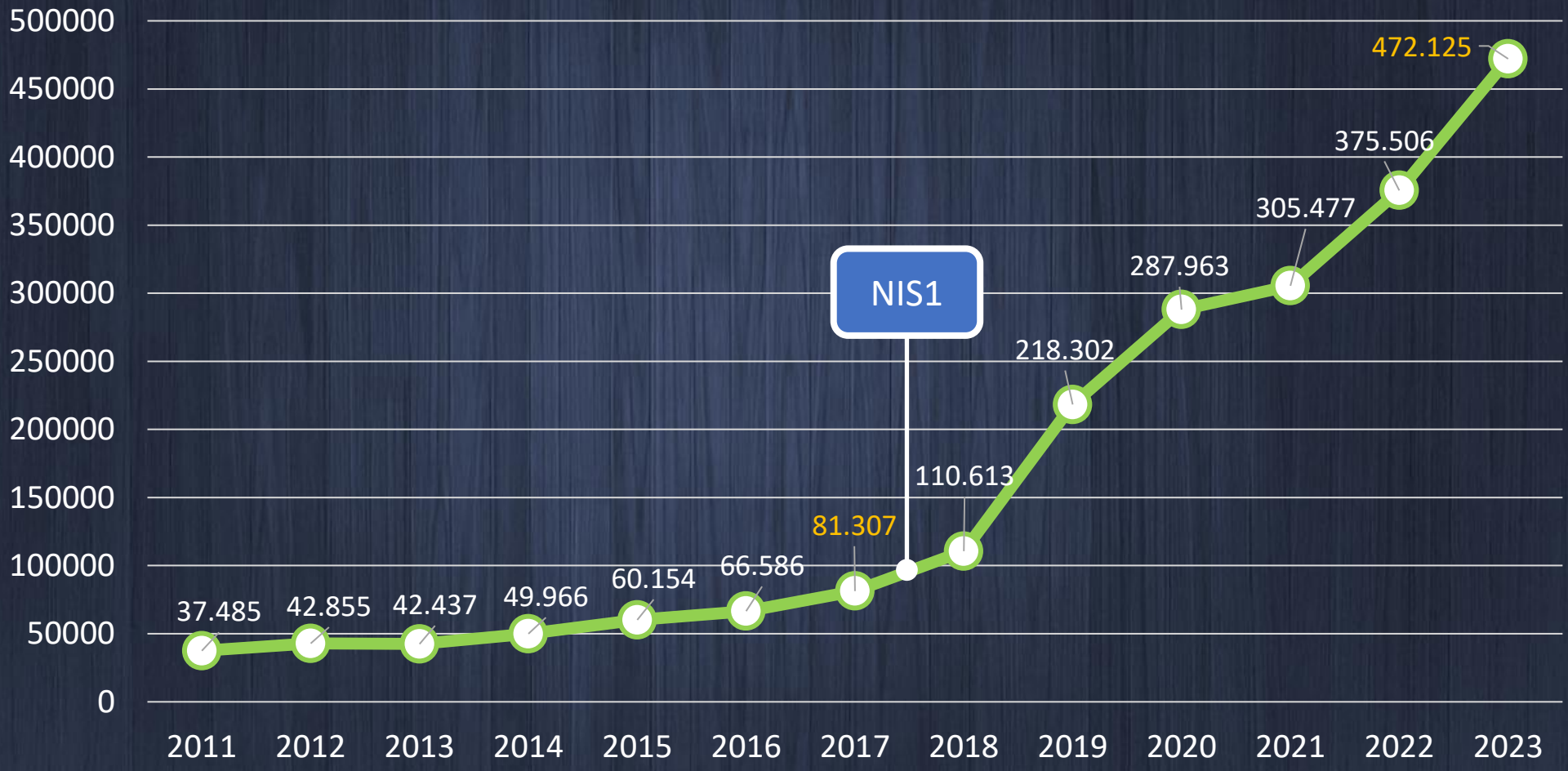

NIS2
¿Estamos preparados para gestionar un incidente de ciberseguridad?
trc

Aumentan un 13,5% los ciberdelitos, que ya suponen el 20% de las denuncias en España



Fuente: Ministerio del Interior

TENDENCIAS DEL CIBERCRIMEN EN ESPAÑA 2025 (Universidad de Cádiz)

Hechos denunciados por cibercriminalidad en las distintas CC.AA. en 2023

(Tasa por cada 100.000 hab.)

