos casos, operar

Características de las ciber crisis



- Intensidad de los impactos
- Ubicuidad de los ataques
- Possible propagación Global
- Incertidumbre a largo plazo
- Desconocimiento Técnico
- Duración muuuuyyyy larga

Se requiere TENER un plan y PROBAR el plan

Preparando una ciber crisis

Crisis Management



96% of directors are confident their board can guide the company through a crisis



Yet, **70%** have not participated in tabletop exercises



48% have not created a crisis management escalation policy

¿Cómo se afrontan? → con **PLANES**

- **DRP**: Plan de recuperación de desastres
- **BCP**: Plan de continuidad del negocio
- Plan de **comunicación**
- Plan de ... x



Yo: YA TENGO UN PLAN



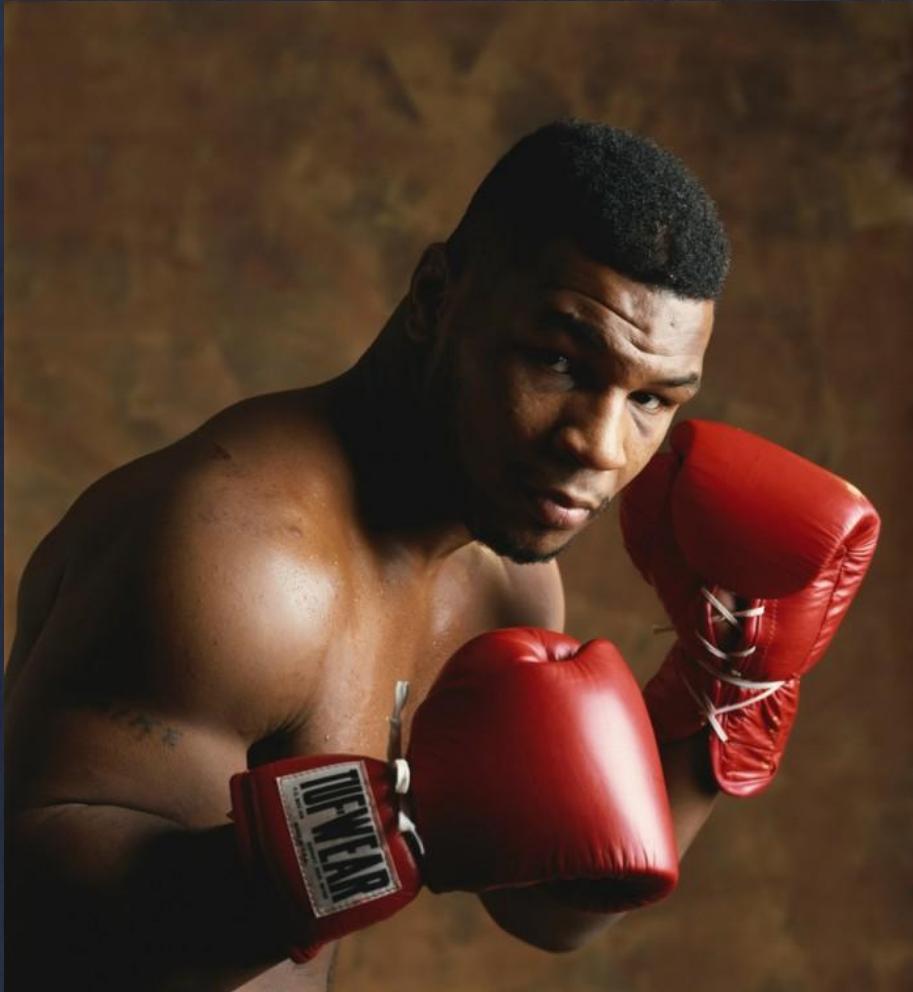
El plan :





Helmuth Karl Bernhard von Moltke
Mariscal de Campo Prusiano
(1800-1891)

“Ningún plan de batalla
sobrevive al primer contacto
con el enemigo”



