PLAY THE GAME

In previous episodes ....

(C1b3rWall2022)

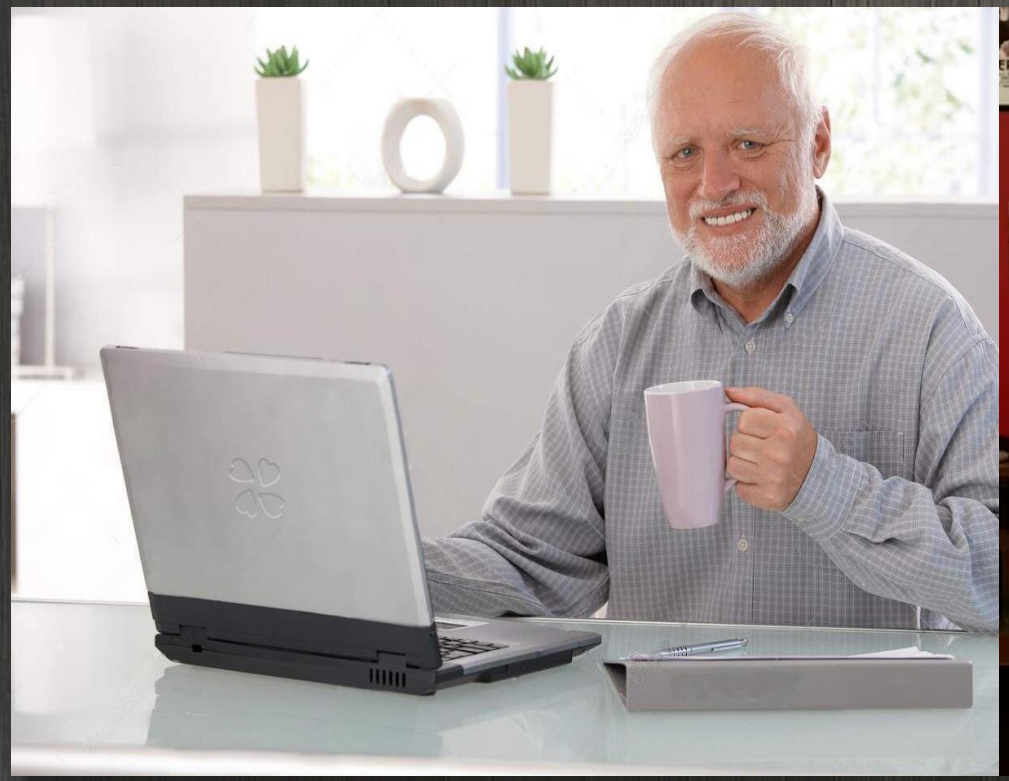
CIBER CONSEJO

NO SUBVALORAR LA AMENAZA !!

Houston, tenemos un problemilla

Roadmap to crisis

Yo: TENGO UN PLAN



El plan : 😂😂😂

“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

Características de las ciber crisis

- Intensidad de los impactos
- Ubicuidad de los ataques
- Posible propagación Global
- Incertidumbre a largo plazo
- Carácter Técnico
- Complejidad de atribución
- Duración muuuuyyyy larga

Se requiere PROBAR el plan → Haz EJERCICIOS

CIBER EJERCICIOS

- **Modelo**
  - Basado en debates
    - Seminario
    - Taller
    - Tabletop
    - Juego
  - Basado en Operaciones
    - Simulacro
    - Funcional
    - Escala Real
- **Enfoque**
  - Propósito
    - Concienciar
    - Iniciar
    - Mejorar
  - Evaluación
  - Fase Incidente
- **Difusión de resultados**
  - Público
  - Privado
- **Ámbito Participación**
  - Sector
    - Público
    - Privado
  - Geográfico
    - Nacional
    - Internacional
- **Sector Vertical**
  - AA.PP
  - Espacio
  - Nuclear
  - Químico
  - I+D
  - Agua
  - Defensa
  - Energía
  - Salud
  - TIC
  - Transporte
  - Financiero

Taxonomía

INCIBE → https://biblioteca.guardiacivil.es/bib/16139

Guía para ejercicios ISO 22398:2013

Manejar las ciber-crisis

Las consecuencias de un ciberataque son múltiples, generando efectos…

económicos, financieros, judiciales, regulatorios, legales, profesionales, organizativos, de recursos humanos, reputacionales, … etc, y también técnicos.