- País vasco: 1.259
- C. León: 1.225
- C. Madrid: 1.148
- C.F. Navarra: 1.112
- Cantabria: 1.014
  - Media total España: 982
- Cataluña: 963
- I. Baleares: 949
- Andalucía: 947
- Aragón: 908

NIS2: *Network and Information Security Directive 2*

Directiva de Seguridad de Redes y Sistemas de Información 2 (SRI2)

NIS2 tiene por objeto mejorar la seguridad de las redes y los sistemas de información en la UE, exigiendo a los operadores de infraestructuras críticas y servicios esenciales que apliquen las medidas de seguridad adecuadas y comuniquen cualquier incidente a las autoridades pertinentes.

CALENDARIO de APLICACIÓN

Enero 2023
El 17ENE empezó el periodo de transposición de NIS2 por parte de los estados miembros.

Octubre 2024
Los Estados miembros tienen hasta el 17·OCT·2024 para trasponer la Directiva NIS2.

Enero 2025
Los Estados miembros deben comunicar a la Comisión Europea el régimen sancionador aplicable

2025
Los Estados miembros determinarán qué entidades se consideran esenciales e importantes

Abril 2025
Los Estados miembros deben elaborar una lista de entidades esenciales e importantes, así como las que prestan servicios de nombres de dominio

2027
Revisión periódica del funcionamiento de la Directiva (informe antes del 17·OCT·2027 al Parlamento y al Consejo)

(*) La Directiva NIS2 ya es vinculante y, sin embargo, las empresas españolas aún no tienen un marco legislativo nacional claro que les permita adaptarse

SUJETOS OBLIGADOS

ESENCIALES
IMPORTANTES

+250 trabajadores
volumen anual +50 M€

https://nis2directive.eu/

El foco de NIS2:

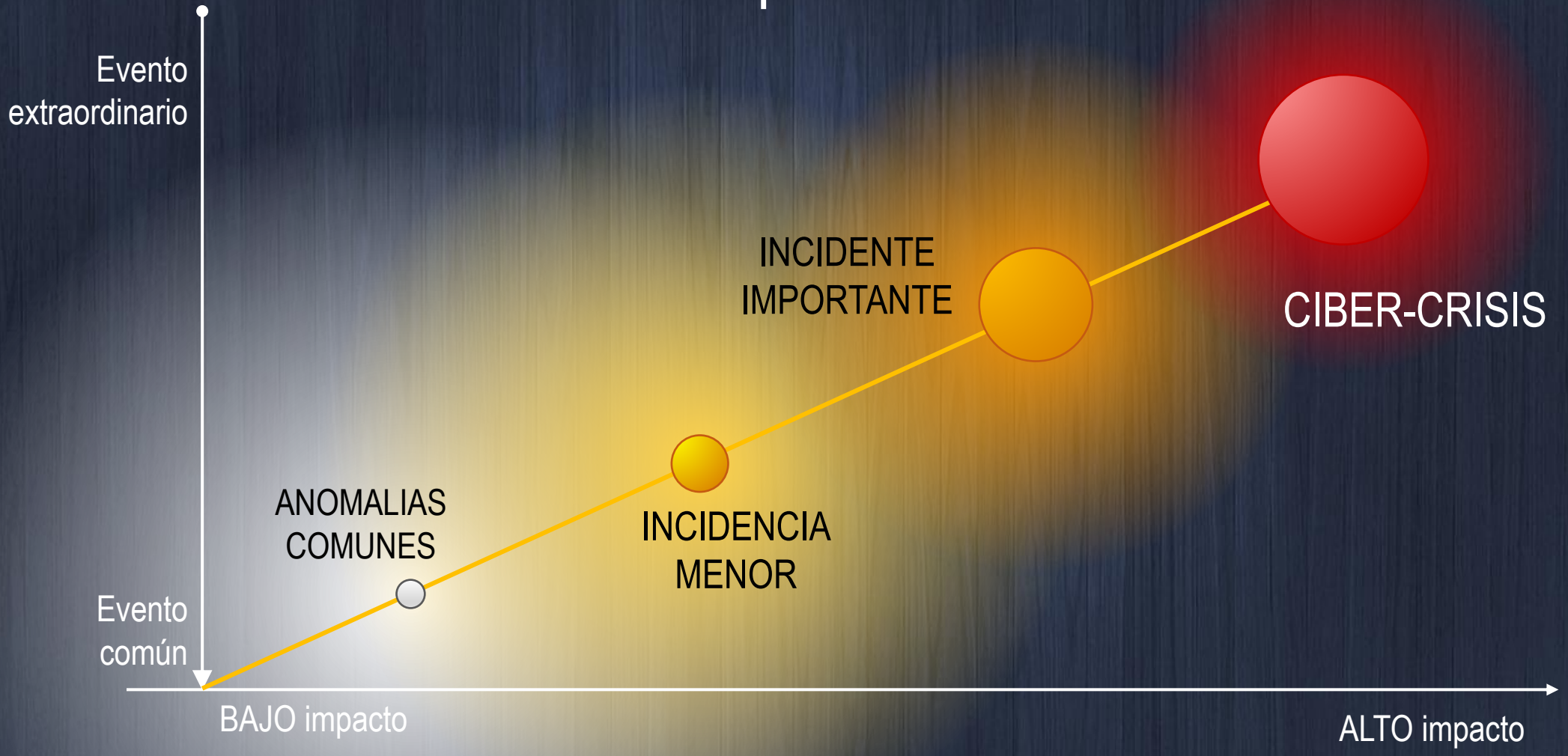
- Ampliación de sectores afectados y el tamaño de las entidades
- Requisitos más estrictos en gestión de riesgos.
- **Gobierno y responsabilidad de la DIRECCIÓN**
- Gestión de Incidentes y Notificaciones
- Cadena de suministro y productos certificados
- Mejora del intercambio de información (vulnerabilidades)
- Mayores sanciones por incumplimiento.
- Mayor cooperación entre países de la UE.