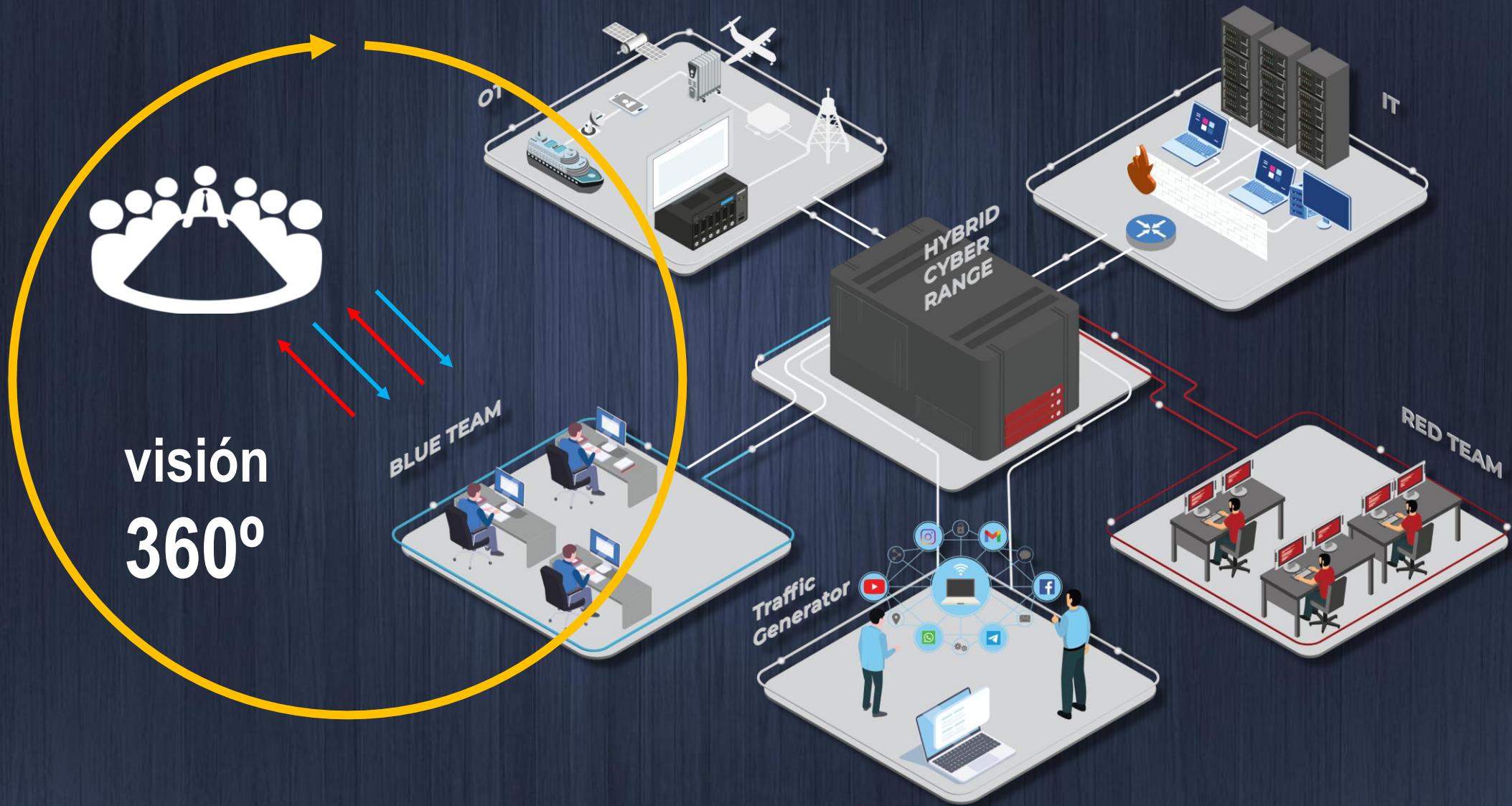
Michael Gerard «Mike» Tyson
Boxeador
Brooklyn NY, 1966

“Todo el mundo tiene un plan, ... hasta que le doy el primer puñetazo en la boca”



Los planes hay que **probarlos**

EX Gama top





CIBER EJERCICIOS: Simulaciones, Role Play, TTX



Entrenamiento para una gestión de crisis.