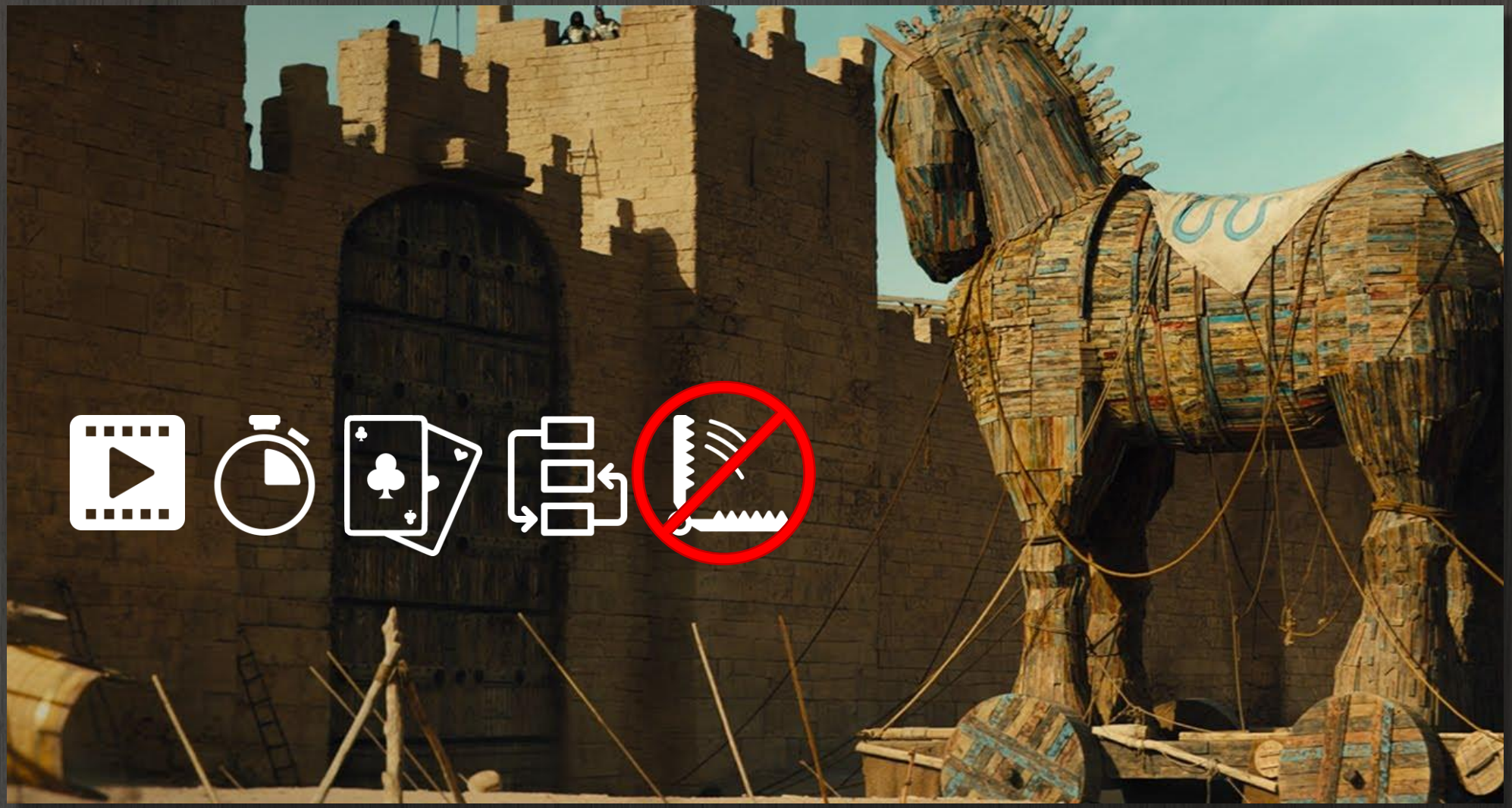
Sin olvidar que también pueden generar una fuerte presión mediática.

Se requiere la implicación de la directiva

Las crisis afrontan riesgos, riesgos …. del negocio

NIS2: introduce la responsabilidad de la alta dirección por el incumplimiento de las obligaciones de ciberseguridad

¿Qué es un Ciber-Ejercicio de gestión de crisis?



Atención, STOPPERS!!

"Esto no es real, no es así"

"¿Me estás cuestionando?"

"Esto no va conmigo"

"¿Y si lo hago mal?"

Organizando un TTX: step by step

OBJETIVO

RESPALDO

MODALIDAD

JUGADORES

METRICAS

ESCENARIO

EVENTOS

PROGRAMACION

EJECUCION

MEJORA

ESCENARIO (background)
EVENTOS
EVENTO 1
EVENTO 2
EVENTO 3
INCIDENTES
I1
I2
I3
I4
In
I5
INYECCIONES
1
2
3
4
5
NEWS
REALISTA

Fases y Actividades

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

Entregables: 1. 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.

