Práctica cibernética: Creación y edición de ejercicios de ciberseguridad para organizaciones

Mejores Prácticas en Ciberseguridad

A.09

Volumen A:
Un enfoque metodológico

BID

Cyber Israel
National Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *"Práctica cibernética: Construcción y edición de ciberejercicios para la organización"*. © (2020) Dirección Nacional de Ciberseguridad de Israel.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la división de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/Departments/General/cyberexercise**. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *startups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Clúster de Datos y Gobierno Digital (DDG) de la división Innovación para Servir al Ciudadano (ICS) de BID, disponible en: **https://www.iadb.org/es/reforma-modernizacion-del-estado/cluster-de-datos-y-gobierno-digital**.

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

/01. Introducción

Los principios y reglas para la planificación, construcción y realización de cualquier ejercicio no dependen del campo profesional en el que se realice. En este sentido, la práctica es una actividad genérica. Sin embargo, si bien los principios y reglas son genéricos, su aplicación en cualquier campo profesional no lo es, sino que está influenciada por el campo en cuestión.

Desde esta perspectiva, como se explicará a continuación, el término ejercicio de ciberseguridad tiene sentido, ya que la práctica en este campo tiene características que la distinguen de la práctica en cualquier otro campo.

Esta guía proporciona una base conceptual en el área de la práctica, en general, y en el campo de la cibernética, en particular. Presenta los principios y reglas para planificar, construir y editar un ejercicio de ciberseguridad, y el proceso para aprender del mismo. También hace mención brevemente a la construcción de un programa de ejercicios anual y plurianual. Su objeto de referencia es la organización, y el contexto más amplio de su contenido es el esfuerzo general de la organización para mantener, preservar y promover su resiliencia cibernética.

En consecuencia, la guía se compone de dos grandes bloques. El primero está conformado por cuatro partes en las que se desarrolla la base conceptual. El segundo se centra en algunos temas seleccionados del primer bloque y proporciona pautas para traducir la discusión conceptual en términos prácticos.

Este segundo bloque está compuesto por cuatro apéndices que tratan, en orden, los siguientes cuatro temas:

01

Elaborar un esquema de ejercicio de ciberseguridad.

02

Crear un escenario de ejercicio de ciberseguridad.

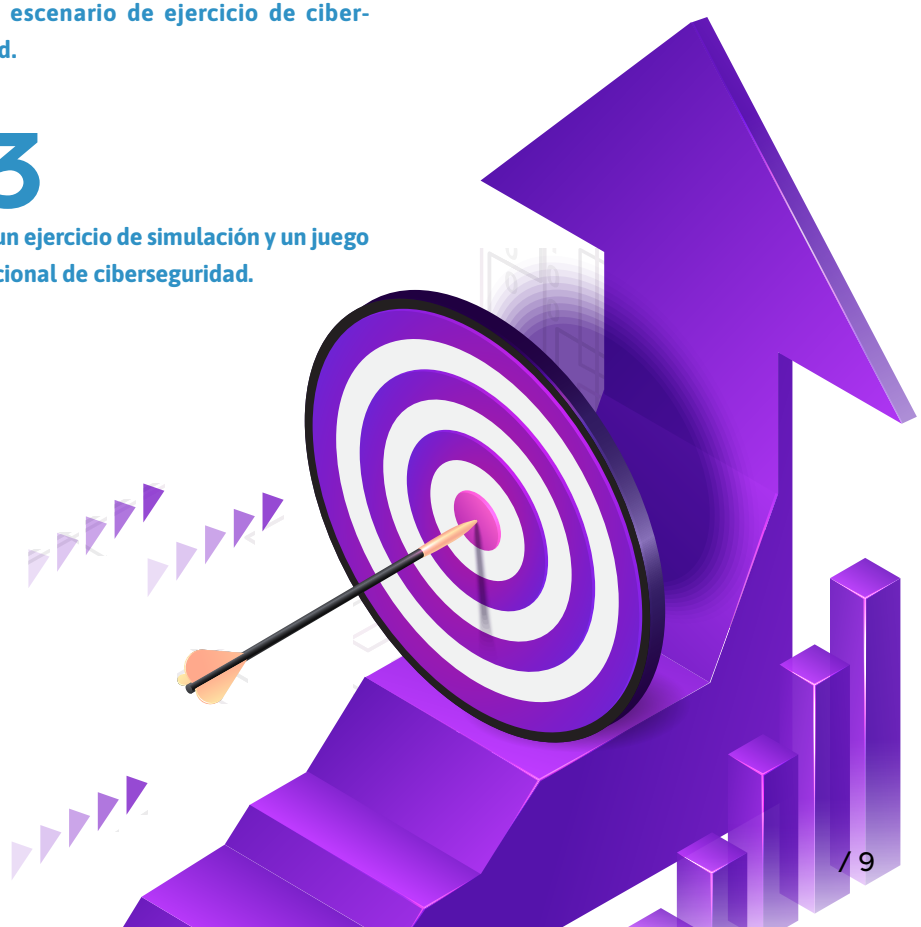
03

Realizar un ejercicio de simulación y un juego organizacional de ciberseguridad.

04

Realizar un ejercicio operativo de ciberseguridad.

Es importante tener en cuenta que, al igual que en otros campos profesionales, la experiencia necesaria para construir y realizar ciberejercicios solo se puede adquirir a través de una práctica constante. Esta guía proporciona al lector la base teórica necesaria para la práctica concreta en su área respectiva.



/02. Fundamentos de la práctica

Conceptos básicos

La práctica es una de las actividades diseñadas para mantener, preservar y promover la resiliencia organizacional. A fin de comprender adecuadamente su propósito, en primer lugar, es necesario conocer y comprender los conceptos involucrados, de los cuales conviene detenerse en dos: la competencia y la preparación.

La **competencia** es la capacidad de un individuo o de un marco organizativo para realizar una función particular. En cambio, la **preparación** es la capacidad de un marco organizativo para llevar a cabo una tarea específica y concreta. Por ejemplo, para que un equipo de respuesta a incidentes de ciberseguridad (RI) realice sus tareas regulares definidas como un marco organizativo, cada uno de sus miembros debe ser capaz de realizar las funciones que se le requieran para cumplir su parte en estas tareas.

La competencia expresa una habilidad fundamental genérica. Siguiendo el ejemplo anterior, es posible que cierta competencia de un miembro del personal de RI sirva para desempeñar tareas fijas del equipo e incluso para cumplir tareas fijas de otros marcos organizativos.

Por su parte, la preparación expresa una capacidad dirigida hacia una necesidad u objetivo particular y en muchos casos se adapta a una escena particular o entorno de acción. También es siempre una característica de organizaciones y marcos a nivel grupal, no individual. La preparación se basa completamente en las competencias, pero no son solo las competencias de los individuos o equipos sino también de los medios y recursos. Es decir, la solidez de los medios y la disponibilidad de recursos en los niveles requeridos de inventario.

La competencia y la preparación del individuo y la organización son cualidades que requieren una construcción gradual, mantenimiento continuo y promoción según sea necesario y de acuerdo con el plan definido. La responsabilidad general de llevar a cabo todas estas acciones recae en el directorio de la organización.

Las dos herramientas principales que utiliza la organización para este fin son la **formación** y la **actualización**.[2] La formación imparte y desarrolla habilidades, mientras que la actualización las preserva. Por lo tanto, el objetivo primordial de ambas es mejorar la capacidad del marco individual u organizacional para desenvolverse y cumplir con sus tareas. Esto se logra implementando la formación y actualización a través de cursos avanzados, capacitaciones y seminarios.

Como cualquier otra actividad, las actividades de formación y actualización de la organización también requieren cierto control. Gracias a que la competencia y la preparación son conceptos mensurables, cuantitativos, dentro lo posible, y en cualquier otro caso cualitativos, su nivel puede evaluarse mediante índices predefinidos y predeterminados. De esta manera, la organización utiliza estas métricas para garantizar que los cursos de formación y actualización sean **efectivos** (es decir, que logren sus objetivos) y que lo hagan de manera **eficiente** (en otras palabras: que aprovechen al máximo los recursos invertidos).

A nivel operacional, este control se realiza a través de dos tipos de actividad: la **auditoría** y el **ejercicio**.

La **auditoría** es una actividad de gestión, cuyo objetivo principal es obtener una instantánea actualizada del organismo auditado en las áreas en las que se ha decidido que sea auditado. Por su propia naturaleza, la auditoría es una actividad evaluativa: el organismo auditado se valora a partir de una serie de puntuaciones que se determinan de acuerdo con los índices antes mencionados.

2. Existe un grado de ambigüedad en la conceptualización y terminología, tanto en hebreo como en español, en el campo de la instrucción. En cualquier caso, en el contexto militar y de seguridad se acostumbra utilizar el término "formación" para denotar cualquier actividad de entrenamiento o mantenimiento de competencias. Desde este punto de vista, por lo tanto, la formación es la herramienta central para desarrollar la competencia y la preparación.

Por supuesto, la auditoría es una herramienta esencial para controlar las actividades de formación y actualización de la organización.

Por su parte, el **ejercicio** es una actividad de aprendizaje, diseñada para producir guías y lecciones cuya adopción y aplicación mejorará la competencia y preparación de la organización. En consecuencia, no se trata de una herramienta evaluativa dado que su conducta está enteramente destinada a ayudar a la organización y no a ponerla en una situación de amenaza.

Además, si bien tanto la auditoría como el ejercicio están destinados al aprendizaje organizacional, una entidad controlada tiende a percibir los resultados del aprendizaje derivados de la auditoría como una interferencia perturbadora en sus asuntos internos por parte de la autoridad que la realiza.

En cambio, si un practicante aprende a través de la experiencia personal, esto lo anima a identificarse con los objetivos de aprendizaje y adoptarlos.[3] Estas características del ejercicio, y ciertamente la diferencia esencial entre este y la auditoría, son extremadamente importantes. No solo deben ser tenidas en cuenta por los planificadores y editores del ejercicio desde el momento en que este se inicia hasta el final de las lecciones aprendidas, sino que también deben ser bien comprendidas por los practicantes.

A continuación se muestra una serie de distinciones entre las formas de entrenamiento, seguida de los modos en que estas se utilizan. Es importante mencionar que cualquier ejercicio se basa en la simulación de situaciones y circunstancias que pueden ocurrir en la realidad.[4] En la práctica, realizar un ejercicio significa exponer a los practicantes de manera controlada a los detalles de esta simulación y gestionar su respuesta de acuerdo con principios y reglas didácticas.

3. Como parte de una auditoría, se acostumbra realizar una actividad a la que comúnmente se denomina “ejercicio sorpresa”. Con base en lo mencionado, se entiende que esto no es un ejercicio, sino una especie de prueba práctica basada en la simulación.
4. Por su propia naturaleza, los ejercicios tienden a depender en gran medida de la simulación. Una de las principales razones de esto es la necesidad de evitar dañar componentes reales del entorno como resultado del trabajo del practicante. En la dimensión cibernética, este asunto es particularmente delicado. Más adelante se presenta una discusión detallada sobre el tema de la simulación en el ejercicio.

A.09 Práctica cibernética: Creación y edición de ejercicios de ciberseguridad para organizaciones

Métodos de práctica

Existen dos métodos de entrenamiento: el **teórico** y el **práctico**.

En el **método teórico** los practicantes deben enfrentar a nivel mental desafíos que no tienen una respuesta fácil, a menudo utilizando su ingenio, creatividad y pensando fuera de la caja. Las actividades de los practicantes se basan en la comunicación, discusiones y consultas en equipo. En realidad, no responden a los eventos que se les presentan, pero declaran (por lo general de manera oral y, a veces, por escrito) lo que habrían hecho de tratarse de un evento real. Como regla general, este método se lleva a cabo cuando todos los practicantes están reunidos en un sitio y organizados en uno o más grupos.

En el **método práctico** los practicantes deben enfrentar los desafíos que se les presentan mediante una actividad lo más cercana posible a la que habrían realizado si se tratara de hechos reales. En este caso, no declaran verbalmente, sino que **actúan**. Como regla general, este método se realiza cuando cada practicante opera en su verdadero entorno funcional. En esta modalidad también los practicantes tienen un diálogo entre sí, pero que no se limita a consultas y discusiones, sino que se realiza con base en los medios de comunicación destinados a esa actividad en casos reales.

El cuadro 1 resume las ventajas y desventajas de ambos métodos.

Cuadro 1. Ventajas y desventajas de los métodos teórico y práctico

	Ventajas	Desventajas
Actividad teórica	Es un método barato de prueba, ya que requiere una necesidad mínima de ayuda. Permite centrarse en los componentes blandos de la organización (percepciones [*insights*], políticas, metodología). Requiere una preparación relativamente corta. Requiere un manejo sencillo. Tiene un riesgo bajo para el funcionamiento de la organización y sus sistemas.	No permite la práctica de la función organizativa más allá del nivel del individuo. Es una práctica de naturaleza estática.
Actividad práctica	Permite la práctica eficiente y eficaz de la función organizacional a todos los niveles, a gran escala y con gran eficiencia.	Es costosa de realizar: requiere muchos recursos y una preparación larga y relativamente compleja. Es compleja de gestionar. Supone un alto riesgo para los sistemas de la organización.