- Establece una red europea de soporte de crisis (EU-CYCLONe).
- Se apoya en otras nuevas directivas sectoriales (más ambiciosas y estrictas) como DORA (sector financiero) o CER para entidades críticas (operadores críticos)


BEEN PWNED

Oh!, oh!, tenemos un problema

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**

Características de las ciber crisis

- **Perdida de Servicios**
- Intensidad de los **impactos**
- Escalabilidad de los ataques
- Posible propagación Global
- Incertidumbre (según plazos)
- Complejidad de atribución
- Duración muuuuy larga (BCP🔑)
- Y sí, un carácter Técnico

Características de las ciber crisis (2)

Toda crisis implica

- Toma de decisiones bajo mucha presión.
- En poco tiempo.
- Probablemente con información incompleta.
- Diversos frentes en paralelo y con muchos grupos y personas interviniendo.
- Es difícil conciliar prioridades.
- Hay que entender los diferentes lenguajes.
- No existe suficiente conciencia sobre la importancia de la seguridad de la información.

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.
- **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
- **CFO/CIAO/CLO**: Deben dotar del presupuesto adecuado y auditar el trabajo de las primeras líneas de defensa.

Directrices a seguir

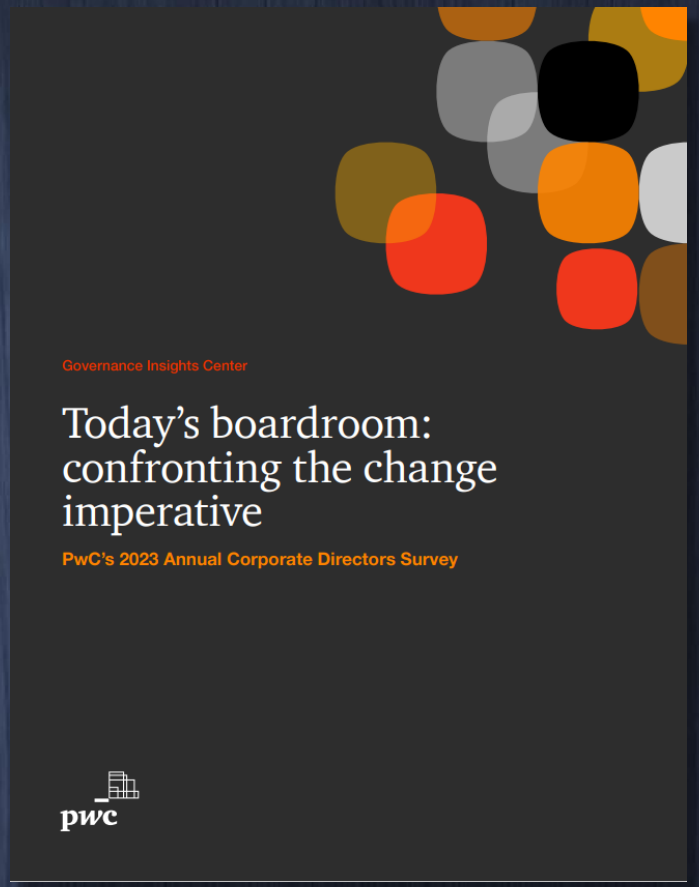
a) Identificar lo antes posible el evento que dispara la crisis, definiendo las soluciones alternativas y las respuestas apropiadas de forma rápida.
b) Tomar las decisiones de forma ágil, clara y efectiva.
c) Controlar la situación en el menor tiempo posible.
d) Actuar de manera ética, legal y responsable para proteger la reputación de la empresa.
e) Mantener una comunicación honesta y puntual, interna y externa, mediante un único portavoz.
f) Asegurar una adecuada interacción con clientes, proveedores, áreas de la empresa y con las autoridades a las que se deba informar y con las que se ha cooperar hasta su resolución.
g) Ejercer el liderazgo de forma efectiva en todos los niveles de la organización.
h) Asignar roles a las personas que tengan las competencias necesarias para enfrentarse de forma efectiva a la gestión de la crisis.
i) Registrar todas las decisiones y hechos para garantizar la trazabilidad.
j) Hacer un análisis postcrisis y las lecciones aprendidas aplicarlas para evitar recurrencias.

Establecer de una base de datos con toda la información necesaria para la gestión de crisis:

- Teléfonos de proveedores, socios, autoridades, clientes, … y procedimientos de notificación y escalado.
- Playbooks de respuesta técnica a incidentes (listado de proveedores especializados en DFIR con sus capacidades).
- Plan de comunicación ad-hoc

¿HAY MARGEN DE MEJORA?