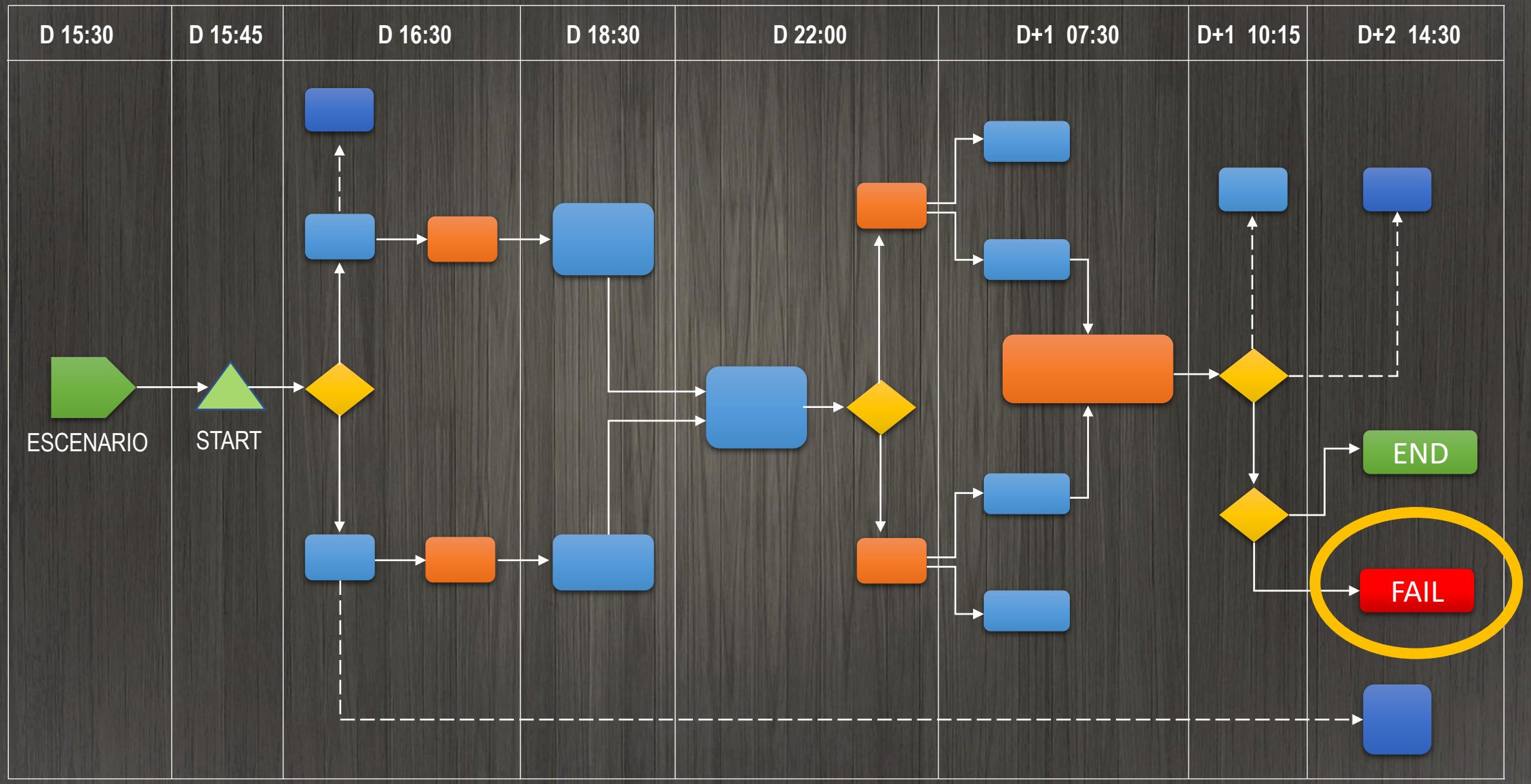
Nº	TIME	INCIDENCIA	SENDER	RECEPTOR	Modo Iny.	REACCION ESPERADA	Observaciones
1	YYMMDD **09:30**	"Hola, llamo porque mi equipo no arranca , …."	DIREX	C.A.U.	llamada	Abrir incidente y escalar a SOC	

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

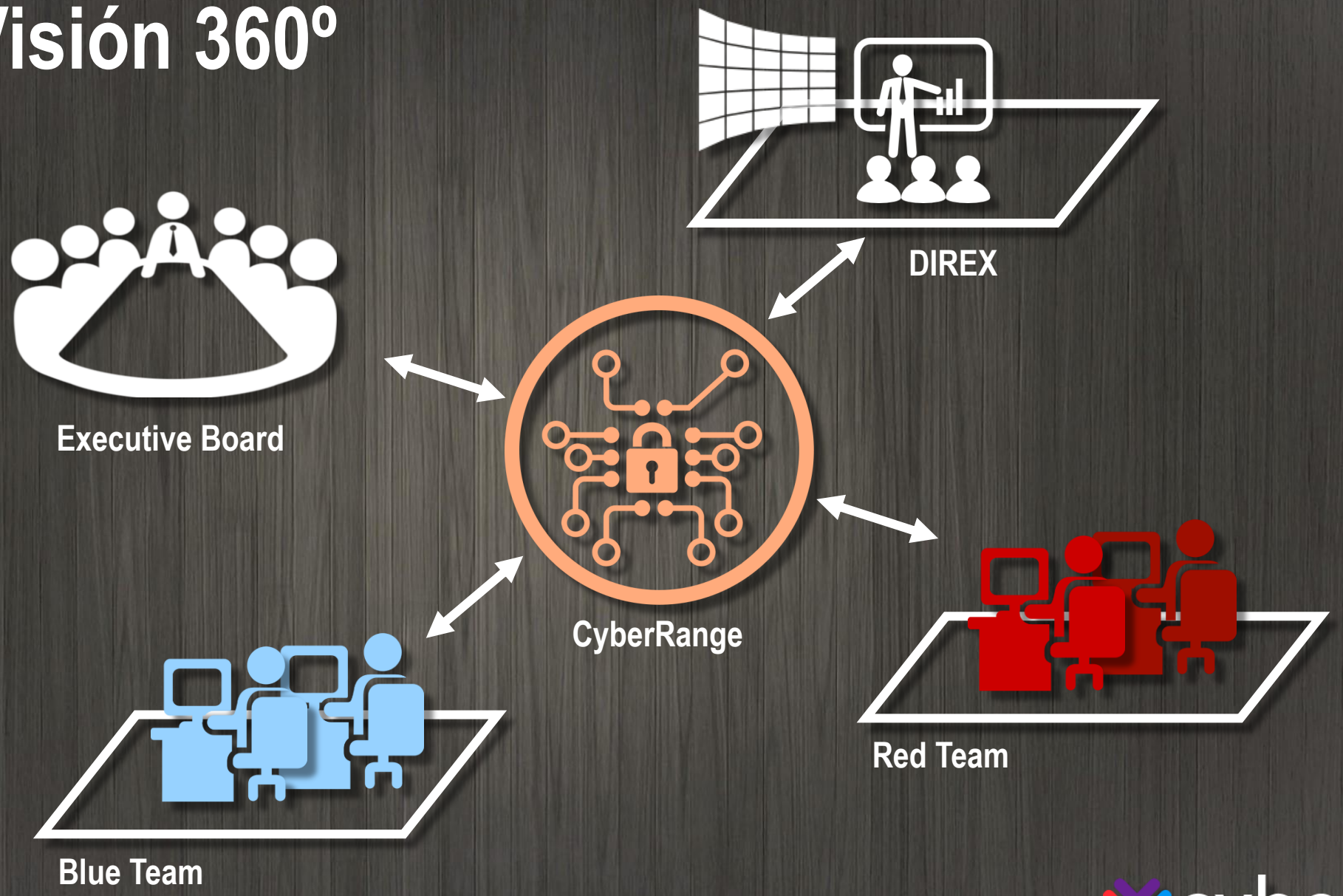
Reacciones esperadas: deben estar ajustadas a los procedimientos existentes.