Además de lo mencionado en el cuadro, se recomienda utilizar el método teórico cuando:

01

Es el primer ejercicio (nunca antes se ha realizado o se lleva a cabo por primera vez en ese ámbito) para toda la organización o para los agentes clave de la misma.

02

La organización evalúa la necesidad de realizar un cambio estructural, sea o no resultado de la actualización de la misión o de las tareas habituales de la organización.

03

La organización examina la necesidad de realizar un cambio de proceso o cualquier otro tema de principio relacionado con el desempeño de la organización.

Sin embargo, se recomienda utilizar el método práctico cuando:

01

Se trata de una organización relativamente joven, pero cuya Dirección estima que ya ha alcanzado la madurez operativa y busca examinar esta evaluación.

02

La organización ha implementado recientemente un proceso o cambio estructural y busca evaluar la corrección del cambio o el éxito de su proceso de implementación.

03

La organización identifica brechas importantes en la efectividad o eficiencia de su funcionamiento y busca aprovechar el potencial diagnóstico del ejercicio para analizar el problema y aprender a resolverlo.

Formatos de práctica

Cada uno de los métodos de práctica mencionados se puede implementar en ciertos formatos. El escenario manifiesta la forma en que se implementará el método de práctica elegido. Si bien el formato debe basarse en uno de los métodos descritos anteriormente, es posible, e incluso aceptable, incorporar componentes del otro método. A continuación se muestran los dos formatos principales para la realización de una **práctica teórica** y luego el formato principal para realizar un **ejercicio práctico**.

Ejercicio de simulación de mesa

En el ejercicio de simulación de mesa (TTX, por sus siglas en inglés) los practicantes se reúnen en uno o más equipos. Cada grupo se dirige a una mesa y lleva a cabo un diálogo sobre cómo lidiar con los desafíos/problemas que se le presentan, generalmente como parte de una historia "rodante". La estructura del equipo puede reflejar una verdadera estructura organizativa. De manera alternativa, pueden construirse como laboratorios de ideas (*think tanks*) para permitir la lluvia de ideas y fomentar el pensamiento creativo en un entorno de práctica libre de limitaciones cotidianas.

Los practicantes responden a un escenario en el que están expuestos a declaraciones, las cuales, por lo general, se hacen en la sala, aunque también pueden documentarse en tiempo real como parte del debate continuo de los practicantes. Cabe señalar que el escenario en este formato es completamente moderno (metódico, como se le llama comúnmente).

Dado que el ejercicio es un instrumento diseñado para permitir el aprendizaje, los datos de la situación en su punto final pasan a un segundo plano, debido a que la importancia radica en el desenvolvimiento de los practicantes y no en sus resultados.

El uso principal del TTX cibernético tiene como objetivo aumentar la conciencia general sobre las amenazas cibernéticas, memorizar e internalizar conceptos y validar planes de acción y procedimientos. Al hacerlo, se pueden identificar fortalezas y debilidades significativas en el sistema de defensa contra ciberataques de la organización. Por ese motivo, es particularmente adecuado para entrenar los rangos de la organización que se desarrollan en su nivel operativo y estratégico.

Por sus características y las circunstancias en las que se realiza, es sencillo coordinar la ejecución de un TTX, por lo que se considera una herramienta certera, en el sentido de que es relativamente fácil cumplir con los objetivos marcados originalmente.

Juego organizacional[5]

De manera similar a un TTX, el juego organizacional también emplea varios equipos de practicantes, que se ocupan de un escenario en evolución, pero a diferencia de un TTX, el juego organizacional es un juego de rol (de ahí su nombre), en el que todos los participantes forman juntos un sistema. En este sentido, es típico que cada uno de esos equipos represente un organismo u organización en particular (o incluso un país entero).

Las interacciones entre los equipos y sus miembros están predefinidas (y pueden ser amistosas, competitivas u hostiles). Su accionar está impulsado y controlado por reglas que también son predeterminadas, aunque algunas pueden mantenerse ocultas para los practicantes durante el juego.[6]

Debido a la forma y naturaleza del juego organizacional, y a diferencia del TTX, los resultados del desempeño de los practicantes suelen tener significado intrínseco y, por lo tanto, pueden ser un componente importante para extraer lecciones del juego. Desde el punto de vista de una organización específica, está destinado principalmente a entrenar personal interno a nivel operativo y estratégico en organizaciones relativamente grandes.

5. En el resto del mundo, el juego organizacional se llama comúnmente juego de guerra (*War Game*).
6. Debido a la naturaleza de la interacción en el juego organizacional, es habitual que entre los practicantes prevalezca cierta tensión estructural, que los estimula a pensar y actuar (metódicamente, por supuesto), y crea una atmósfera competitiva que ayuda al aprendizaje.

Ejercicio operativo

Este es el formato principal para realizar un ejercicio **práctico**. En él los practicantes operan en su verdadero entorno funcional, bajo sus componentes y condiciones. Por sus características y las circunstancias en las que se desarrolla, este formato permite una práctica que va desde el nivel técnico-táctico, donde el foco está en las áreas de especialización personal y de equipo (principalmente a través de ejercicios prácticos [*hands-on*]),[7] hasta el nivel estratégico, que es sistémico e integral a nivel interno y multiorganizacional.

La atención se centra en los procesos de toma de decisiones y de trabajo, interfaces entre órganos y unidades, procedimientos y cuestiones de políticas. De hecho, en la práctica operativa es posible utilizar elementos de escenarios reales,[8] pero suele ser un uso muy limitado y en una escala relativamente pequeña.

Sin subestimar en modo alguno la importancia y necesidad de la práctica a nivel técnico-táctico, no cabe duda de que la máxima realización del potencial inherente al formato operativo es a nivel operativo y estratégico. Por lo tanto, a partir de ahora, la discusión se centrará en estos niveles. En el apéndice 4 se proporcionan más detalles sobre el nivel técnico-táctico.

Una condición clave para asegurar la efectividad de un ejercicio operativo es que la combinación de practicantes represente fielmente a la totalidad de la organización. Esta condición se explica por el hecho de que no es posible entrenar a toda la organización, por lo que, de esta manera las lecciones aprendidas en el ejercicio serán relevantes para la organización en su conjunto, aunque solo se entrene a una parte de la misma.[9]

7. Los ejercicios prácticos están destinados al personal que se ocupa de los aspectos técnicos y tecnológicos de la ciberseguridad: análisis, ingeniería inversa, respuesta a incidentes, etcétera. Su eficacia suele requerir el uso de medios de simulación especialmente asignados.
8. La intención aquí es llevar a cabo acciones reales en relación con los componentes auténticos de la organización. En especial, un ataque real a su ciberseguridad o, alternativamente, cualquier daño real que se pueda provocar por otros medios.
9. Es importante aclarar que cumplir con esta condición no significa necesariamente esforzarse por entrenar a la mayor parte de la organización. En otras palabras, se trata de una cuestión de esencia y calidad, no de cantidad.

/03. Carpeta de ejercicios

Un ejercicio es un tipo de operación y, por lo tanto, para que su desarrollo alcance los objetivos propuestos, es necesario planificar con antelación. Este programa es la **carpeta de ejercicios** e incluye los siguientes componentes:

Esquema del ejercicio

Escenario del ejercicio

Archivo de eventos del ejercicio

A continuación, se detallan en orden los pasos de preparación de estos componentes.

Esquema del ejercicio

Como su nombre lo indica, se trata de un conjunto de todas las características que determinan la naturaleza y carácter del ejercicio, las cuales se presentan a continuación en el orden en que se determinan:

- **Propósito del ejercicio**
- **Composición de los practicantes**
- **Subobjetivos del ejercicio**
- **Temas de práctica**
- **Formato de práctica**
- **Indicador del ejercicio**

El esquema debe determinarse como parte de la construcción del programa de ejercicios anual/plurianual de la organización. Los otros componentes de la carpeta de ejercicios se definirán antes de la fecha del ejercicio (puede leerse más al respecto en el apéndice 1).

El **propósito del ejercicio** expresa la intención de la organización de examinar ciertos componentes o aspectos de su preparación en un momento dado. Por lo tanto, debería definirse como **practicantes** a los responsables de su existencia y mantenimiento en el nivel adecuado. Ellos deben ejercer esta responsabilidad mediante una serie de tareas regulares y específicas, para cada una de las cuales se determina un logro requerido. De ello se desprende que cualquier logro de este tipo es también un **subobjetivo** del ejercicio.[10] Los **temas de práctica** se derivarán de los subobjetivos.[11]

Un fundamento importante para determinar el propósito del ejercicio es la regla de inversión entre los medios y el propósito del ejercicio. En situaciones reales, la organización se da cuenta tanto como puede de su preparación para lograr sus objetivos comerciales y cumplir su misión. Sin embargo, en el ejercicio el centro de interés es el nivel de preparación organizacional. En efecto, su objetivo es examinar hasta qué punto la organización tiene el poder de lograr sus metas y misión. En otras palabras, su objetivo central es examinar los medios organizativos (el cómo) utilizando las mismas tareas fijas mencionadas anteriormente, las cuales están determinadas por la organización, mientras que los objetivos y la misión de la organización (el qué) se expresan de forma indirecta.

10. Debe enfatizarse que se debe definir un solo objetivo para el ejercicio. En consonancia con el dicho "el que mucho abarca, poco aprieta", se recomienda deducir un máximo de tres subobjetivos.
11. Luego de los subobjetivos, se recomienda definir un máximo de tres temas de práctica.

Como se ha mencionado, el ejercicio no es en esencia una actividad evaluativa. Al mismo tiempo, se sobrentiende que los logros de los practicantes son información fundamental para lograr el objetivo del ejercicio, ya que solo a través de ellos será posible evaluar el estado de preparación de la organización. La medición de los logros y evaluación de los practicantes deben realizarse de acuerdo con **los índices de competencia y preparación** definidos en la organización en las áreas respectivas de funcionamiento.

Por lo tanto, la carpeta de ejercicios debe incluir una colección de todas las métricas relevantes para los propósitos del ejercicio y los temas de práctica derivados de ellas. Este compendio se conoce como **indicador de ejercicios**.

Con respecto al uso de estos índices, se debe tener en cuenta que no se trata de una ciencia exacta, por lo que las acciones de medición y evaluación requieren un gran cuidado. Si bien existen varias herramientas que pueden ayudar a minimizar el grado de distorsión (sesgo) de la imagen de competencia y disposición que se obtendrá al final del proceso (como la confiabilidad entre evaluadores), la discusión sobre este vasto campo profesional excede los objetivos de esta publicación.

También es importante enfatizar que la construcción de un esquema para un ejercicio en particular no es autosuficiente. Cada ejercicio debe ser un eslabón en una cadena continua de tales acciones y su propósito es, como ya se explicó, mantener, preservar y promover la preparación organizacional para enfrentar ciberataques y crisis de seguridad cibernéticas.

Esto afecta directamente la determinación del nivel de requisitos que cada ejercicio exigirá a los practicantes. La situación óptima es que cada ejercicio presente exigencias más altas que su antecesor. Un elemento clave en el diseño del esquema de un ejercicio son las lecciones de los ejercicios ya realizados anteriormente.

Si bien el esquema expresa lo que la organización está interesada en aprender del ejercicio, el componente de la carpeta de ejercicios que realmente permite este aprendizaje es el **escenario**.