Entender los Table Top Exercises



“Esto no es real, no es así”

“Esto era cosa tuya”

“¿Me estás cuestionando?”

“¡Lo estas haciendo mal!”



Organizando un TTX: step by step



OBJETIVO



RESPALDO



MODALIDAD



ESCENARIO



JUGADORES



METRICAS



EVENTOS



PROGRAMACION



EJECUCION



MEJORA

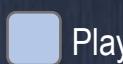
Organizando un TTX: step by step





El Escenario: malware, robo de datos, insider, ...

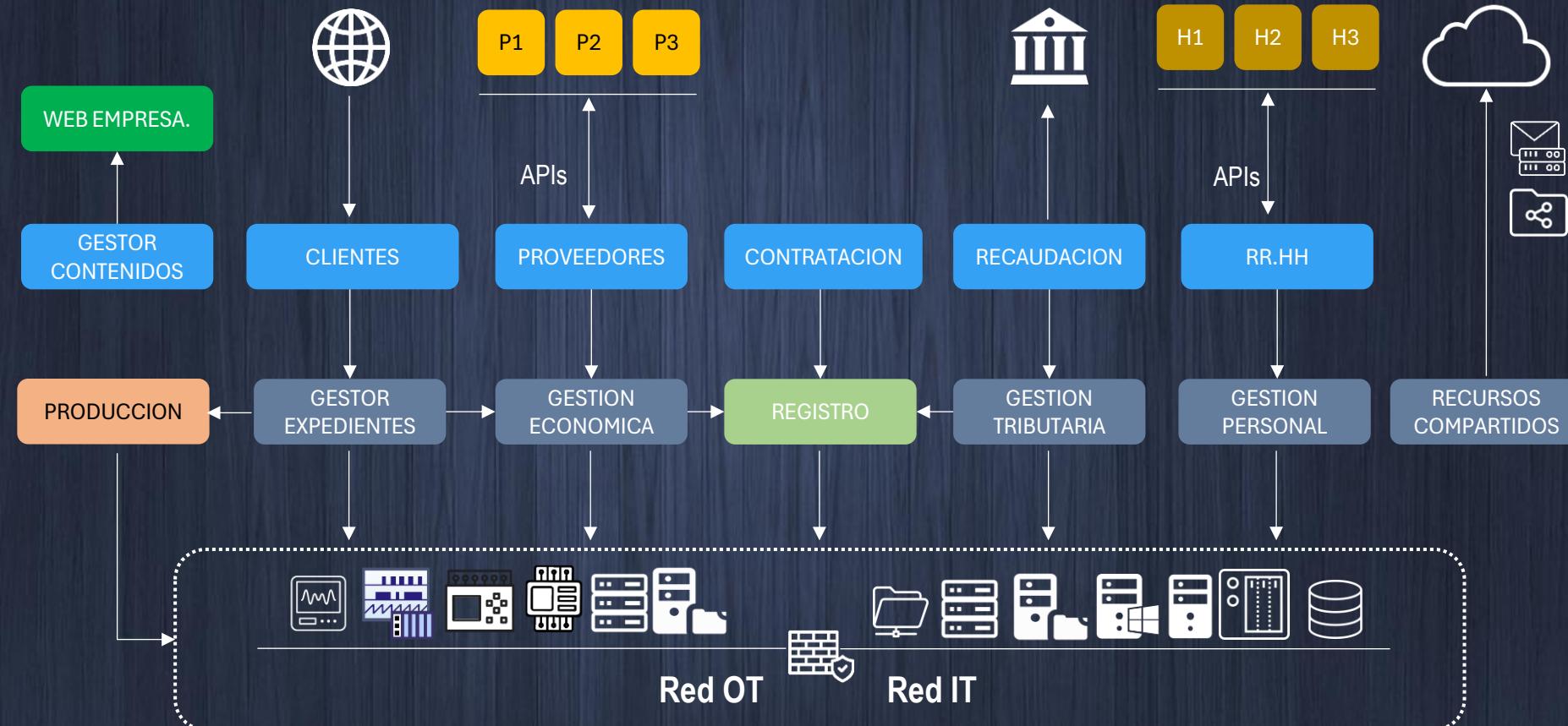




Players

- Resto: son actores que originan inycts, pero NO juegan

Mejor: Funciones y servicios





Story line principal + eventos



Story line principal + eventos