Leyenda: Iluminar filas para identificar roles, organizaciones, …

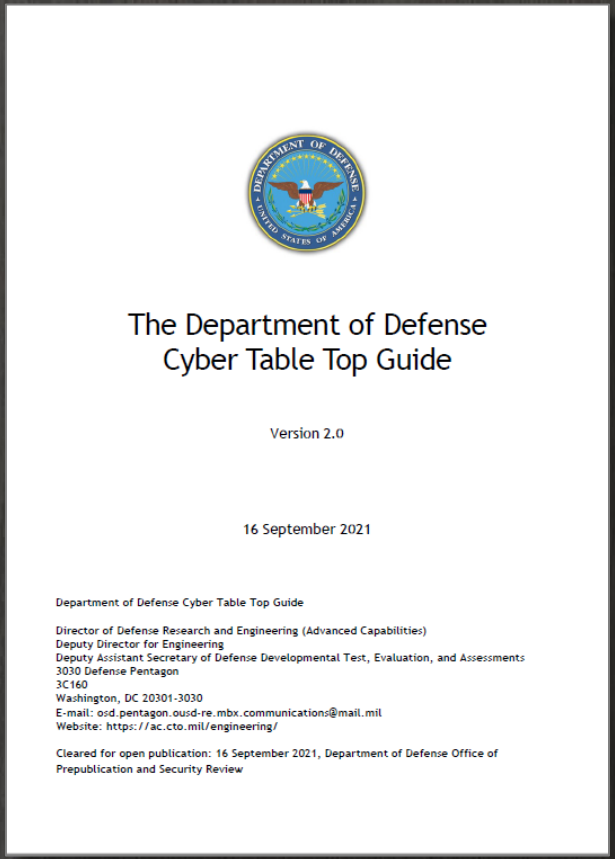
Entregables: 2. Programación del ejercicio



TTX: Visión 360º



Referencias CERTs / CSIRTs



The Department of Defense
Cyber Table Top Guide

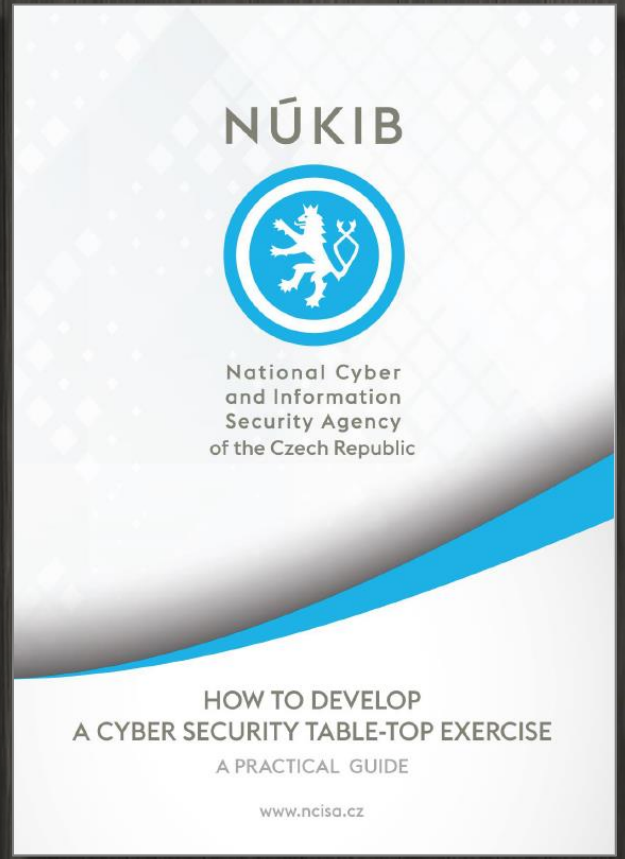
Version 2.0

16 September 2021

Department of Defense Cyber Table Top Guide

Director of Defense Research and Engineering (Advanced Capabilities)
Deputy Director for Engineering
Deputy Assistant Secretary of Defense Developmental Test, Evaluation, and Assessments
3030 Defense Pentagon
3C160
Washington, DC 20301-3030
E-mail: osd.pentagon.ousd-re.mbx.communications@mail.mil
Website: https://ac.cto.mil/engineering/

Cleared for open publication: 16 September 2021, Department of Defense Office of Prepublication and Security Review