Escenario del ejercicio

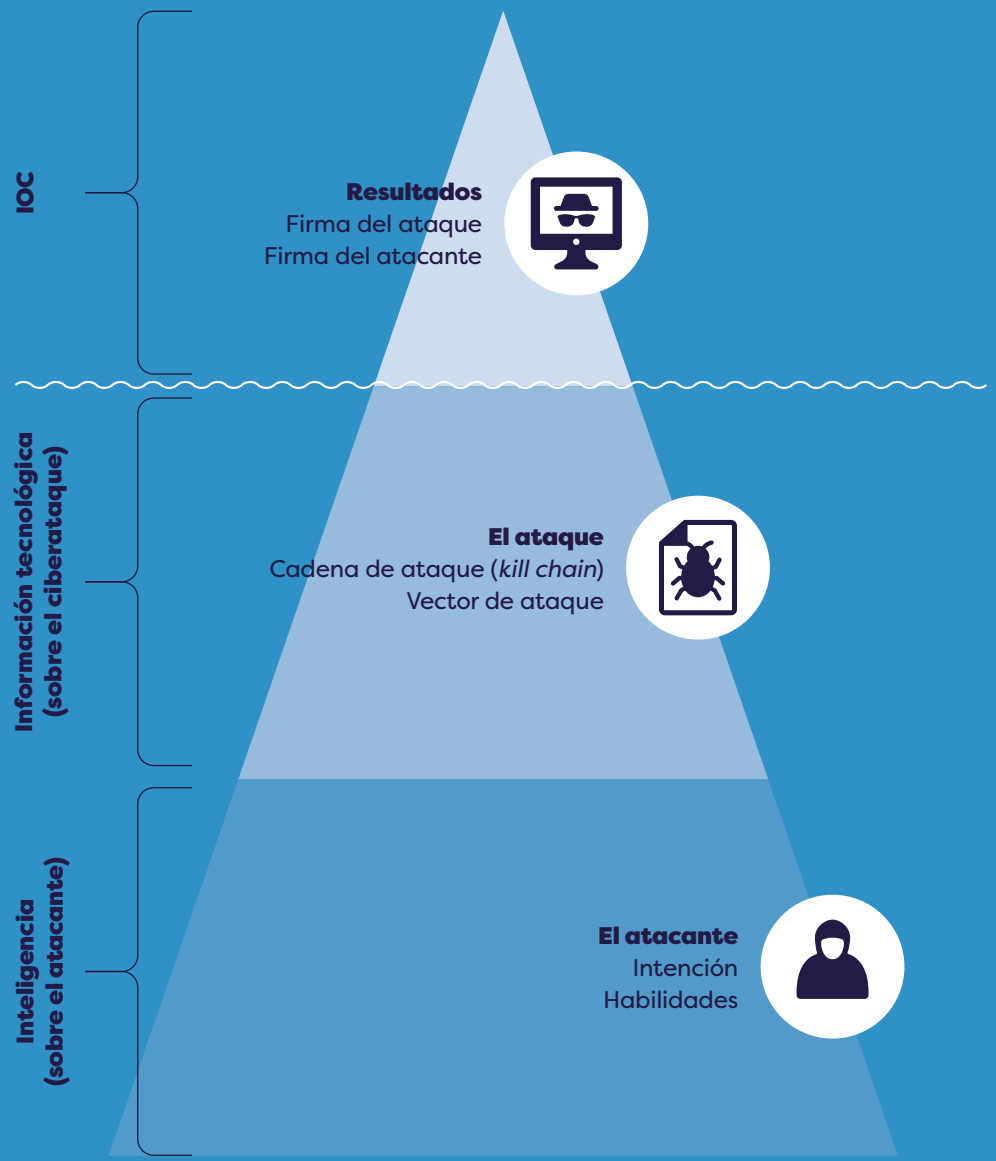
Es la trama del ejercicio. Las cosas que suceden en su marco son los estímulos a los que se supone que los practicantes deben responder durante el mismo.[12] El escenario debe ser realista, justificado y desafiante (véase el apéndice 2 para más información). La piedra angular del escenario es un **ciberataque**. Un escenario puede contener uno o más ataques, pero se recomienda que el número total no supere los cinco. **Por definición cada ejercicio tiene un solo escenario.** Al mismo tiempo, el escenario puede construirse como una serie de tramas, cada una de las cuales se sostiene por sí sola sin ninguna conexión con las demás. En ese caso, cada trama contendrá al menos un ciberataque.[13]

El gráfico 1 muestra el modelo iceberg, un modelo de ciberataque, desde dos ángulos: el del atacante y el del defensor. Desde el punto de vista del atacante, es un movimiento diseñado para lograr un objetivo que ha definido y que sirve a sus intenciones, mientras utiliza sus habilidades en el campo. El ataque produce diversas consecuencias visibles (efectos) que ocurren dentro de los sistemas del defensor, los cuales se manifiestan en alteraciones de su accionar y, a menudo, también en otros signos visibles que indican su existencia (varias firmas[14] de origen humano y medios involucrados en el ataque).

Desde la perspectiva del defensor, está expuesto a una serie de indicadores de compromiso (IOC, por sus siglas en inglés), lo que indica la posibilidad de un ciberataque. Estos incluyen todos los resultados y señales mencionados anteriormente, ya que son visibles para el defensor. Sin embargo, es de esperar que a sus ojos muchos de ellos sean irrelevantes, ya que indican una actividad que por su propia naturaleza se realiza en secreto.

12. Lo dicho a continuación es aplicable a todos los aspectos de la práctica.
13. Un escenario de este tipo es principalmente adecuado para la práctica teórica (TTX o juego organizacional). En cambio, en la práctica es de gran importancia la visualización efectiva de una realidad posible y, por lo tanto, el escenario más adecuado es una trama continua.
14. El término *firma* se refiere a información relacionada de una forma u otra con las acciones del atacante, que ha sido revelada al defensor. Ejemplos de ello son la interceptación de una referencia a la organización en una conversación en la red oscura (*darknet*) o un escaneo de puertos realizado con frecuencia.

Gráfico 1. El modelo iceberg



Estas señales están representadas en el diagrama en forma de punta de iceberg flotando en la superficie del agua y, por lo tanto, son evidentes a simple vista. A su vez, el resto de la información sobre el atacante y el ciberataque, que se encuentra inmerso en las profundidades del ciberespacio atacado, se materializa en la forma del resto del iceberg que está hundido en el mar y oculto a la vista.

Por lo tanto, a efectos prácticos esta información es un secreto del ejercicio. Los detalles serán conocidos por los practicantes (es decir, los defensores) solo en dos casos: si los dedujeron por sí mismos con base en la información que recibieron o si les fueron revelados por iniciativa de los coordinadores del ejercicio. Más adelante se trata en extenso este caso.

La dinámica del ejercicio se resume en los esfuerzos del practicante por superar con éxito los desafíos que presenta el escenario, mientras se enfrenta constantemente a la falta de referencias, con información irrelevante y con datos (al menos en apariencia) contradictorios.

Esta dinámica existe en dos niveles simultáneos: el operativo (procesos organizacionales: operacionales, empresariales o de otra índole) y el tecnológico (procesos que tienen lugar dentro del ciberespacio). Por supuesto, existe una fuerte afinidad entre estos dos niveles, ya que el propósito de la infraestructura de la tecnología de la información (TI) de la organización es dar soporte a sus diversos procesos operativos y cuando estos son atacados, se perjudica la finalidad de los procesos operativos.[15]

Esta situación dual establece la base para la formación de dilemas funcionales, no solo en el ejercicio sino también en la vida real. Por ejemplo, el responsable de ciberdefensa de la organización puede recomendar a la Gerencia que deshabilite proactivamente un proceso operativo particular para reducir la superficie de ataque organizacional frente a potenciales avances del ataque que ya se está produciendo. Por su parte la Gerencia puede oponerse a tal movimiento por un claro interés comercial.[16]

15. Esto aplica tanto para el entorno TI como para el de tecnología operativa (OT, por sus siglas en inglés).
16. En este contexto, es importante la gestión de riesgos durante una crisis cibernética y, dentro de ella, el análisis del impacto de un ciberataque en el negocio (BIA, por sus siglas en inglés).

Para asegurar que el ejercicio logre su objetivo, los desafíos que el escenario presentará a los practicantes deben surgir de los temas de la práctica. También es preciso alentar a los practicantes a actuar en áreas directamente relacionadas con los subobjetivos del ejercicio (puede leerse más al respecto en el apéndice 2).

De hecho, el gráfico 1 muestra una imagen parcial de la estructura del escenario. En el contexto de la dimensión cibernética lo que parece ser la punta de un iceberg que sobresale del agua puede resultar, en una inspección más cercana (esto es, después de una investigación adecuada), un montículo de espuma en la cresta de una gran ola. En un lenguaje menos pintoresco, no todo lo que parece ser un ciberataque lo es.

Con base en esto, y con el fin de construir una simulación lo más cercana posible a la realidad, también se deben incluir en el escenario eventos inocentes, como fallas en el sistema u operativas. En la jerga del campo de los ciberejercicios, este componente se denomina ruido.

Construcción de escenarios: principios rectores

01

Peso del componente cibernético en el ejercicio: el escenario debe presentar a los practicantes un desafío en el campo de la ciberseguridad durante todo el ejercicio, sin excluir la importancia del aspecto operativo del ejercicio.[17]

02

Realismo: el escenario debe presentar a los practicantes la realidad con la que están familiarizados hasta en el más mínimo detalle. Esto se aplica no solo a la información sobre lo que está sucediendo en la simulación del ejercicio, sino también a los desarrollos que tienen lugar en la misma como resultado directo del accionar de los practicantes, dado que esta es una respuesta a la simulación que se les presenta. Esto es necesario para asegurar que los practicantes confíen en lo que se les dice, sientan empatía por la situación en desarrollo del ejercicio y se desenvuelvan naturalmente dentro de la misma, es decir, de la manera más cercana a como habrían actuado si lo planteado sucediera en la realidad. Por esta razón, es recomendable involucrar en el proceso de construcción del escenario a representantes de las unidades organizativas más experimentadas en asuntos de prácticas.[18]

03

Gravedad: es la gravedad de la situación general de la organización como resultado del daño acumulativo causado por los ciberataques incluidos en el escenario. Desde el principio, la construcción del escenario debe tener en cuenta los resultados del proceso de evaluación de riesgos y el análisis realizado por la organización.[19] En este sentido, el centro de gravedad del escenario se basará en los mismos ataques que se incluirán allí, cuya expectativa de daños se estima alta. Dentro de estos ataques, es importante incorporar al menos uno cuya probabilidad de ocurrencia se estima que sea baja.

04

Dificultad: la experiencia humana muestra que los fracasos motivan el aprendizaje en mayor medida que los éxitos.[20] Por lo tanto, el escenario debe construirse de manera que sea difícil para los practicantes, hasta el punto de que sus posibilidades de fallar al menos en algunos de sus esfuerzos sean probables. Por un lado, el nivel de dificultad del escenario debe ser lo suficientemente alto como para sacar a los practicantes de su zona de confort y, de esta manera, motivarlos a realizar esfuerzos para enfrentar los desafíos que presenta. Por otro lado, la dificultad debe ser suficientemente baja como para evitar la frustración de los practicantes con los desafíos del escenario, lo que finalmente los priva de la motivación para invertir tales esfuerzos.[21]

17. En el apéndice 2 se ofrece un análisis más amplio de esta cuestión.

18. A estos expertos se les prohibirá participar en el ejercicio, ya que han estado expuestos de antemano a los detalles del escenario. Es mejor lidiar con el dilema "¿practicante o cómplice del ejercicio?" antes de la actividad, que enfrentarse a un hecho consumado en el transcurso del ejercicio.

19. Existen diferentes enfoques para evaluar los riesgos planteados a la organización, independientemente del campo exclusivo de la ciberseguridad. Por supuesto, este es un tema muy importante, pero abordarlo va más allá de los límites de la discusión de esta guía y, por lo tanto, no se ampliará el tratamiento del caso.

20. En este contexto sería apropiado citar la famosa declaración de Winston Churchill sobre la importancia del fracaso: "El **éxito** consiste en pasar de un **fracaso** a otro **fracaso** sin perder el entusiasmo".

21. Se debe recordar que existe una afinidad entre la gravedad del escenario y su dificultad.

05

Historia de fondo: hasta ahora, la discusión del escenario se ha basado en la suposición de que este será revelado a los practicantes solo en el momento en que se realice el ejercicio. Sin contradecir esto, es posible preceder la publicación de una historia de fondo. Se trata de una recopilación de nociones, algunas de las cuales contienen información sobre los ciberataques que se producirán en el ejercicio y otras son ruido. En cualquier caso, la historia de fondo no contendrá información ya incluida en el escenario.

La idea detrás de este componente opcional es animar a los practicantes a comenzar a prepararse para el ejercicio y crear entre ellos tensión y anticipación en relación con el mismo. Por lo tanto, si se utiliza una historia de fondo, se recomienda distribuirla a los practicantes aproximadamente una semana antes de la fecha del ejercicio. Por definición, la historia de fondo es una parte integral del esquema del ejercicio, aunque, como se ha mencionado, se distribuye en un momento separado del mismo.

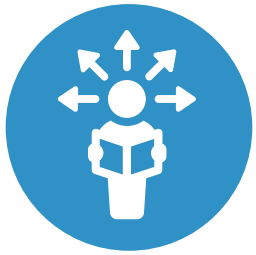
06

Distorsiones del ejercicio: incluso si se cumplen todas las instrucciones anteriores, sigue habiendo una limitación que los mejores escenarios no pueden evitar: el escenario permite simular la realidad; sin embargo, no hay simulación que pueda ser un sustituto perfecto de la realidad. De ello se desprende que en cada ejercicio habrá ciertas distorsiones en relación con lo que se espera que ocurra, en circunstancias idénticas, en la vida real.

El daño más significativo, inherente a estas distorsiones, amenaza principalmente la validez de las lecciones que se pueden aprender del ejercicio (para eso, se brindan detalles a continuación). Por lo tanto, se agudiza la necesidad de construir un escenario que no solo exprese de la manera más fiel los desafíos que se supone que deben enfrentar los practicantes, sino que también pueda desplegarse de manera que refleje la realidad en la que están acostumbrados a desenvolverse en su vida diaria.

Eventos del ejercicio

Con base en lo descrito anteriormente, el escenario del ejercicio no es más que una colección de icebergs construidos por los planificadores del ejercicio. La simulación dentro de la cual los practicantes tendrán que desenvolverse se basa en la colección de señales que forman la superficie visible de cada iceberg. Sin embargo, esto no es suficiente, ya que en la vida real es probable que los practicantes estén expuestos a elementos adicionales de información sobre los ataques y quienes los causan.