- Crisis de ciberseguridad
- Crisis en la reputación



Diseño de la Matriz de eventos

MODERADOR: No juega. Simula al profesional pone en juego la incidencia

JUGADOR: Destinatario de la incidencia.
No todos aparecerán. Las relaciones producirán interacciones entre equipos y roles.

Nº	TIME	INCIDENCIA	SENDER	RECEPTOR	envío	REACCION ESPERADA	Observaciones
1	YYMMDD 09:30	"Hola, nos llaman al CAU porque los equipos no arrancan,"	Jefe CAU	Dtor. Informática	llamada	Abrir ticket de incidente y escalar a Sistemas.	

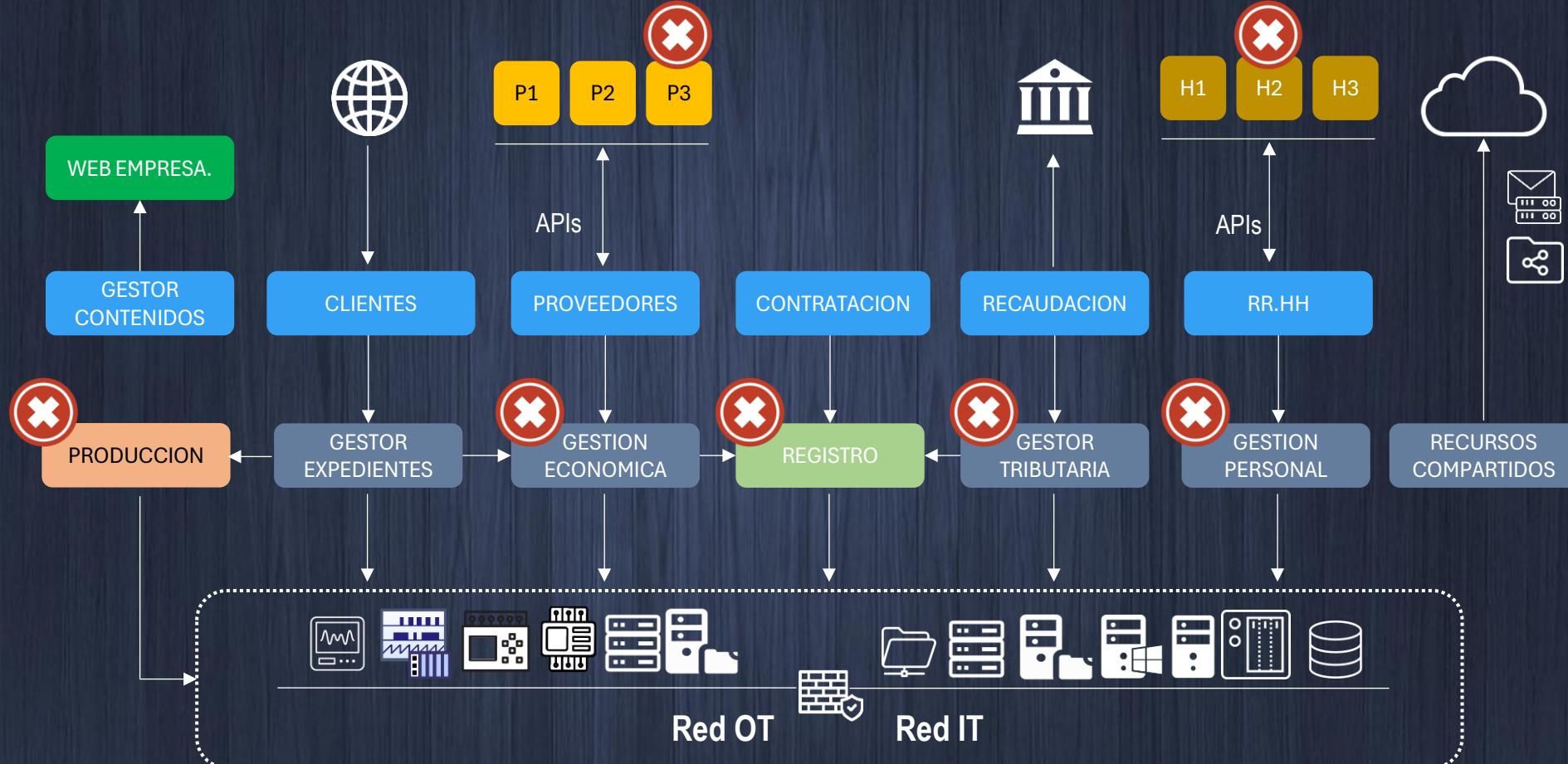
Una fila = Una inyección. Deben usar la terminología correcta para que el ejercicio sea realista.