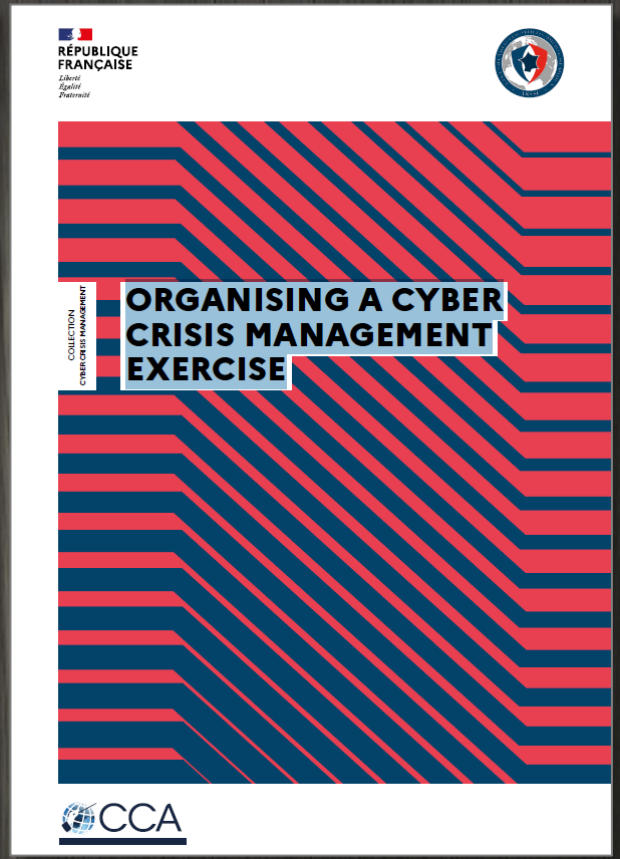
NÚKIB

National Cyber
and Information
Security Agency
of the Czech Republic

HOW TO DEVELOP
A CYBER SECURITY TABLE-TOP EXERCISE

A PRACTICAL GUIDE

www.ncisa.cz

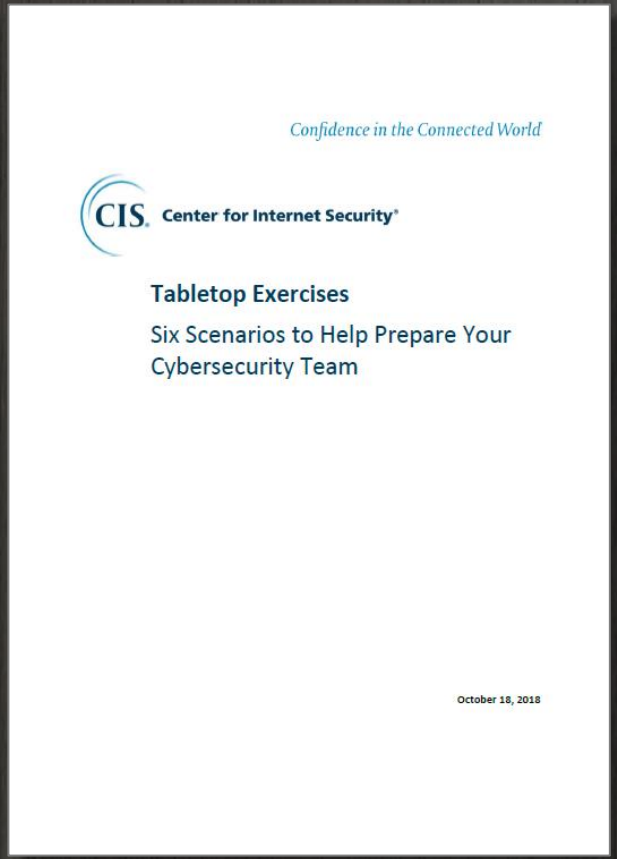


RÉPUBLIQUE
FRANÇAISE

COLLECTION
CYBER CRISIS MANAGEMENT

ORGANISING A CYBER
CRISIS MANAGEMENT
EXERCISE

CCA



Confidence in the Connected World

CIS Center for Internet Security®

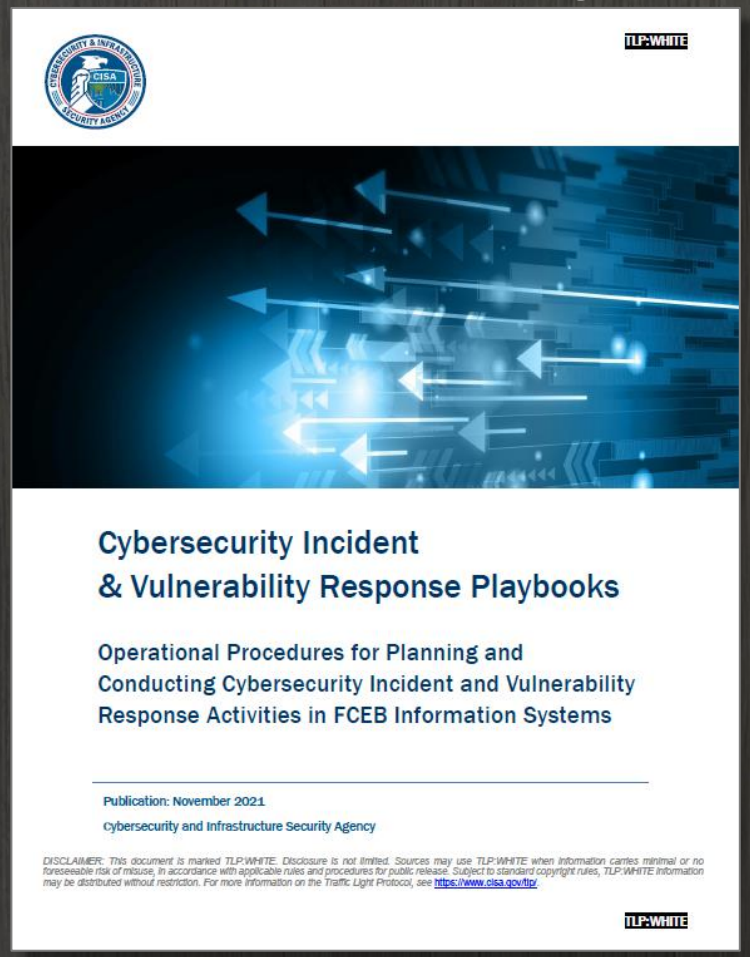
Tabletop Exercises

Six Scenarios to Help Prepare Your
Cybersecurity Team

October 18, 2018