Falta de ENTENDIMIENTO



Falta de ENTRENAMIENTO

Kaspersky-Speaks-your-Language-Report-spain_DEF.pdf
pwc-gic-acds-2023.pdf

Preparando una ciber crisis

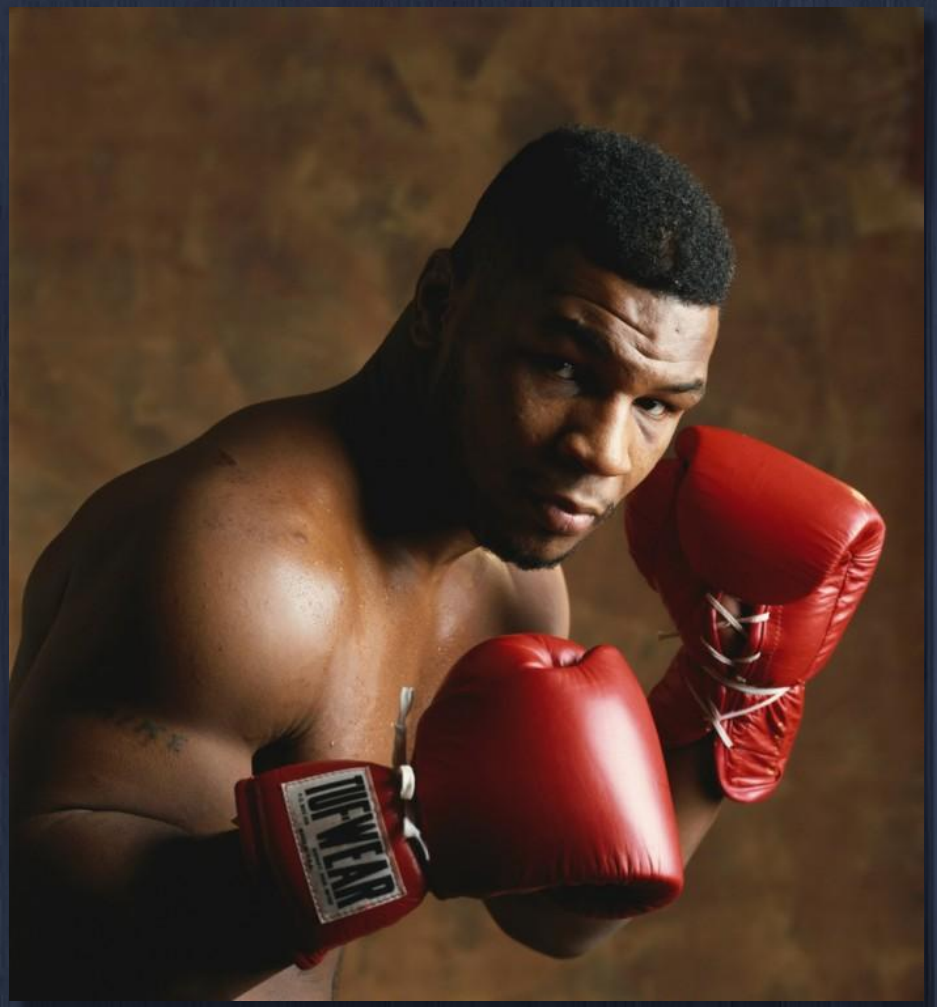
¿Cómo se afrontan? → con **PLANES**

1. DRP: Plan de recuperación de desastres
2. BCP: Plan de continuidad del negocio
3. Plan de comunicación
4. Plan de … x

Pero los planes hay que **probarlos**

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

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



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

Michael Gerard «Mike» Tyson
Boxeador
Brooklyn NY, 1966

CIBER EJERCICIOS: Simulaciones, Role Play, TTX

THE MOST VALUABLE LESSONS ARENT TAUGHT. THEY'RE EXPERIENCED

"Ya he pasado antes por ahí"

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, …

CIBER EJERCICIOS: Simulaciones, Role Play, TTX

Entender los CIBER EJERCICIOS

“Esto no es real, no es así”

“¿Me estás cuestionando?”

“Esto era cosa tuya”

“¡Lo estas haciendo mal!”

¿Cómo respondemos a una ciber crisis?

Correo

Cansa
@Viejit

Correo Contactos Agenda Tareas Maletín Preferencias URG

Cerrar Responder Responder a todos Reenvi

URGENTE! Ramsomware confirmad

De: GRC

Para: oceta ops oceta dco LEGAL GRC

Buenos días, por favor estamos activando e

Correo Contactos Agenda Tareas Maletín Pre

Cerrar Responder Responder a todos Reenviar Archivo Elimin

TERPEL - Operaciones bloqueadas

De: OpenEx4

Para: oceta ops

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

Un cordial saludo
Dtor de Operaciones de TERPEL

terpel

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 cuando podrán restablece el servicio.