Reacciones esperadas: deben estar ajustadas a los procedimientos existentes.



Leyenda: Iluminar filas para identificar roles, organizaciones, ...

Funciones y servicios





DEMO TIME

LAS LECCIONES MAS
VALIOSAS NO SON LAS
QUE SE ENSEÑAN
SON LAS QUE

SE EXPERIMENTAN



OpenEX

trc




DISTRIBUTION OF SCORE BY AUDIENCE (IN % OF EXPECTATIONS)

Dpto Operaciones

Dpto Comunicacion

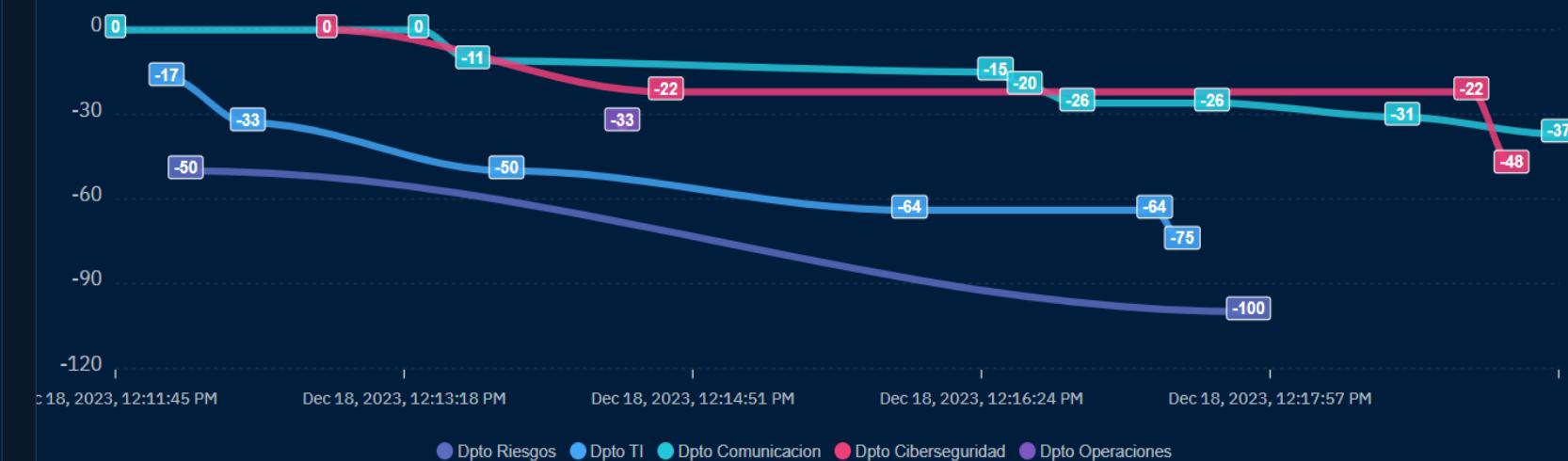
Dpto Ciberseguridad

Dpto TI

Dpto Riesgos



AUDIENCES SCORES OVER TIME (IN % OF EXPECTATIONS)



DISTRIBUTION OF TOTAL SCORE BY AUDIENCE