https://ac.cto.mil/wp-content/uploads/2021/09/DoD-Cyber-Table-Top-Guide-v2.pdf
https://www.govcert.cz/download/manualy/N%C3%9AKIB-How-To-Develop-a-Cyber-Table-Top-Exercise.pdf
https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-organising_a_cyber_crisis_management_exercise-v1.0.pdf
https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team

Referencias Organismos



TLP:WHITE

Cybersecurity Incident
& Vulnerability Response Playbooks

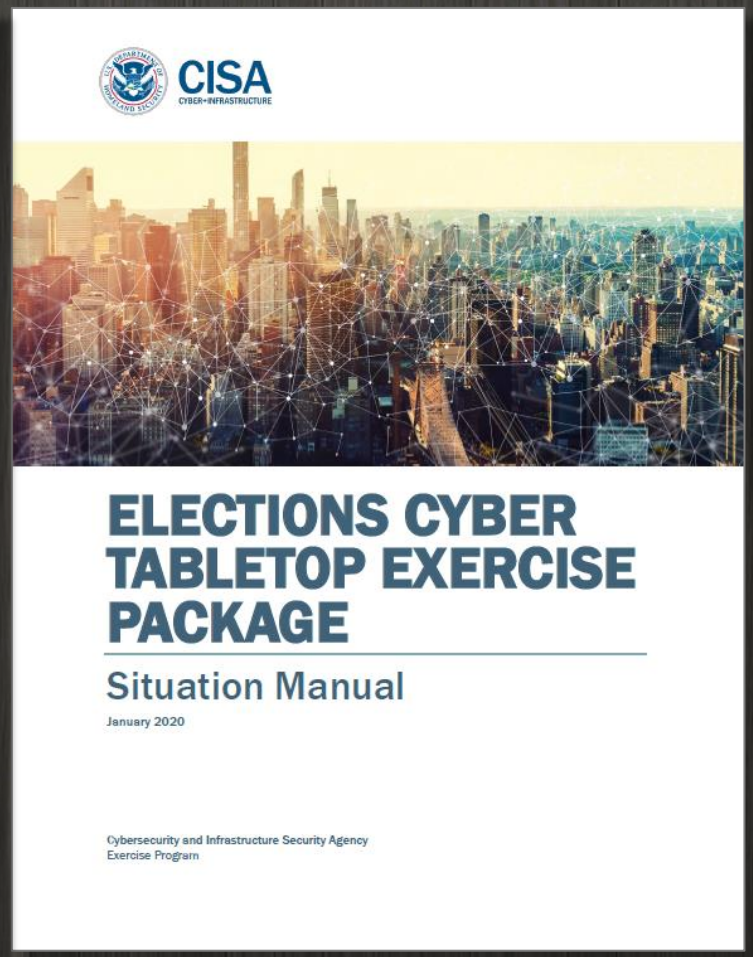
Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