Por lo tanto, el escenario sufre un proceso de descomposición (*break down*), durante el cual tanto su parte visible como los detalles de sus partes ocultas se procesan en una colección de **eventos del ejercicio**.

El **archivo de eventos del ejercicio** resultante expresa tanto los ciberataques como los eventos de ruido incluidos en el escenario. Mientras que el proceso de construcción del escenario se realiza desde el punto de vista del atacante, el proceso de desentrañar la guía del ejercicio se realiza desde el punto de vista de los defensores, es decir, los practicantes.

El evento del ejercicio es un registro de información con una estructura fija, que se presenta bajo dos configuraciones: limitada y extendida. En su configuración limitada, incluye los siguientes campos:

01

Transmisor del evento: un practicante o un no practicante.[22]

02

Receptor del evento (practicante por definición).

03

Fecha y hora del ejercicio en los que se proporcionará el evento a los practicantes.

04

Momento real de transmitir el evento a los practicantes.

05

Contenido del archivo de eventos.

22. En ningún caso este individuo debe ser el coordinador del ejercicio o cualquiera de sus asistentes. Se hace referencia aquí a individuos que deben tomarse del ambiente concreto y funcional de los practicantes. Como se ha mencionado, algunos de ellos pueden participar en el ejercicio por sí mismos, mientras que el resto estará representado por participantes designados por el coordinador del ejercicio.

El evento del ejercicio debe:

01

Expresar fielmente el resultado (efecto) que se supone que se creará durante el proceso de desarrollo del evento ruidoso del ciberataque/ejercicio.

02

No incluir información que sea un secreto del ejercicio.

03

Articular fielmente los flujos de información que se supone o se espera que sucedan en caso de que ocurra un hecho real.

La dinámica general de un ejercicio se puede describir como un viaje de los practicantes hacia las ideas y lecciones aprendidas al final. Aunque el contenido de esto último no se conoce de antemano, los coordinadores del ejercicio saben bien a donde los practicantes deben llegar al final de este viaje: el propósito del ejercicio, sus subobjetivos y los temas de práctica deben indicarlo claramente. Desde este punto de vista, la información proporcionada a los practicantes es el medio que tienen los responsables de los ejercicios para motivar a los practicantes a realizar este viaje y guiarlos en su camino para que efectivamente lleguen al destino deseado.[23]

Al mismo tiempo, los coordinadores son incapaces de controlar la respuesta de los practicantes a los eventos y, por lo tanto, puede haber una situación en la que los practicantes se pierdan o simplemente se atasquen sin poder avanzar. En ese caso, los coordinadores de ejercicio tienen a su disposición un tipo especial de evento de orientación: **el conocimiento guía**. La información de orientación no tiene una fecha de entrega planificada previamente, sino que está lista y, en caso de necesidad, se entrega a los practicantes. El conocimiento guía es una parte orgánica del escenario y trama del ejercicio. De hecho, su entrega se basa en la expectativa de los coordinadores de que esa información proporcionada ayudará a los practicantes a progresar según sea necesario.

Sin embargo, a veces esta medida no es suficiente. En tal caso, se requerirá la intervención directa de los coordinadores en el desenvolvimiento de los practicantes, con el fin de hacer avanzar las cosas.

23. Como regla general, no debe haber un diálogo directo entre los coordinadores del ejercicio y los practicantes durante el ejercicio. Más información al respecto se incluye en la discusión sobre la gestión del ejercicio en los apéndices.

Archivo de eventos del ejercicio, reacciones de los practicantes a los eventos y el reloj del ejercicio

El archivo de eventos del ejercicio es un cuadro en el que cada fila está dedicada a un evento del ejercicio. Como se desprende de lo anterior, este archivo no debe ser una recopilación aleatoria de piezas de información, sino una cadena estructurada de mensajes que expresen fielmente el desarrollo de los eventos incluidos en el escenario (tanto ataques como ruidos). También tiene en cuenta las reacciones esperadas de los practicantes hacia los mismos, lo que ayudará a los coordinadores del ejercicio a controlar su desarrollo y movimientos.

Para lograr esto, las reacciones de los practicantes a cada evento deben mapearse de antemano. Debe hacerse una distinción entre una respuesta deseada y una esperada. La **respuesta deseada** expresa la forma adecuada y correcta de tratar los datos de situación presentados por la guía. El **indicador de ejercicio** puede ayudar mucho a determinarlo. Sin embargo, la **respuesta esperada** refleja lo que es probable que hagan los practicantes en el ejercicio, y se basa en la familiaridad de los coordinadores del ejercicio con los practicantes y con la situación existente en su conjunto.

Es importante señalar que no es necesario completar estos dos campos en el contenido de cada guía. En ocasiones, sería correcto y adecuado expresar un cambio significativo en la imagen del ejercicio a través de una secuencia de varios eventos. Solo al final (es decir, en el último evento) tendría sentido definir las respuestas de los practicantes a los nuevos datos que se les proporcionan.

A partir de todo ello, los eventos se ordenan en el archivo de eventos del ejercicio en su **configuración extendida**, que contiene dos campos adicionales en comparación con la configuración limitada:

01

Respuesta deseada de los practicantes a los eventos.

02

Respuesta esperada de los practicantes a los eventos.[24]

La necesidad de controlar el curso del ejercicio y su desarrollo también debe abordar la cuestión del reloj del ejercicio en la compilación de este archivo. El escenario del ejercicio puede representar una realidad simulada que ocurre en una fecha y hora diferentes a las que realmente tienen lugar (tiempo real). Por lo tanto, la fecha y horas establecidas en el escenario se denominan reloj de ejercicio y se expresan en el momento de los eventos.

En su mayor parte (y ciertamente cuando se trata de ataques cibernéticos), la cantidad real de tiempo dedicado al ejercicio es significativamente menor que la duración de los eventos en el escenario. Para superar esta dificultad, es necesario reducir la cantidad de tiempo real que se habría requerido para responder a lo que ocurre en el escenario y asignar a los practicantes períodos de tiempo significativamente más cortos para responder a la información de los eventos que reciben.

Por lo tanto, los eventos se programan en efecto dos veces: la primera, utilizando el campo "fecha de ejercicio y momento de brindar el evento a los practicantes", y la segunda, utilizando el campo "tiempo real de proporcionar el evento a los practicantes". Así, por ejemplo, los practicantes pueden recibir dos eventos consecutivos con una diferencia de tiempo real de media hora entre sí, cuando las situaciones descritas en ellos ocurrieron en la práctica con una diferencia de 12 horas entre sí.

La brecha constante entre las dos escalas de tiempo discutidas aquí (que también se espera que aumente a medida que continúa el ejercicio) puede crear en los practicantes la sensación de que el reloj del ejercicio avanza a saltos. Por lo tanto, los coordinadores del ejercicio deben esforzarse por mantener estos saltos lo menos abruptos posible.

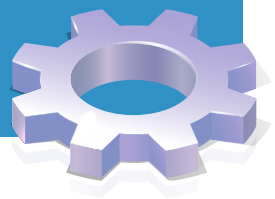
24. Para evitar dudas, los coordinadores del ejercicio utilizan el archivo de eventos del ejercicio para controlar sus movimientos, pero su contenido no se divulga, como tal, a los practicantes. La información contenida en el mismo se les transmite en su configuración limitada (es decir, sin los campos respuesta deseada y respuesta esperada). Técnicamente, se puede transportar por diversos medios, tanto de forma manual como mecánica.

En cuanto al grado de contracción, se debe tener en cuenta el período de tiempo (real) que sería apropiado asignar a los practicantes para responder a cualquier evento. Asignar un período de tiempo demasiado corto puede afectar la efectividad de la práctica y, por lo tanto, debe evitarse tanto como sea posible.

En este contexto, es apropiado discutir la tendencia de los coordinadores del ejercicio a cargar tareas a los practicantes con el fin de examinar su desempeño en condiciones de estrés. En primer lugar, cabe decir que la tensión no es necesariamente una consecuencia de la **cantidad** de información con la que tienen que lidiar los practicantes, sino del **significado** de esta información, y por lo tanto, es necesario centrarse en el correcto diseño del contenido de la guía y no en su número para lograr este propósito.

En segundo lugar, debe considerarse que funcionar bajo estrés es una habilidad básica y sobre todo personal y, por lo tanto, su práctica es relevante principalmente para el método práctico, es decir, para los ejercicios operativos y más precisamente (por razones metodológicas y didácticas) para los realizados a nivel técnico-táctico de la organización. Sin embargo, en este caso, la distancia entre practicar esta habilidad y desarrollarla es bastante pequeña y, por ello, es recomendable que la organización la aborde a través de actividades formativas (como, por ejemplo, en el marco de la formación ejecutiva).

Una regla importante en el mundo de los ejercicios es nunca copiar manualmente una carpeta de ejercicios existente para un nuevo ejercicio. La práctica es una de las formas más efectivas de obligar a una organización a salir de su zona de confort y, por lo tanto, de reducir el riesgo de fijación perceptiva y de transformar comportamientos aceptados en patrones de acción "sagrados".



/04. Coordinación del ejercicio

División de Administración del Ejercicio y Unidad de Ejercicios de la organización

Hasta aquí se ha utilizado en la guía el término coordinadores de ejercicios, dado que un ejercicio no se construye ni se realiza por sí solo. Para ello existe una **División de Administración del Ejercicio**, la cual en la dimensión cibernética se apoya en cuatro pilares:

- **Un metodólogo** (que a menudo también actúa como jefe administrativo)[25]
- **Un tecnólogo** (por definición, también responsable de inteligencia sobre ataques)[26]
- **Un experto en procesos**
- (En algunos casos) **un experto en inteligencia** sobre los atacantes[27]

25. Por lo general, se espera que el jefe de la Unidad de Ejercicios actúe como jefe de la División de Administración del Ejercicio. Al mismo tiempo, y principalmente por motivos de representación, se nombrará para este puesto a un empleado de mayor jerarquía dentro de la organización.
26. Se refiere principalmente a lo que se conoce en este ámbito como "inteligencia azul", es decir, información tecnológica. Gran parte del negocio está en el contexto de la dimensión cibernética y sujeta tanto a ciberataques como en manos de funcionarios especializados en ciberseguridad (locales e internacionales) especializados en el tema.
27. Además de lo explicado en la nota anterior, se refiere aquí a lo que se llama "inteligencia roja", es decir, la que está bajo la responsabilidad de los organismos de inteligencia nacional. Aunque en la actualidad los límites entre estos dos mundos de inteligencia a menudo se difuminan, los miembros de la comunidad todavía tienen capacidades únicas significativas.

Por lo general, la División de Administración del Ejercicio incluirá funcionarios adicionales, por lo que en adelante se hará referencia a los cuatro antes mencionados como el **equipo líder** del ejercicio.[28]

Por lo tanto, el término División de Administración del Ejercicio se refiere a un marco organizativo especialmente designado y temporal, que se establece antes de la fecha de realización de un ejercicio particular estipulado en el plan de trabajo y se desmantela una vez finalizado el proceso de extraer lecciones del mismo. De hecho, para la construcción del programa anual de ejercicios de la organización (que incluye, como ya se ha explicado, el esquema de cada uno de los ejercicios que en este se exponen), es suficiente una pequeña plantilla, compuesta por una o dos personas como máximo.

En este sentido, es apropiado que este pequeño grupo constituya una unidad permanente dentro de la organización, que será responsable de administrar todas sus actividades de práctica de manera continua. De aquí en adelante se hará referencia a este grupo como la **Unidad de Ejercicios** de la organización para diferenciarla de la División de Administración del Ejercicio. En este sentido, la Unidad constituirá el núcleo alrededor del cual se formará el principio de cada ejercicio específico.

Como regla general, la División de Administración hace las veces de cualquier empleado u organismo que no participa realmente en el ejercicio. Con el fin de prepararse de antemano para una respuesta al desarrollo esperado y al ocasional del curso del ejercicio, estos se pueden representar a través de eventos previamente preparados. De hecho, esta regla puede invertirse en muchos casos de entrenamiento teórico. Sin embargo, en la práctica el potencial desarrollo durante el ejercicio puede requerir la preparación previa de un gran número de tales conocimientos.

Además, la necesidad de su transferencia debidamente programada a muchos practicantes en períodos cortos de tiempo puede crear una carga insoportable para la División de Administración. Por ello, para este fin se recomienda y se acostumbra utilizar durante el ejercicio la asistencia de personal especialmente asignado, el cual se puede dividir en dos subgrupos. El primero estaría formado por aquellos sobre los que los practicantes tienen cierta autoridad. Así, por ejemplo, en un ejercicio destinado a la Dirección de la empresa, este grupo podría incluir personal propio y de organizaciones que son proveedores de la organización que realiza la práctica. El segundo grupo estaría constituido por la Junta Directiva de la empresa, altos ejecutivos no capacitados o cualquier regulador estatal.[29]

Dado que existen ciertas similitudes entre la actividad del funcionario y la de un practicante, la experiencia sugiere que el funcionario también sea recompensado con algún beneficio por participar del ejercicio, aunque no fuera parte del grupo de practicantes. De cualquier manera, los funcionarios son miembros de la División de Administración a todos los efectos.