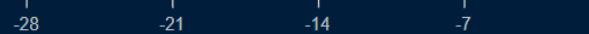
Dpto Operaciones

Dpto Ciberseguridad

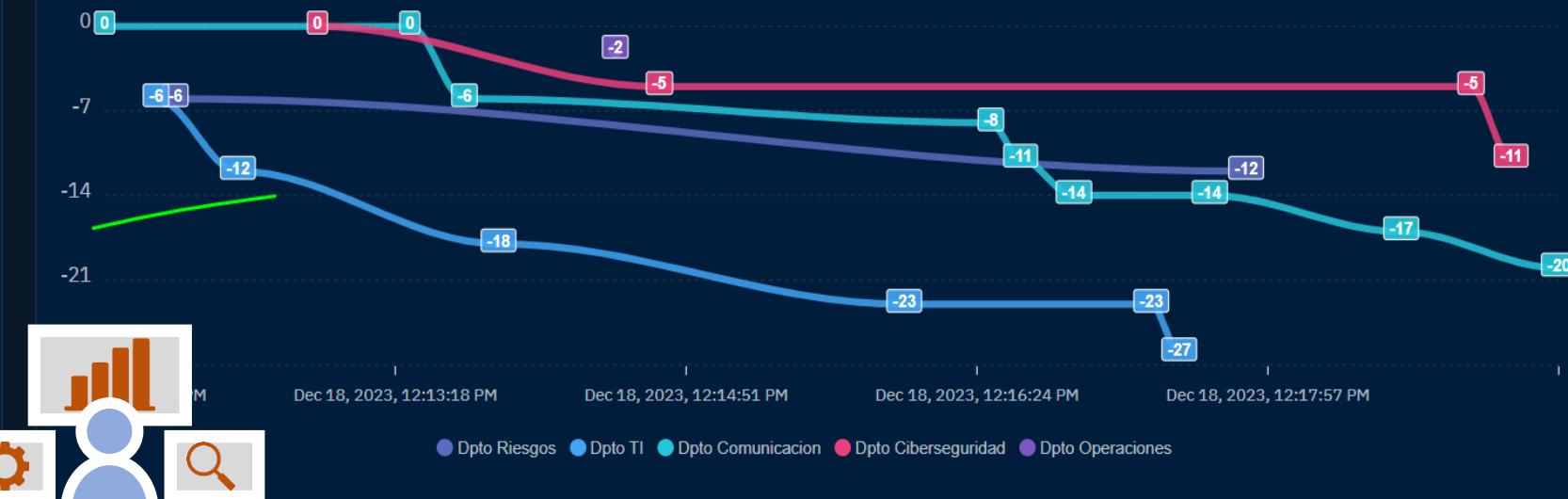
Dpto Riesgos

Dpto Comunicacion

Dpto TI



AUDIENCES SCORES OVER TIME





Cerrar Responder Responder a todos Reenviar

Correo

URGENTE! Ramsomware confirmado

De: GRC

Para: oceta ops oceta dco LEGAL GRC

Buenos días, por favor estamos activando el

Correo Contactos Agenda Tareas Maletín Preferencias

Cerrar Responder Responder a todos Reenviar Archivo Eliminar



TERPEL - Operaciones bloqueadas

De: OpenEx4

Para: oceta ops

Hola.