Opinión

Pura vida
Ramón Palomar
Las almas perdidas

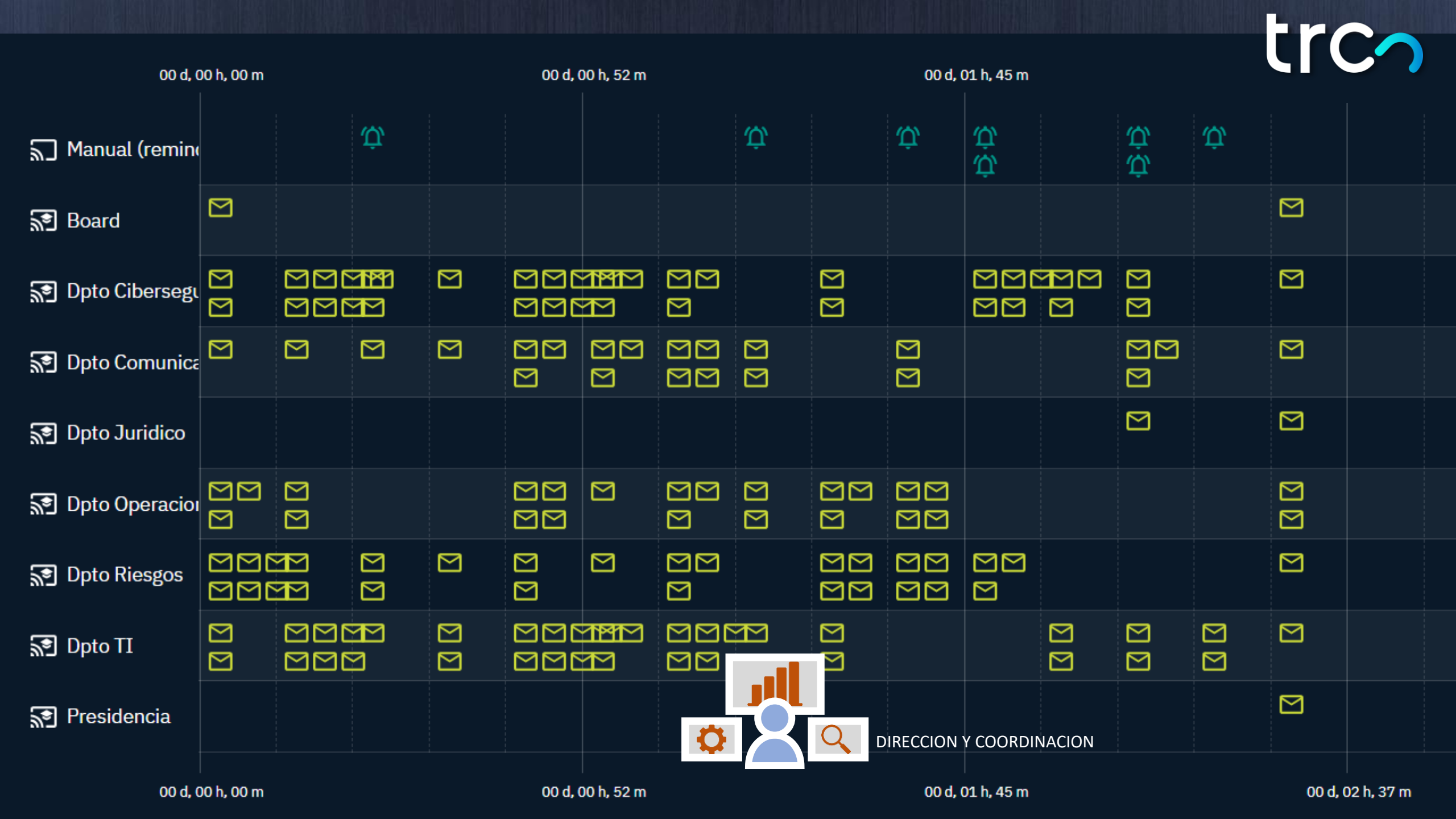
Belvedere
Pablo Salazar
Óscar Puente, ¿alcalde de Valencia?