Para hacer el seguimiento del desempeño de los practicantes, la División de Administración recibe la asistencia de **veedores**. El veedor está físicamente presente en el entorno de la práctica y realiza una observación no participativa de los movimientos de los practicantes. Lleva a cabo dos funciones: durante el ejercicio desarrolla un vínculo continuo entre la División de Administración y el entorno de práctica, y después de su finalización elabora un informe final sobre el desempeño de los practicantes. Al igual que los funcionarios, los veedores son miembros plenos de la División de Administración del Ejercicio.

28. Como se explicará más adelante en esta sección, las características únicas del ciberespacio desde el principio imponen limitaciones considerables a la capacidad de incluir en el escenario acciones de intervención reales, tanto por iniciativa de la División de Administración como por iniciativa de los practicantes. Al mismo tiempo, la División de Administración debe considerar la designación de un **veedor de seguridad**, que supervisará la actividad real que se lleva a cabo durante el ejercicio y evitará la concreción de circunstancias que de alguna manera puedan poner en peligro el ciberespacio organizacional.

29. En el lenguaje común, es costumbre referirse a estos funcionarios como "control bajo" y "control alto", respectivamente.

Por regla general, el personal directivo y los veedores no deberían interferir con el funcionamiento de los practicantes. De hecho, la División de Administración debe esforzarse por ser lo más transparente e imperceptible posible. Hay dos excepciones a esta regla:

01

Si la División de Administración no ha podido dirigir las actividades de los practicantes de acuerdo con su plan en un momento determinado, incluso después de utilizar el conocimiento guía, hay espacio para su intervención directa en el desempeño de los practicantes para este propósito. En este contexto, vale la pena señalar que la División de Administración se esfuerza por lograr el objetivo del ejercicio, por lo que no toda la información que preparó para los practicantes se les entregará al final del ejercicio.

02

Los practicantes pueden contactar a la División de Administración con preguntas sobre las reglas de coordinación del ejercicio (por ejemplo, con respecto al reloj, el rol que desempeña un funcionario en particular, etcétera).[30]

30. Por el contrario, y de acuerdo con lo ya explicado, se espera que los practicantes estén en constante interacción con los funcionarios.

Entorno de práctica

Allí es donde trabajan los practicantes. Existe una diferencia fundamental entre el entorno de ejercicios utilizado para la parte teórica y el empleado para la parte práctica: en esta última, el objetivo es, como se ha mencionado, que los practicantes operen dentro de su entorno de funcionamiento real y natural. También se deduce que el entorno de la práctica generalmente abarcará varios sitios, algunos de los cuales contendrán más de un espacio funcional. Por su parte, en la práctica teórica el objetivo es crear condiciones que fomenten el pensamiento libre a partir de las limitaciones cotidianas y, por lo tanto, es típico que los practicantes operen en este marco en un entorno artificial, cuyo diseño está guiado por consideraciones didácticas y logísticas.

Por lo general, el entorno de práctica contendrá un espacio: la sala donde se llevará a cabo el ejercicio. En caso de que el formato de práctica específico implique el trabajo en equipo, el entorno incluirá espacios de trabajo complementarios. Una consideración adicional que incide en el diseño del entorno de práctica teórica es la seguridad de la información, es decir, el nivel de clasificación de seguridad del material de ejercicio. Por lo tanto, puede ser necesario crear áreas de práctica aisladas, lo que permitirá la división entre diferentes equipos de trabajo.

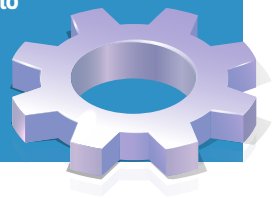
Otra diferencia entre los dos métodos de práctica es el peso y la importancia de los medios de simulación. En términos educativos, la práctica natural es querer realizar un ciberataque real a los sistemas informáticos de la organización. Desafortunadamente, esta aspiración está limitada por consideraciones legales, de seguridad, materiales, económicas y de imagen. La solución aparentemente obvia a este problema es utilizar un entorno TI independiente y especialmente asignado, o un entorno con fines prácticos, que imite fielmente la estructura y funcionamiento de la verdadera infraestructura TI de la organización.

Sin embargo, una solución de este tipo suele ser cara y requiere mantenimiento y actualización constantes, de modo que siga representando fielmente cualquier cambio o actualización en el ciberespacio corporativo real. Pero más allá de eso, su efectividad será limitada, ya que realmente no existe una posibilidad práctica de simular ni siquiera todos los procesos comerciales que dependen de esta infraestructura. En muchos casos, esto requerirá el establecimiento de toda una organización ficticia.

Por lo tanto, y en ausencia de tales infraestructuras de simulación (que es, presumiblemente, el caso predominante), la práctica en el entorno real a menudo requiere no solo un uso limitado de sus componentes y recursos, sino también el empleo de componentes y medios separados de él y utilizados solo para la práctica. Este es un principio de acción conocido como "separar el entorno de práctica del entorno real". Como consecuencia, en un ejercicio operativo, la División de Administración debe tener especial cuidado en diseñar los eventos del ejercicio para ayudar a ilustrar el ataque y sus consecuencias y, de esta manera, asegurar en la mayor medida posible que la reproducción del ejercicio basada en ellos compensará, incluso parcialmente, tales compromisos en el entorno de la práctica.

Por su propia naturaleza, la práctica teórica plantea demandas más modestas en este campo. De hecho, en este caso se trata más de una recreación que de una simulación, es decir, de dar un carácter lo más auténtico posible a los sucesos descritos en los eventos del ejercicio. Así, por ejemplo, la cobertura informativa puede recrearse en gran medida proyectando un *flash* noticioso, producido especialmente para ese propósito, en la sala donde se realiza el ejercicio.

Es importante señalar que el uso de ayudas de simulación e ilustración tiene como objetivo inicial mejorar la impresión auténtica que la situación del ejercicio produce en los practicantes con el fin de alentarlos a funcionar "naturalmente" y no, por el contrario, dar al ejercicio una apariencia impresionante. Dado que tales ayudas son un recurso relativamente valioso, dentro de lo posible es aconsejable evitar su uso para crear "pirotecnia" y limitar la inversión en ellas a casos concretos en escenarios que lo justifiquen.



Seguridad en el ejercicio

Sin contradecir lo anterior, y además de lo descrito al principio de la sección, la División de Administración del Ejercicio debe examinar cuidadosamente el escenario y el archivo de eventos del ejercicio en el **aspecto de seguridad**. Si la División de Administración considera que la implementación del escenario puede crear circunstancias en las que puede haber algún riesgo para el ciberespacio corporativo (lo que puede dañar los activos informáticos corporativos e incluso crear daños incidentales), entonces debe nombrar un **veedor de seguridad** para el ejercicio.[31] Este elaborará un **anexo de seguridad** al esquema del ejercicio, que incluirá una serie de instrucciones dirigidas a todos los participantes, cuya finalidad es prevenir la concreción de los riesgos e instruir a los participantes sobre cómo actuar en caso de que se materialice algún riesgo.

Preparación técnica y logística del entorno de práctica

El ejercicio teórico se diferencia del práctico en el aspecto técnico y logístico. Este asunto se discutirá en detalle en los apéndices. Sin embargo, estas dos modalidades también tienen características comunes, como se detalla a continuación:

01

Se recomienda grabar (en video y si no es posible, al menos en audio) durante el transcurso de la práctica. Sea cual sea la documentación de los veedores, nunca podrán documentar por escrito todo lo que se dice. Después del ejercicio, se debe revisar todo el material grabado y extraer de él toda la información necesaria para investigar el ejercicio. Es recomendable hacer esto dentro de una semana a partir de la fecha del ejercicio.

02

Es aconsejable no llevar comida ni medios para preparar bebidas calientes al espacio de ejercicio y contentarse con agua y refrescos, con el fin de evitar lo más posible la distracción de los practicantes. Al mismo tiempo, es recomendable colocar en el exterior, en un lugar accesible y cercano, un puesto que incluirá refrigerios. En un ejercicio que dura medio día, se sugiere brindar a los participantes un almuerzo ligero. En las prácticas que duran un par de días, hay que asegurarse de que la satisfacción de las necesidades de *catering* de los participantes no interfiera con el curso del ejercicio y, en consecuencia, brindarles de manera proactiva y planificada comida y bebida según sea necesario.

03

El acceso al lugar donde se realiza la práctica es de suma importancia. Por lo tanto, los participantes deben recibir indicaciones para llegar en automóvil y transporte público, aproximadamente una semana antes del evento. Además, se debe adjuntar información sobre las disposiciones de estacionamiento disponibles en el lugar.

04

En ocasiones, se necesitará emplear servicios de seguridad especialmente asignados, tanto en el campo físico como en el de la seguridad de la información. La División de Administración debe incluir un plan de seguridad ordenado en la carpeta del ejercicio y garantizar su implementación al realizar el ejercicio, según sea necesario.[32]

31. En caso de que se reconozca la existencia de dichos riesgos, la División de Administración deberá realizar un proceso de análisis de riesgos y determinar la configuración final del escenario y el archivo de eventos del ejercicio de acuerdo con los resultados. Además, el proceso de aprobación del esquema del ejercicio incluirá aprobar la planificación de seguridad para el mismo, prestando la debida atención a los aspectos críticos.

32. Aparte del aspecto de seguridad de la práctica, también hay un aspecto de seguridad propio. Dado que se supone que los ciberataques en el ejercicio son simulados, y teniendo en cuenta que es necesario separar el entorno de práctica del entorno real, el aspecto de seguridad se manifiesta especialmente en el caso de actividades físicas que involucran riesgos de seguridad.

Informar a los practicantes antes del ejercicio

Un ejercicio es en definitiva una especie de juego y, como tal, se realiza en un campo definido y de acuerdo con reglas predeterminadas. Por lo tanto, es muy importante que los practicantes estén bien familiarizados con el campo del ejercicio y las reglas de la actividad antes de la fecha del ejercicio.

Para ello, la División de Administración debe preparar una sesión informativa para los practicantes. Cabe destacar aquí nuevamente que esta información debe incluir el hecho de que el ejercicio no es una herramienta evaluativa de ningún tipo.[33] El momento de la sesión informativa y su énfasis dependen del método de práctica:

01

En un ejercicio teórico se puede proporcionar una breve instrucción (de hasta 15 minutos) al comienzo del ejercicio. Durante el mismo, se recomienda realizar una presentación pública de los participantes. La referencia es principalmente a los que están sentados en la mesa de práctica, en caso de que haya participantes adicionales ubicados de manera diferente. Es importante especificar el horario completo del ejercicio y, en caso de que se realice en dos o más espacios físicos, esto debe anotarse en la explicación de las reglas del juego.

02

En la práctica, donde suele haber una dispersión física/geográfica de los practicantes, una videoconferencia permite superar las limitaciones de tiempo y espacio y realizar la sesión informativa al comienzo del ejercicio. En el caso de que este medio no se halle disponible, se puede realizar una teleconferencia, pero es recomendable concertar previamente una sesión informativa presencial que tendrá lugar aproximadamente una semana antes de la fecha del ejercicio. Si es posible convocar a todos los practicantes en un lugar, alcanza con una sesión informativa; de lo contrario, se deben realizar varias sesiones de este tipo. En la sesión informativa previa a un ejercicio práctico, se recomienda enfatizar en los métodos de comunicación del ejercicio y en las reglas para separar el entorno de práctica del entorno de funcionamiento real de los practicantes (se incluye más información sobre este tema en el apéndice 4).

33. En este contexto, es común definir en inglés el entorno de práctica como *no fault environment*.

/05. Estudiar el ejercicio y aprender de él

El estudio: teoría

El olvido humano amenaza la supervivencia de cualquier conocimiento no documentado y sus efectos son inmediatos. Esto va acompañado de otra tendencia humana: recrear el pasado por medio de la imaginación. Por lo tanto, el proceso de aprendizaje del ejercicio debe comenzar inmediatamente después de su finalización. El primer paso de este proceso es la realización de un **estudio**, que es una ayuda de aprendizaje esencial para cualquier actividad y, por ese motivo, este capítulo se abrirá con declaraciones generales al respecto.

Un estudio (AAR, siglas en inglés para *After Action Review*) es una aclaración de los detalles del desempeño de una actividad particular con base en su propósito, resultados y procesos que tuvieron lugar durante la misma. Todo esto con el objetivo de extraer la mayor parte de la información y los datos necesarios para sacar conclusiones y extraer lecciones. Hay dos tipos de estudio: **interno** y **experto**.

Un **estudio interno** (*debriefing*) se realiza en nombre del organismo responsable de la actividad estudiada y solo participan los funcionarios que intervienen de alguna manera en ella. Su propósito es extraer la mayor cantidad de *insights* que han surgido de la actividad, en un ambiente cerrado y amigable, que permitirá una comunicación abierta y visible.