Publication: November 2021

Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/

TLP:WHITE



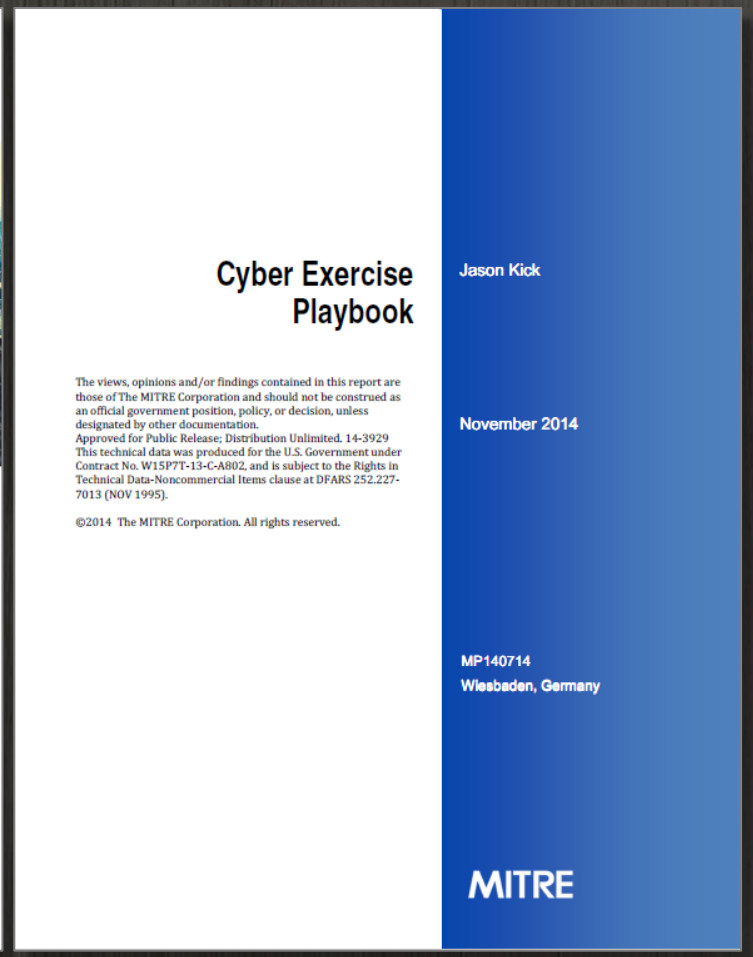
CISA
CYBER+INFRASTRUCTURE

ELECTIONS CYBER TABLETOP EXERCISE PACKAGE

Situation Manual

January 2020

Cybersecurity and Infrastructure Security Agency
Exercise Program



Cyber Exercise Playbook

Jason Kick

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.
Approved for Public Release; Distribution Unlimited. 14-3929
This technical data was produced for the U.S. Government under Contract No. W15P7T-13-C-A802, and is subject to the Rights in Technical Data-Noncommercial Items clause at DFARS 252.227-7013 (NOV 1995).

©2014 The MITRE Corporation. All rights reserved.

November 2014

MP140714
Wiesbaden, Germany

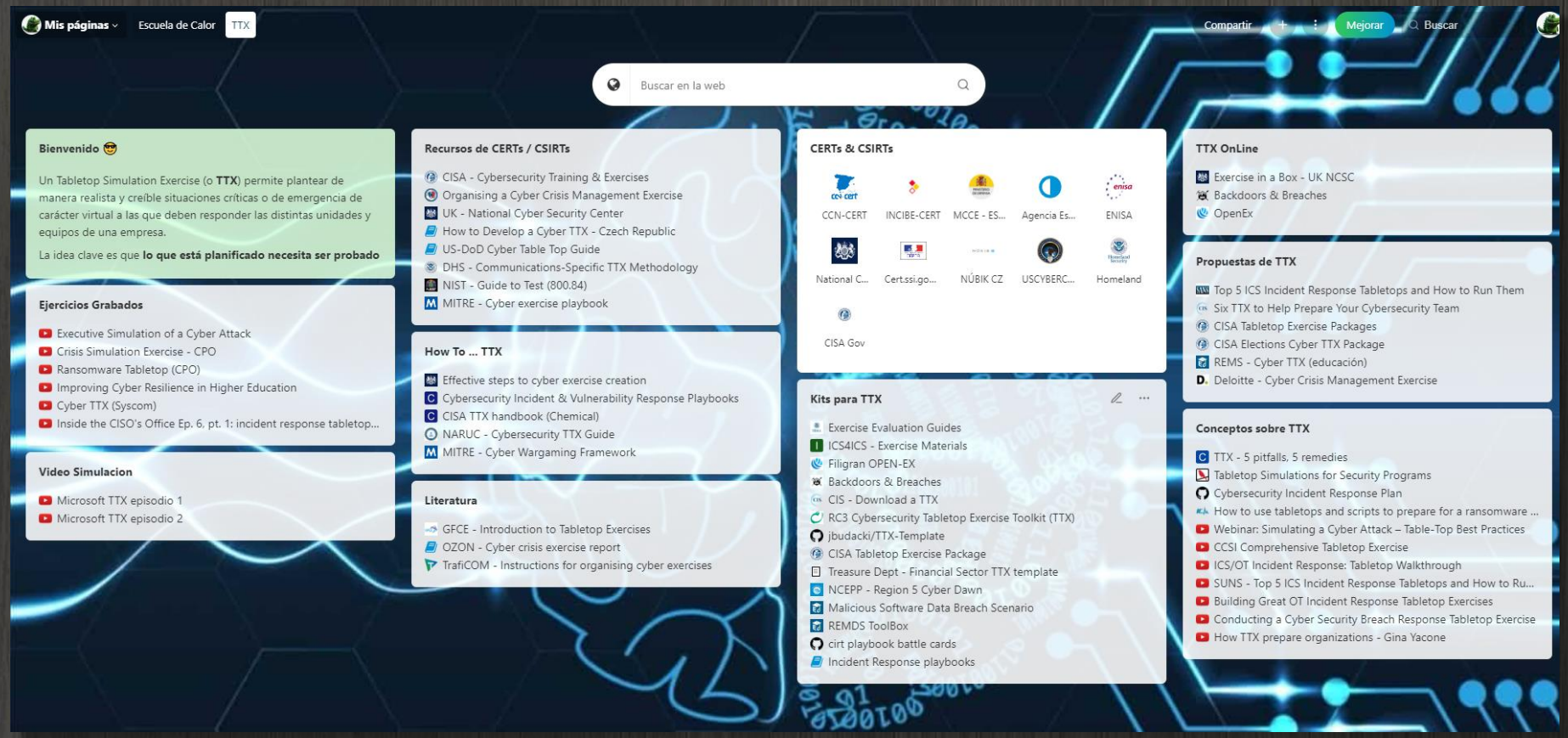
MITRE

https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios
https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Recursos OnLine

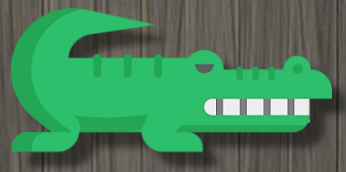
https://exerciseinabox.service.ncsc.gov.uk/
https://demo.openex.io/