Como un aviador
Mikel Labastida
Poner distancia

A tope
Borja Rodríguez
Más bonito es reciclar si te premian

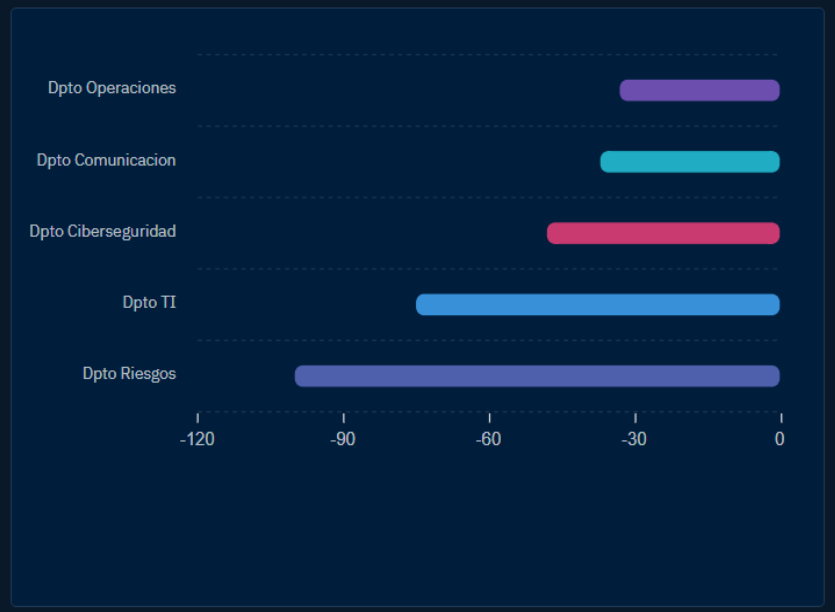
Sansón
La viñeta de Sansón

Más opinión >

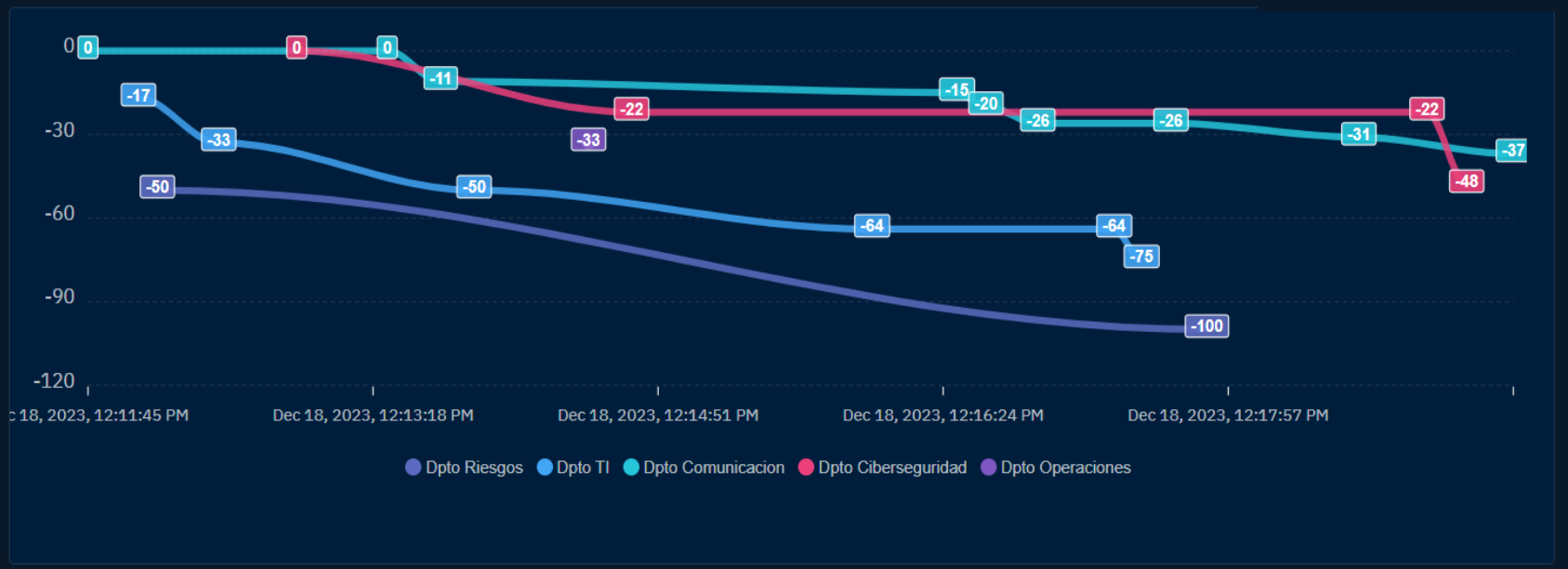

00 d, 00 h, 00 m
00 d, 00 h, 52 m
00 d, 01 h, 45 m
Manual (remin
Board
Dpto Ciberseg
Dpto Comunica
Dpto Juridico
Dpto Operacio
Dpto Riesgos
Dpto TI
Presidencia
DIRECCION Y COORDINACION
00 d, 00 h, 00 m
00 d, 00 h, 52 m
00 d, 01 h, 45 m
00 d, 02 h, 37 m