En virtud de lo mencionado al inicio, es muy importante realizar un estudio preliminar interno,[34] inmediatamente después de la finalización de la actividad estudiada, con el fin de capturar los aspectos más importantes que le conciernen.

El estudio interno tiene dos ventajas principales: la primera es que la información en cuestión se basa en las experiencias de los individuos más cercanos a la actividad investigada, y la segunda, que las lecciones aprendidas con base en esta información servirán directamente a quienes necesitan prepararse para la próxima actividad.

Como tal, el estudio interno es una herramienta de aprendizaje organizacional (y personal) insustituible. Sin embargo, tiene dos limitaciones. En primer lugar, incluso en la atmósfera más amigable de debate los asuntos en cuestión pueden ser deficientes o es posible que triunfe una interpretación distorsionada. En segundo lugar, los participantes en el estudio no son, necesariamente, los más expertos en las áreas de contenido que se investigan.

En función de esto, en muchos casos se acostumbra agregar un **estudio experto** al interno. Este tipo de estudio se realiza sobre temas seleccionados por el organismo que realizó la actividad estudiada, y es llevada a cabo por profesionales expertos. Al mismo tiempo, se debe tener cuidado de que ninguno de estos expertos haya participado en la actividad bajo estudio.

Cabe destacar que si bien un estudio interno es necesario, la decisión de realizar un estudio experto queda a discreción del organismo estudiado. En el caso de que la actividad estudiada apunte a una organización grande o varias organizaciones, se recomienda realizar un estudio interno de manera escalonada: cada organización u organismo que participó en la actividad se estudia a sí mismo e informa los resultados del estudio al nivel a cargo.

34. En inglés se acostumbra llamarla *Hot Wash*.

Cuando se trata de un alcance organizacional limitado o falta tiempo suficiente, es posible realizar un estudio en un formato unificado en el que todas las partes relevantes conducen juntas el estudio interno. No obstante, este estudio inicial no reemplaza un estudio interno ordenado, ya sea que se realice en un formato escalonado o unificado.

Lo anterior es aplicable a cualquier actividad. En lo que respecta al ejercicio, se deben tener en cuenta dos características especiales. La primera se relacionada con el estudio inicial: sin contradecir lo anterior, es importante mencionar que los miembros de la División de Administración pueden participar, pero su contribución activa a la conversación debe limitarse al caso de que los practicantes pidan conocer detalles sobre el escenario del ejercicio y la manera en la que se desarrolla realmente el ejercicio. Esta es información que se definió en un principio como secreto del ejercicio. Por lo tanto, al menos una parte permanece oculta a los practicantes incluso al final del mismo.

Para evitar dudas, no está dentro de la autoridad ni del rol de la División de Administración criticar el desempeño de los practicantes y, excepto por lo mencionado anteriormente, esta debe abstenerse de interferir de cualquier manera en los procesos de estudio del ejercicio.

La segunda es la necesidad de que la División de Administración, al igual que los practicantes, lleve a cabo su propio estudio ordenado, cuyo propósito es examinar hasta qué punto el ejercicio ha tenido éxito en el cumplimiento de los objetivos establecidos. Este estudio también se llevará a cabo en un foro interno, sin la participación de los practicantes.

El estudio: práctica

Este comienza desde el momento en que se realiza el ejercicio. Su primer paso es recopilar la mayor cantidad de información acumulada a lo largo del ejercicio y que los practicantes la documenten. Esto incluye, por ejemplo, registros producidos por sistemas automatizados o redes de comunicación, registros escritos, de operaciones, diversos formularios de informes, etcétera.

Por supuesto, documentar esta información es una condición necesaria para el proceso de aprendizaje del ejercicio.[35] Naturalmente, la información recopilada sin procesar puede contener datos inexactos y otros que son correctos pero no relevantes para las lecciones aprendidas. Por lo tanto, el siguiente paso en el proceso de estudio es verificar los datos recopilados. Lo que se ha reconocido como incorrecto (o incluso no verificable de manera razonable) se elimina de la información recopilada. Los datos que quedan después de este paso se definen como **hechos**. A continuación, se determina cuáles de los hechos son relevantes para las lecciones aprendidas. Entonces, se filtran los que no lo son y se guardan en un repositorio separado, ya que pueden ser relevantes en otros contextos de práctica o reales, actuales o futuros.

Los hechos que quedan después de esta etapa se definen como **hallazgos**. En la etapa final y crucial del proceso de estudio, los interrogadores deben adjuntar los hallazgos en una descripción consistente y lo más completa posible de sus movimientos a lo largo del ejercicio. La combinación se realiza con base en la identificación de las relaciones entre los hallazgos, principalmente del tipo causa-efecto. Por ejemplo, el hallazgo X provocó la ocurrencia del hallazgo Y; el hallazgo X ocurrió en un momento determinado en cierto activo informático de la organización, y dos horas después, el hallazgo de Y, idéntico en esencia y señales, ocurrió en otro de los ciberactivos.

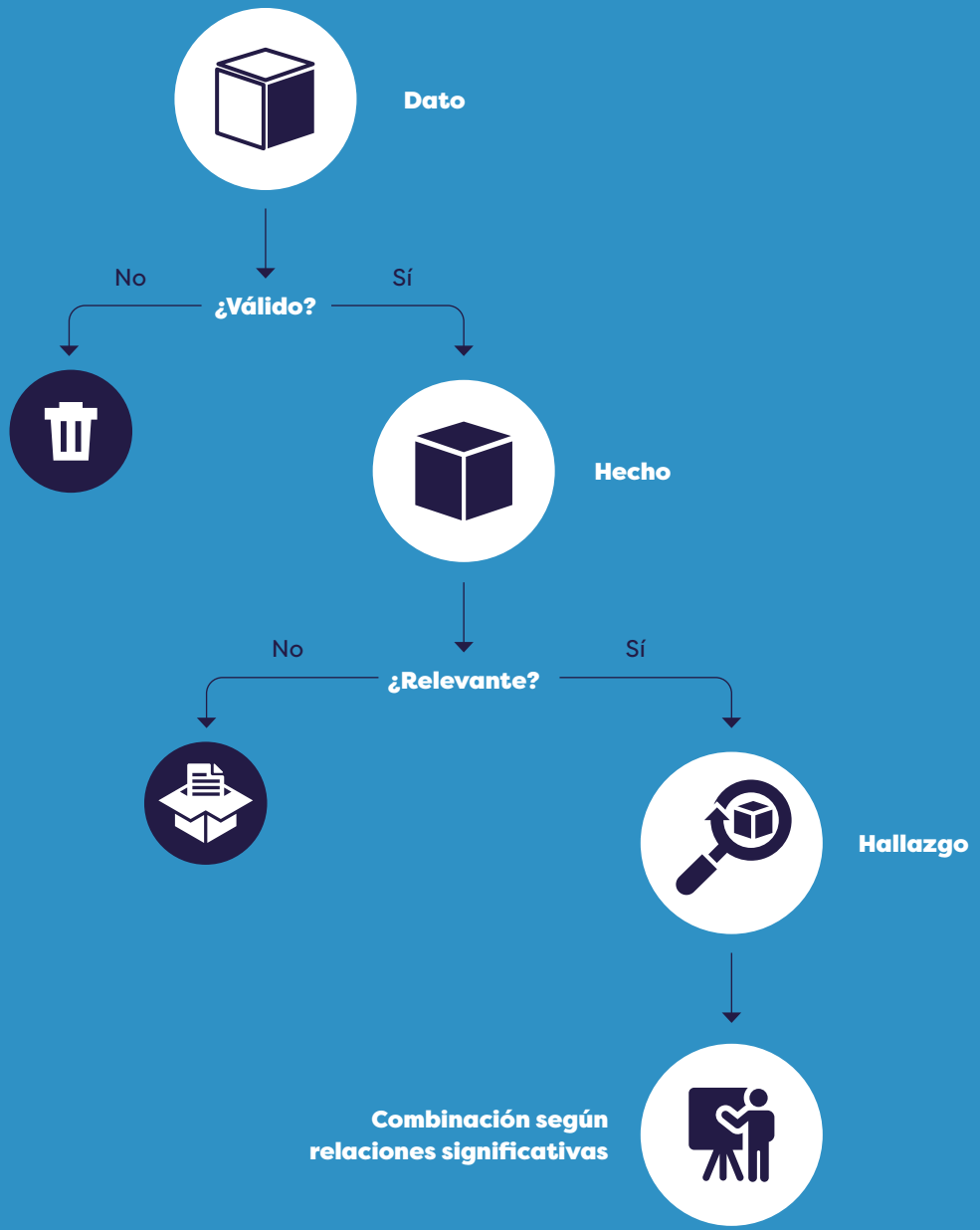
El hecho de que el ciberespacio corporativo sea, por definición, una combinación de activos, facilita la creación de conexiones significativas entre los hallazgos relacionados con estos activos. El gráfico 2 describe el proceso de interrogación de principio a fin.

Se debe buscar que la representación de la combinación de hallazgos sea aceptable para todos los participantes del estudio, ya que esta es una medida importante del grado de confiabilidad. Por lo tanto, este resultado, en lo sucesivo denominado imagen del ejercicio, debe contar con la aprobación de la máxima autoridad dentro de la organización que participó en el ejercicio.[36]

35. La realización de esta condición depende, en esencia, de la cultura organizacional de los practicantes: la existencia de una estrategia panorganizativa. Preguntarse cuál es la misión de la organización, sus metas y objetivos, sus tareas regulares, qué acciones deben tomarse para asegurar la relevancia de la organización para su público objetivo, etcétera. Verificar la existencia de conceptos operativos organizacionales, de procedimientos de trabajo internos, extraorganizacionales e interorganizacionales, etcétera. Por supuesto, este asunto sitúa la eficacia de la práctica organizativa en un contexto más amplio.

36. La esencia de esta confirmación es una declaración oficial de que la representación del ejercicio es una descripción fiel de lo que sucedió a lo largo del mismo. La intención aquí no es examinar en detalle la representación del ejercicio y el proceso de interrogatorio.

Gráfico 2. Proceso de estudio



Lecciones aprendidas

Una vez que se ha resumido y aprobado la imagen del ejercicio, se puede examinar de qué manera se forma a lo largo del ejercicio, de acuerdo con las métricas predeterminadas, como se ha mencionado al comienzo de la guía. De hecho, lo que está en juego se resume en un par de preguntas clave: ¿Por qué sucedió lo que sucedió? ¿Es cierto (dadas las circunstancias) que podría haber sucedido de manera diferente? Las respuestas a estas preguntas son las ideas que servirán de base para extraer lecciones del ejercicio.

> No todo lo que surge de esto es necesariamente nuevo; sin embargo, las perspectivas conocidas también son importantes, ya que cualquier exposición a las mismas aumenta la validez de lo que se dice en ellas y ayuda a establecer convenciones sobre las que se basará el funcionamiento futuro de la organización.

Como continuación directa de esto, los nuevos *insights* o percepciones deben ser bienvenidos, pero también deben tratarse con cierto grado de precaución: las circunstancias de los que surgen pueden haber sido, por ejemplo, una coincidencia extraordinaria. Además, conviene mencionar una y otra vez que se trata de un ejercicio, por lo que es posible que sin la simulación esta coincidencia no hubiera ocurrido en absoluto. Dentro de esta guía se destaca la importancia del fracaso como herramienta de aprendizaje. Por lo tanto, en el contexto aquí discutido debe tenerse en cuenta que los éxitos de los practicantes deben ser estudiados tanto como sus fracasos.

Así como convalidó la imagen del ejercicio, la Dirección de la organización también debe confirmar la lista de ideas formuladas sobre su base. La información aprobada se define como una **lección** y, como tal, tiene un estado vinculante en la organización. La siguiente es una lista de los componentes clave acerca de la preparación organizacional que las lecciones pueden tratar:

01

Planes de trabajo y procedimientos de la organización.

02

Estructura de cada organismo o de la organización en su conjunto.

03

Procesos de gestión de la organización (los procesos de flujo de información en la organización y los mecanismos de toma de decisiones basados en ellos).

04

Recursos organizativos (mano de obra; sistemas de tecnologías de la información y la comunicación [TIC], como *hardware* y *software;* otros sistemas; medios logísticos; presupuestos, alcance y distribución, etcétera).

En el lenguaje común de muchas organizaciones, se acostumbra distinguir entre una lección para preservar (un *insight* que señala una fortaleza digna de ser preservada) y una lección para mejorar (que señala una falla, debilidad o deficiencia que requiere corrección). Este acto de aprobación es de gran importancia, ya que una lección no solo enseña algo sobre la organización y su función, sino que también implica un deber de actuar que deviene de ella.

En otras palabras, una lección aprendida no tiene sentido a menos que también se aplique. Por lo tanto, las lecciones aprendidas deben "traducirse" en tareas e incorporarse al plan de trabajo de la organización. Dado que el aprendizaje es un proceso circular, la forma en que se aplican las lecciones y sus resultados reales deben volver a examinarse en los ejercicios futuros de la organización, los cuales también están diseñados para aprender y aplicar lecciones.