Recursos ++



https://start.me/p/GEYLYm/ttx

TTX – DEMO & EX



Informe KASPERSKY: los altos directivos consideran que las ciberamenazas son un riesgo mayor para sus empresas que el empeoramiento de la economía, pero son incapaces de priorizar la protección frente a este tipo de ataques al no comprender la terminología utilizada en ciberseguridad.

https://media.kasperskydaily.com/wp-content/uploads/sites/88/2023/05/30114918/Kaspersky-Speaks-your-Language-Report-spain_DEF.pdf

Ciberconsejo 1: Practica y prueba tus planes

Ciberconsejo 2: #UsaProtectorSolar

MUCHAS GRACIAS

GRUPO TRC®

#PasionPorLoNuestro

Link de Recursos

TOMAS FALSAS

GRUPO TRC

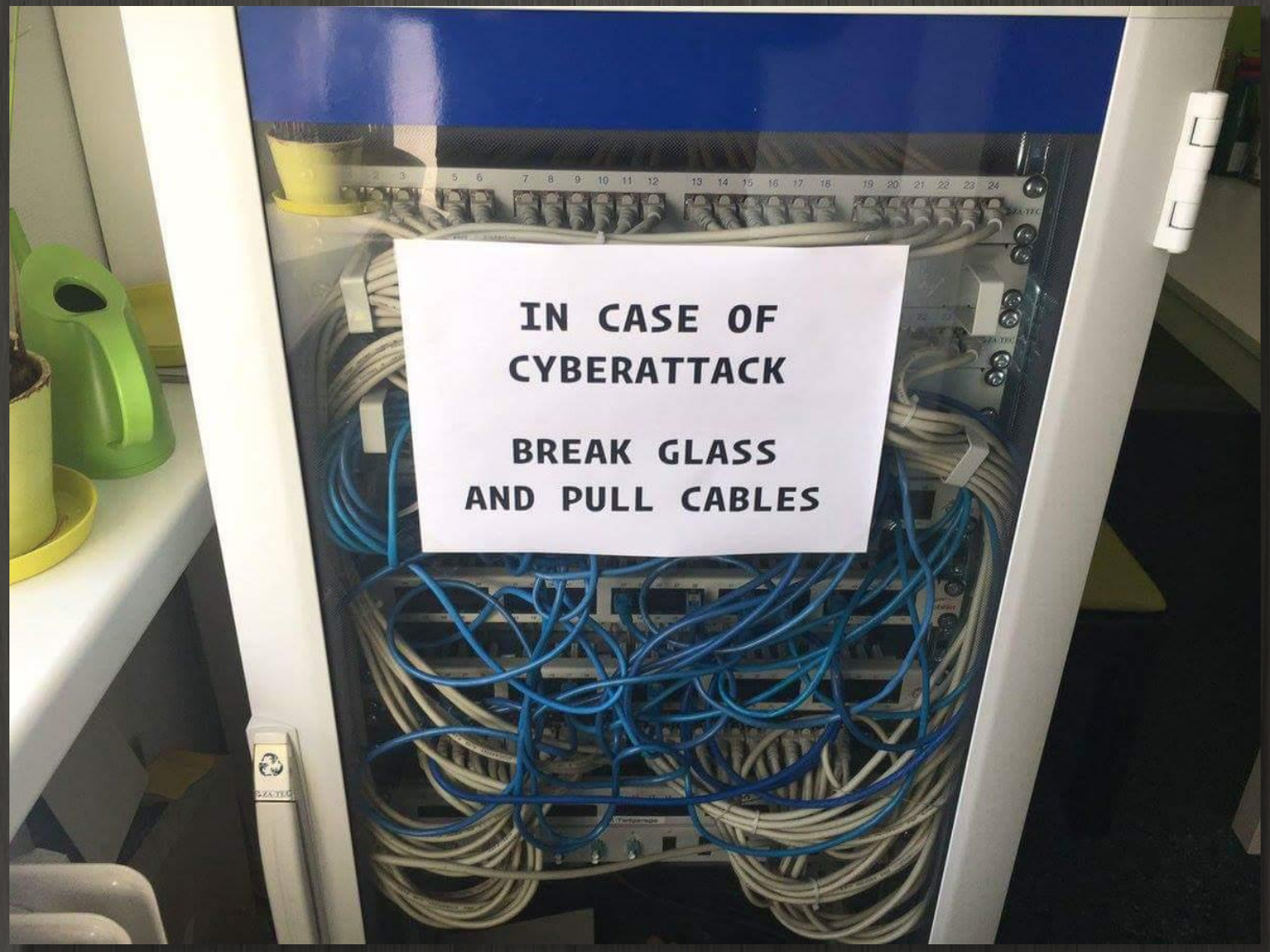
La práctica hace al maestro

Link de Recursos

TOMAS FALSAS

GRUPO TRC

Incident Response Plan ☺



Link de Recursos

TOMAS FALSAS

GRUPO TRC

Link de Recursos

TOMAS FALSAS

GRUPO TRC

Link de Recursos

TOMAS FALSAS

GRUPO TRC

“Os dieron a elegir entre gastar en ciberseguridad y el ransomware… elegisteis el ransomware, y ahora también tendréis una multa.”

NIS2: Parafraseando a Winston Churchill

Link de Recursos

TOMAS FALSAS

GRUPO TRC

All we need to do is rename "the problem" as "the solution" and we're good to go.

Link de Recursos

MUCHAS GRACIAS

GRUPO TRC®

#PasionPorLoNuestro

Link de Recursos