Exercise results

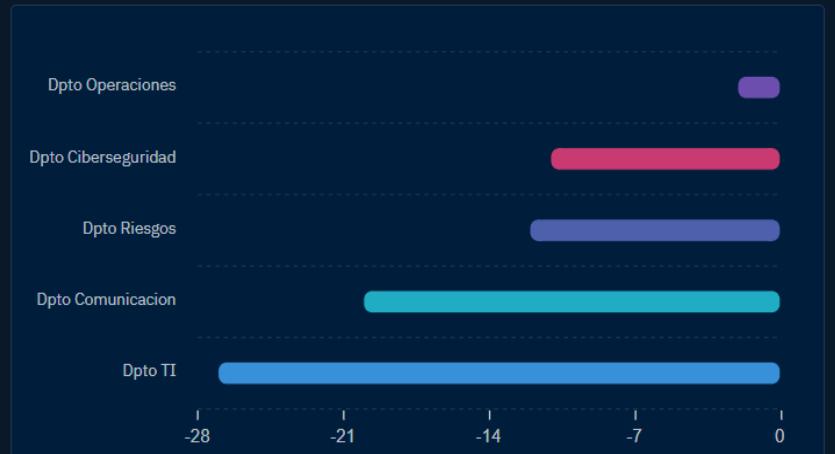
DISTRIBUTION OF SCORE BY AUDIENCE (IN % OF EXPECTATIONS)



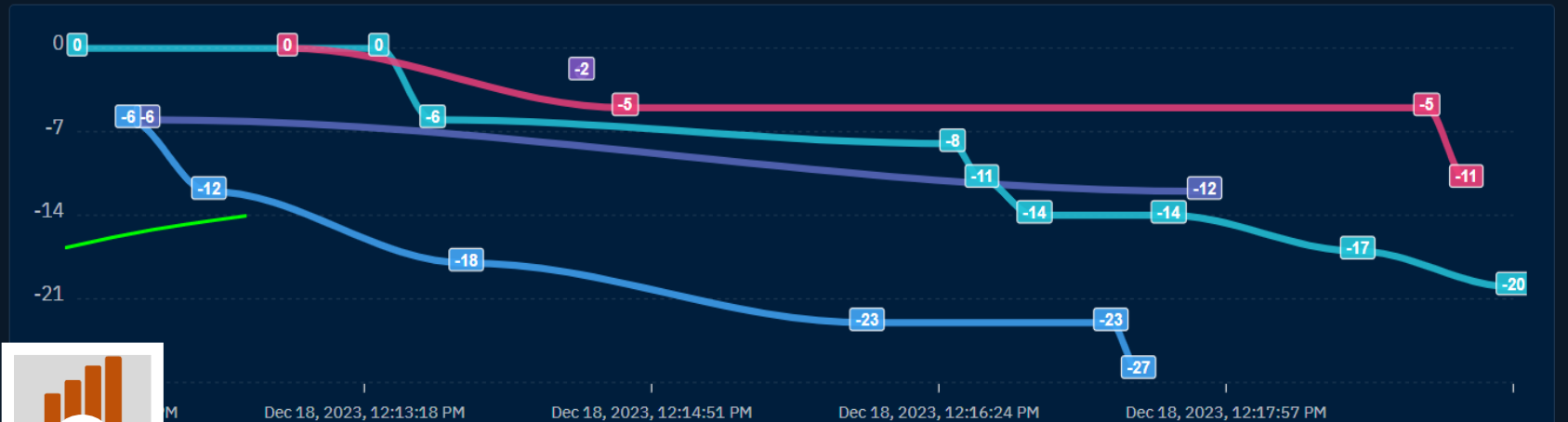
AUDIENCES SCORES OVER TIME (IN % OF EXPECTATIONS)



DISTRIBUTION OF TOTAL SCORE BY AUDIENCE



AUDIENCES SCORES OVER TIME



Ciberconsejo: Prueba tus planes

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**.
4. Se requiere un alto grado de concienciación del personal clave.

La práctica hace al maestro


Gracias