Imagino que sabes que no podemos trabajar con vosotros. La web está t preocupa que no finalicéis a tiempo el proyecto de financiación que tiene Eso acarrearía unos retrasos difíciles de asumir y las consiguientes pérdid cuando estaréis y tu garantía de que entregareis a tiempo.

Un cordial saludo

Dtor de Operaciones de TERPEL



Q

LAS PROVINCIAS

Suscríbete

Iniciar sesión



EUROCOPA2024

España Calendario Resultados y clasificación Dónde ver los partidos por TV



El cuadro definitivo de los octavos de la Eurocopa: terroríficos cruces para España con dos 'cocos' en el horizonte



Cuándo juega España los octavos de final: día, hora y televisión



Un georgiano lidera la lista de goleadores de la fase de grupos

Valencia prohibirá en 2028 la circulación de coches contaminantes por la ciudad

+ Arturo Checa y Álex Serrano López

El borrador de la ordenanza que ultima el Ayuntamiento fija 2027 como fecha en la que no podrán entrar en la capital conductores no empadronados y el año siguiente como veto para los residentes en la urbe

- Estas son las etiquetas de la DGT: de menos a más contaminantes

La inquietante llamada a Emergencias del sospechoso de los fuegos del Saler: «Sí, sí. Hay un incendio otra vez»

+ A. Rallo

Todo es política en el Consell de Cultura

+ Laura Garcés



¡¡ACME ciber atacada!!

Un virus informático ha devastado la red de ACME. Las operaciones de la compañía están paralizadas. Responsables técnicos no saben cuándo podrán restablecer el servicio.

Opinión

Pura vida

+ Ramón Palomar

Las almas perdidas

Belvedere

+ Pablo Salazar

Óscar Puente, alcalde de Valencia?

Como un aviador

+ Mikel Labastida

Poner distancia

A tope

+ Borja Rodríguez

Más bonito es reciclar si te premian

Sansón

La viñeta de Sansón

Más opinión >

Antes

ESTRATEGIA

- **OBJETIVOS**
- Alcance
- Metodología
- Participantes
- Fecha

DISEÑO

- ESCENARIO
- Eventos
- Incidentes, Inyecciones
- Fichas Informativas

Especificaciones

- Equipo y condicionantes
- Identificación de actores

Durante

HABLAR Y CAPACITAR

Después

DEBRIEFING

- Recopilación de información:
 - frustraciones causadas
 - y puntos fuertes observados
- Cuestionario de evaluación

INFORME FINAL

- Resumen ejecutivo + Informe Completo
- Identificar áreas de mejora y propuestas
- Sugerir un plan de acción para resolver brechas o debilidades
- Marca tareas, responsables y fechas de consecución



Ciberconsejo: Prueba tus planes



Beneficios de la Simulación



- Mejorar el tratamiento y la **gestión del riesgo**
- Mejorar la eficacia en los **procesos** de gestión
- Optimizar los **costes** económicos frente a potenciales pérdidas
- Optimizar los **tiempos** de reacción y respuesta
- Mejorar el **Trabajo en equipo**: comunicación, coordinación, relaciones, ...

Key Notes



1. Juegas como entrenas → **entrena** como quieres jugar
2. La crisis no es evitable, pero es **gestionable**
3. La gestión de la crisis se **planifica** y **se entrena**.

“Ya he pasado antes por ahí”

La práctica hace al maestro



Emilio Rico Ruiz

Security Advisor at **trc**



@Emilio_RR



Emilio Rico Ruiz



<https://github.com/3MlioRR/TXT-Panama>



#STICPANAMÁ

V JORNADAS STIC & CONGRESO ROOTED_— CON

CAPÍTULO PANAMÁ

COMPROMISO
INTERNACIONAL POR LA
CIBERSEGURIDAD GLOBAL



MUCHAS
GRACIAS