Documentación del proceso

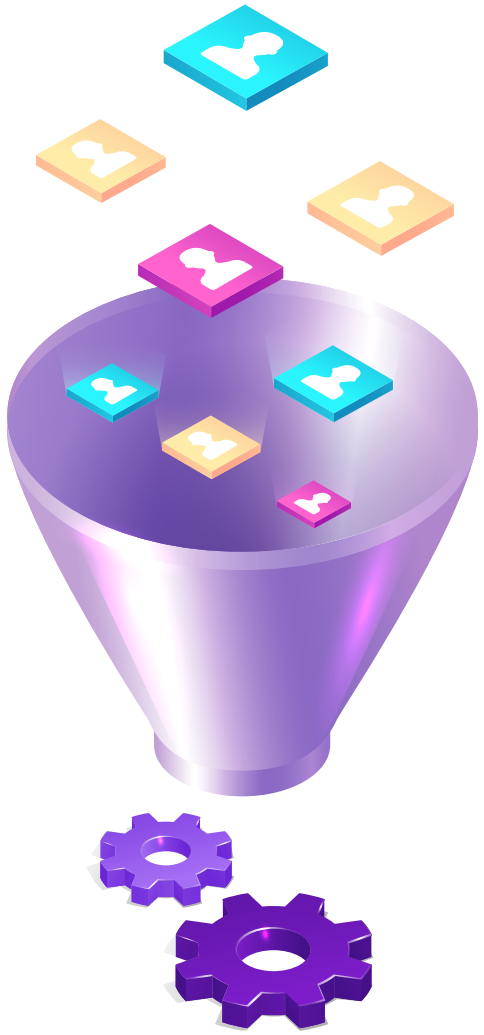
Una vez finalizado el proceso de aprendizaje, la Unidad de Ejercicios publicará un informe para la Dirección de la organización, los practicantes, la División de Administración del Ejercicio y cualquier otra parte interesada, el cual debe incluir lo siguiente:

- **Esquema del ejercicio.**
- **Desarrollo concreto del ejercicio:** puntos principales a destacar.
- **Lecciones del ejercicio:** este componente incluirá la determinación del organismo responsable de aplicar cada lección. Cabe destacar que estos no son planes de trabajo para la aplicación de las lecciones, ya que estos serán elaborados y publicados por los órganos responsables de su implementación.
- **Lecciones de la División de Administración:** *insights* sobre el ejercicio en sí (la carpeta de ejercicios y cómo se implementa en concreto) y las acciones que la Unidad de Ejercicios pretende tomar con base en los ejercicios futuros de la organización.

Apéndices

Panorama general

En línea con lo explicado al inicio, el contenido de esta guía se centra en la conceptualización del mundo de la práctica, con un mayor énfasis en la práctica dentro la dimensión cibernética. Sobre esta base se establecen los cuatro apéndices, dedicados —cada uno en su propio ámbito— a las acciones concretas que deben realizar la Unidad de Ejercicios y la División de Administración de cada ejercicio, con el fin de construir y gestionar ciberejercicios.



En consecuencia, se centran en temas seleccionados que requieren una mayor profundidad y mayor detalle, por lo que se recomienda leerlos solo después de leer el contenido de la guía. El apéndice 1 se centra en el proceso de elaboración del esquema de un ejercicio de ciberseguridad.

Apéndice 1. Directrices para elaborar un esquema de ejercicio de ciberseguridad

Esquema del ejercicio y programa de ejercicios organizativos

Como ya se explicó, los esquemas de ejercicios incluidos en el **plan de trabajo anual** de la organización forman parte integral del **plan de ejercicios anual**, por lo que deben planificarse durante su construcción.

Asegurar esto no solo permitirá a los practicantes prepararse con anticipación para todos los ejercicios, sino también les proporcionará anclajes durante el año laboral, a la luz de los cuales podrán probar sus habilidades y preparación frente a posibles eventos de la vida real. Por lo tanto, la Unidad de Ejercicios debe elaborar el plan de ejercicios anual de manera que refleje fielmente las metas de competencia y preparación de la Dirección de la organización para ese año de trabajo.

Al elaborar el plan anual, se deben tener en cuenta las constantes de tiempo típicas de preparación de los distintos tipos de ejercicios. Un ejercicio teórico requiere por lo general un período de preparación de uno a dos meses, mientras que el ejercicio operativo requiere una preparación más prolongada; por lo general, de tres a cinco meses.

Otro tema a considerar al determinar la combinación de ejercicios teóricos y prácticos a lo largo del año es el hecho de que la práctica teórica siempre puede servir como base para la práctica concreta.

Proceso de construcción del esquema

El proceso de construcción del esquema incluye las siguientes tareas:

01

Determinar los objetos de aprendizaje del ejercicio (objetivo, composición de los practicantes, subobjetivos y temas de práctica).

02

Establecer el formato de la práctica.

03

Definir el cronograma según el cual se llevará a cabo el proceso de preparación de la División de Administración y practicantes para el ejercicio (que incluye establecer fechas concretas para los eventos relevantes a partir de los cuales se construye el proceso).

04

Determinar los recursos necesarios para la planificación y realización del ejercicio (presupuesto, mano de obra, ubicación física del ejercicio, medios tecnológicos y logísticos, etcétera). Esto deberá programarse en un calendario como parte del plan general de trabajo.

Determinar el propósito del ejercicio

La construcción del esquema del ejercicio comienza con la determinación del propósito del ejercicio. El objetivo debe formularse en términos que se relacionen directamente con el ciberespacio organizacional y, más precisamente, con la visión de mejorar y promover la resiliencia de la organización en el ciberespacio. Sin embargo, como ya se ha explicado, el ciberespacio organizativo no se sostiene por sí solo, por lo que, como norma, es necesario abordar en esta materia también la continuidad de la función organizativa y empresarial.

Puede aplicarse una excepción en el caso de un ejercicio a nivel técnico-táctico (como el destinado al personal tecnológico y operativo de bajo rango, a cargo de la ciberseguridad de la organización). Por supuesto, el establecimiento de objetivos debe basarse en toda la información relevante acumulada en la organización hasta ese momento, incluidas las lecciones aprendidas de ejercicios anteriores.

Los objetivos típicos que por lo general se recomiendan y se establecen para un ejercicio cibernético son los siguientes:

01

Sensibilizar a la Dirección de la organización sobre la importancia de la ciberseguridad.

02

Sensibilizar a los empleados de la organización sobre la importancia de la ciberseguridad.

03

Exponer brechas en la ciberresiliencia organizacional en sus diversos aspectos (debilidades y vulnerabilidades en la arquitectura de los sistemas TI de la organización; su dependencia de las cadenas de suministro; los procesos de ciberseguridad establecidos o practicados en ella; la efectividad y eficiencia de sus mecanismos técnicos de defensa existentes, etcétera).

04

Exhibir brechas en la competencia y preparación del personal responsable de la ciberseguridad organizacional.

05

Exponer brechas en la competencia y preparación del personal de la organización, tanto a nivel individual como colectivo.

Una vez formulado, el objetivo planteado indica el nivel en el que se realizará el ejercicio (estratégico, operativo o técnico-táctico). De ahí también se deriva su influencia decisiva en los practicantes. De hecho, los objetivos 1 y 2 determinan esto —aunque no específicamente— ya en su redacción: ambos están dirigidos al ejercicio a nivel estratégico.

El objetivo 3 está dirigido en esencia al nivel operativo, pero también puede dirigirse al nivel táctico. En el primer caso, el punto de vista de la División de Administración será sistémico, por lo que la mayoría de los practicantes serán gerentes senior y junior responsables de llevar a cabo los procesos de ciberseguridad en la organización. En el segundo caso, se refiere a la práctica de personal seleccionado dentro de la organización, o incluso de un solo empleado. Por lo tanto, los practicantes serán tanto los gerentes como al menos algunos de los empleados involucrados.

Los objetivos 4 y 5 son tácticos e incluso técnico-tácticos, por lo que los practicantes serán principalmente empleados en diferentes áreas de especialización, siendo el área de especialización del empleado mucho más importante que su nivel de antigüedad.

Es importante mencionar que no solo es correcto establecer un solo objetivo de práctica, sino que es muy aconsejable centrarse en la práctica de un único nivel organizacional.

Puede ser sensato aprovechar la propia realización del ejercicio para abordar una serie de objetivos o, al menos, para entrenar más de un nivel principalmente por razones de eficiencia y ahorro de recursos. Sin embargo, este intento probablemente socave la efectividad del ejercicio, en consonancia con el dicho "el que mucho abarca, poco aprieta". Esto se explica porque las actividades de cada nivel se llevan a cabo en gran medida a partir de una lógica interna que le es única.

Los intereses estratégicos no solo son diferentes de los tácticos, sino que a veces incluso pueden contradecirse entre sí.

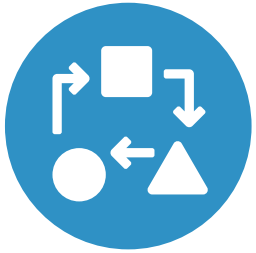
Dado que cada nivel considera un deber promover los intereses con base en los cuales opera, la práctica de cada nivel crea un ejercicio separado. Es cierto que esto también plantea un desafío, ya que cada nivel lidia con conflictos de intereses en sí mismo y con otros niveles organizacionales. Pero esto no requiere entrenar a los otros niveles, sino que es suficiente con que sean simulados por la División de Administración del ejercicio a través de roles apropiados.

Determinar el formato de la práctica

Una vez determinado el objetivo del ejercicio y el conjunto de practicantes, se pueden decidir los subobjetivos y temas de la práctica. El siguiente paso en el proceso de construcción del esquema también es la transición del "qué" (¿cuál es el propósito del ejercicio?) al "cómo" (¿cómo se realizará este propósito?). Tras la discusión presentada en la guía, el formato más apropiado para la práctica, basado en el objetivo 1, es un **TTX** o un **juego organizacional**. Por el contrario, el formato más apropiado para los objetivos 2 y 4 es un ejercicio operativo. El objetivo 3 es, por su propia definición, bastante amplio, por lo que se requiere una definición lo más precisa posible de los subobjetivos y temas de práctica derivados de él para poder seleccionar el formato de práctica más adecuado para su realización.

En general, si la materialización del propósito del ejercicio requiriera un amplio funcionamiento sistémico de la organización, sería aconsejable realizar un **ejercicio operativo**. Por el contrario, si la práctica se enfoca solo en ciertos componentes de la actividad en su conjunto, ciertos aspectos de la misma o ciertas secciones transversales de toda la organización, entonces sería aconsejable realizar un **TTX** o un **juego organizacional**.

Cabe señalar que el formato de práctica que se construirá en el esquema puede adoptar muchas formas concretas: las características de la práctica, tal como se definen en esta guía (especialmente el TTX y el juego organizacional), son más que nada tipos representativos primarios, cada uno de los cuales puede incorporarse físicamente en una variedad de formas. El factor decisivo para influir en el diseño del formato de práctica que se utilizará en el ejercicio es el conjunto de aquellas características únicas de la organización, que inciden en el propósito del ejercicio y, específicamente, la ubicación y posicionamiento de cada practicante dentro de la estructura organizacional. En el recuadro A1.1 se presenta un caso representativo para ilustrar lo anterior.



Recuadro A1.1. Ejercicio de simulación de mesa para la compañía X

Una compañía X, que pertenece a la industria química, posee un número de plantas de fabricación que consumen y también producen una serie de sustancias peligrosas. A la luz de esto, la compañía ha establecido un plan de preparación para hacer frente a situaciones de crisis, ya sea una inminente en el horizonte cercano o una que ya se está produciendo. El plan engloba tanto a la alta dirección del grupo como a todas las fábricas que lo integran. Tras una revisión exhaustiva del plan, se le realizaron cambios sustanciales y, por lo tanto, la Junta Directiva decidió examinar el alcance de su eficacia y las implicaciones de su adopción real. Para ello, la Unidad de Ejercicios del grupo ha construido un ejercicio para su Dirección central y para las Gerencias de todas sus plantas de fabricación. Con base en el enfoque del ejercicio, se entendió que este sería teórico y, en consecuencia, se determinó que se realizaría en formato de cuadro. Teniendo en cuenta la estructura organizativa de la compañía, los practicantes se dividieron en equipos de acuerdo con su afiliación (fábricas, alta dirección) y el curso del ejercicio se construyó como se describe en el cuadro de página siguiente.

Como se puede observar en el cuadro, la Unidad de Ejercicios ha optado por llevar a cabo un ejercicio de simulación de mesa mediante la creación de equipos con representantes de cada una de las gerencias de la empresa. A cada equipo se le dio la oportunidad de converger dentro de sí mismo para hacer frente a los desarrollos del escenario. Además, la Unidad de Ejercicios también estableció reglas que regulan el intercambio de información entre los equipos y ellos mismos durante el trabajo en el foro de equipo.

Al mismo tiempo, también se ha establecido un marco para el mapa de situación a nivel de toda la compañía.

Si bien la manera en que se diseñó el formato de ejercicio no pasó del plano teórico al práctico, esto le dio al ejercicio un carácter más dinámico y, en cierta medida, más cercano a la vida real. Todo esto sin apartarse del marco general de la práctica en formato de cuadro, como lo demuestra la duración general del ejercicio, el alcance de los practicantes, su composición y la naturaleza relativamente íntima del evento en su conjunto.

Hora	Evento	Escenario
09:00–09:30	Reunión plenaria: apertura, sesión informativa general y primera transmisión de información.	Salón Plenario
09:30–10:15	Trabajo en equipo: segunda transmisión de eventos, división del equipo.	Salas de reunión del personal
10:15–11:15	Reunión plenaria: mapa de situación, discusión libre y tercera transmisión de información.	Salón Plenario
11:15–12:00	Trabajo en equipo: cuarta transmisión de información, división del equipo.	Salas de reunión del personal
12:00–13:00	Reunión plenaria: mapa de situación, discusión libre y resumen del ejercicio.	Salón Plenario
13:00–14:00	Investigación preliminar	Salón Plenario

Aprobación del esquema del ejercicio y su publicación

Una vez finalizada la construcción del esquema del ejercicio (que incluye también la preparación del indicador del ejercicio), este debe ser aprobado en el nivel responsable correspondiente. En general, es aconsejable que el nivel del organismo de certificación sea superior al del practicante más experimentado o al menos idéntico a él. Esto tiene como objetivo, ante todo, obtener el respaldo y apoyo del nivel a cargo del ejercicio, coordinar con este las expectativas en cuanto al propósito del ejercicio y convertirlo en socio en todos los esfuerzos invertidos en la preparación y edición del mismo.

Tras la aprobación del esquema, este debe publicarse oficialmente con el fin de ponerlo en conocimiento de la Dirección de la organización, los practicantes y cualquier otra parte involucrada en la preparación y edición del ejercicio. Al hacerlo, se debe tener cuidado de que la información publicada no incluya detalles que se supone que están ocultos al conocimiento de los practicantes. La referencia es, en particular, al archivo de eventos del ejercicio. Además, no debe incluirse en la publicación la historia de fondo del ejercicio (en caso de que se haya decidido preparar una), ya que la misma debe distribuirse a los practicantes aproximadamente una semana antes de la fecha del ejercicio.

Publicación del esquema del ejercicio

Es cierto que los lineamientos generales de los ejercicios incluidos en el plan de trabajo anual de la organización se publican entre los empleados como parte de su plan de trabajo general hacia el comienzo del año en cuestión. Sin embargo, aproximadamente un mes antes de cada ejercicio, la División de Administración debe difundir su esquema específico a los practicantes y cualquier otro personal relevante para asegurar que estén al tanto del ejercicio inminente y, por lo tanto, puedan comenzar con la preparación adecuada para el mismo. Aunque el esquema se haya preparado incluso antes del inicio del año de trabajo, este momento brinda una oportunidad para que la organización lo vuelva a examinar y se asegure de que realmente refleja de manera fiel las expectativas del ejercicio.

Apéndice 2. Directrices para la creación de un escenario de ejercicio de ciberseguridad

Panorama general

En cuanto al calendario, la actividad descrita en el apéndice 1 tiene lugar antes de la apertura de un nuevo año de trabajo de la organización y la realiza su Unidad de Ejercicios. Por el contrario, todo lo que se describe a continuación ocurre antes de la fecha de cada ejercicio y lo realiza la División de Administración del Ejercicio, la cual, como se mencionó, es un organismo temporal y exclusivo establecido *ad hoc* con base en la estructura permanente de la Unidad de Ejercicios.

Mecanismo de construcción del escenario

Los practicantes actuarán como **funcionarios** y realizarán **tareas *ad hoc*** derivadas de los temas de práctica, con el fin de lograr **los objetivos requeridos por la organización**. Esta dinámica se implementa a través de los procesos de trabajo definidos para ese fin.

Las acciones de ataque incluidas en el escenario tienen como objetivo **desafiar** esta dinámica, dañando metódicamente los puntos débiles presentes en los procesos relevantes de trabajo. Detrás de estas vulnerabilidades se encuentran los activos cibernéticos de la organización (como un controlador computarizado instalado en la infraestructura de producción de la organización o un componente de *software* instalado en su infraestructura de TI), cada uno de los cuales está expuesto a algún tipo de vulnerabilidad.

Se recomienda que estas vulnerabilidades sean conocidas o similares a aquellas presentes en el ciberespacio.[37] Esto aumentará la credibilidad del escenario a los ojos de los practicantes. En cualquier caso, es importante que estas debilidades sean razonables. En este contexto, es fundamental refinar el requisito de que el escenario sea realista, justificado y desafiante: no hay impedimento para incluir un escenario de ciberataque cuyas posibilidades de materializarse han sido evaluadas por la organización como muy bajas, pero cuyo potencial de daño es alto.

37. Como se ha mencionado, estas vulnerabilidades fueron identificadas con anticipación y seleccionadas como foco de interés, como parte de la determinación de los subobjetivos y temas del ejercicio. También es importante enfatizar que no necesariamente son vulnerabilidades integradas en el *hardware* o *software*, sino también pueden ser aquellas que resultan de una mala definición o gestión de los activos cibernéticos de la organización como, por ejemplo, una mala política de derechos de usuario o mala configuración de las medidas de ciberseguridad instaladas.

Tampoco hay impedimento alguno para utilizar un ciberataque que, al menos según publicaciones de fama mundial y hasta la fecha de construcción del escenario, aún no se haya reconocido como una amenaza.[38]

Lo que se requiere es que la División de Administración proporcione una base lógica adecuada para el inicio y ejecución de dicho ataque (intenciones y capacidades de un ataque y la viabilidad de realizar el vector de ataque). Después de todo, debe tenerse en cuenta que esto es un ejercicio y no un experimento o una discusión tecnológica.

La secuencia lógica descrita anteriormente se aplica, en efecto, en orden inverso mientras la División de Administración construye cada ejercicio de ciberataque, al igual que un ciberatacante planea un ataque concreto que pretende realizar.[39]

Por lo tanto, se deduce que el primer paso en el proceso de planificación del ejercicio de ciberataque es determinar el daño operativo que se causará a la organización. Ante todo, la División de Administración debe dar forma al **proceso de deterioro de la imagen operativa panorganizativa** en el ejercicio.

Esto servirá como punto de partida para construir cualquier ciberataque que se incluya en el escenario, pero, no menos importante, ayudará a la División de Administración a desplegar la **cibercrisis** en la que se encontrará la organización como resultado de lo que está sucediendo en el escenario. Hay dos tipos de cibercrisis, cuyas diferencias radican tanto en la forma en que ocurren en la línea de tiempo como en la forma en que se desarrolla la comprensión de la organización de lo que realmente ocurre:[40]

38. En este contexto, vale la pena mencionar el término cisne negro (como lo define Nassim Taleb), que es un fenómeno poco común que tiene un gran impacto y resulta aparentemente impredecible, pero que se puede estimar que ocurra en algún momento. No hay ningún impedimento para introducir un cisne negro en el escenario, siempre que se incorpore de manera convincente al tejido general de los eventos.

39. En cuanto a su lógica, el proceso de construcción del ataque se basa en los modelos de ciberataque conocidos y aceptados (como, por ejemplo, el *kill chain* de la empresa Lockheed Martin, que aparece en el modelo iceberg presentado en el gráfico 1).

40. A esto se le llama comúnmente comprensión situacional. De hecho, la comprensión situacional de todos los practicantes, y especialmente de aquellos miembros de la Dirección de la organización, es uno de los principales temas a investigar después del ejercicio, ya que da fe de su capacidad para gestionar la cibercrisis. Es decir, construir una situación que refleje la realidad, tomar decisiones informadas, implementarlas de manera efectiva y eficiente, revisar el resultado, etcétera.

01

Forma en desarrollo: al comienzo del ejercicio todavía no hay signos de daños operativos o comerciales a la organización (es decir, a primera vista el negocio parece normal). Al mismo tiempo, hay señales que pueden indicar, como mínimo, una actividad hostil que amenaza el ciberespacio corporativo. Por lo tanto, la situación general se está deteriorando y ya comienzan a producirse ciberataques contra la organización. Como resultado, también se está empezando a infligir daños tangibles operativos o comerciales a la organización.[41]

02

Forma repentina: los ciberataques comienzan a ocurrir al inicio del ejercicio, aunque puede ser que los practicantes aún no los hayan diagnosticado. Estos ataques causan daños tangibles operativos o comerciales a la organización. A partir de este punto, la situación general sigue empeorando.

41. Un caso especial de crisis en evolución es aquel en el que hasta el final del ejercicio no hay ciberataques reales. Su uso es principalmente adecuado para la práctica teórica y, especialmente, para el formato de un juego organizacional.

Vulnerabilidades organizativas y su ataque

El proceso descrito anteriormente finaliza, por lo tanto, con la determinación de los puntos débiles del ciberespacio organizativo hacia los que se dirigirán los ciberataques que se incluirán en el escenario. Las siguientes son formas típicas de tales vulnerabilidades:

01

Un activo cibernético común en la organización.

02

Un activo cibernético que es un punto único de falla (SPOF, por sus siglas en inglés).

03

Un activo cibernético que sea un eslabón esencial en uno de los procesos organizacionales que se ha decidido perjudicar en el marco del escenario.

04

Un activo cibernético que respalda la cadena de suministro de la organización.

El siguiente paso es ajustar los ataques contra las debilidades de los activos cibernéticos seleccionados. Por razones relacionadas tanto con la credibilidad del escenario como con el control de la División de Administración durante el ejercicio, es aconsejable que el número total de ataques en el escenario esté entre uno y cinco. Al mismo tiempo, se recomienda que los ataques se construyan en un esquema que les permita ramificarse durante el ejercicio, e incluso conectarse entre sí. El producto obtenido será un escenario **complejo**, en contraposición a un escenario **agitado**.

Un escenario complejo presentará a los practicantes un desafío importante para dar una interpretación correcta a las señales que aparecerán en los eventos del ejercicio, con el fin de construir una situación que refleje fielmente la verosimilitud de los mismos.

Un desafío igualmente significativo que enfrentarán es la gestión operativa para hacer frente a los ataques. Incluso cuando la representación es correcta y completa, se espera que la situación presente dilemas a los practicantes en cuanto al curso de acción en el que sería correcto actuar.

En otras palabras, un escenario complejo servirá fielmente a la necesidad de desafiar a los practicantes en dos niveles de actividad organizacional: preservar la continuidad de los procesos organizacionales críticos y habilitar y mantener un ciberespacio libre de ataques.

Ejercicios de ruido

Como ya se explicó anteriormente, para asegurar la credibilidad del escenario y efectividad del ejercicio, los ciberataques deben combinarse con eventos de ruido. Es decir, cualquier eventualidad en el contexto del ciberespacio corporativo que no es un ciberataque ni deriva del mismo. Esto incluye fallas técnicas y operativas, así como señales incorrectas de varios indicadores, principalmente en infraestructura y sistemas de producción, pero también en infraestructura y sistemas TI.

Los eventos de ruido deben tener un carácter creíble y, por ese motivo, deben tomarse de los contenidos, funcionalidad y experiencia de los practicantes.

Más allá de eso, es importante que las señales que atestiguan estos eventos de ruido sean similares, acaso idénticas, a las que indican los ciberataques incluidos en el escenario. Finalmente, a pesar de que estos eventos son secundarios, mientras que los ciberataques son principales, es importante construirlos de una manera que motive a los practicantes a actuar como si fueran ataques reales. Todo esto ayudará a desafiarlos tanto en el análisis de las señales (la propia acción llamada triaje) como en la construcción de la imagen del ejercicio, y en la gestión de su respuesta operativa a la luz de la situación. Al mismo tiempo, debe tenerse en cuenta que los eventos de ruido no tienen valor en sí mismos, por lo que debe cuidarse de que su dosis en el escenario no sea excesiva.

Para concluir esta discusión, el recuadro A2.1 ofrece un ejemplo de un evento de ruido en el mundo de los sistemas de TI, que replica la tensión incorporada entre el nivel operativo y el nivel de TIC de la organización.

Recuadro A2.1. Ejemplo: eventos de ruido

Como parte de la práctica de una gran cadena minorista, la División de Administración construyó un evento de ruido en el que, durante la actualización del precio de un producto en particular, se ingresó accidentalmente el dígito cero en lugar de otro dígito en la base de datos de la red. El producto en cuestión se vende solo en algunas de las sucursales de la cadena y, en consecuencia, esta actualización se ha distribuido solo a ellos. En ese momento, los puntos de venta en estas sucursales colapsaron debido a una división a cero realizada por un determinado algoritmo en su sistema operativo.

En el momento de difundir los eventos del ejercicio relativos a este incidente, la red ya estaba sujeta a ciberataques y los practicantes eran muy conscientes de ello. A raíz de todo esto, se enfrentaron a un dilema: ¿asumían que se trataba de otro ciberataque y, en consecuencia, quizás deshabilitaban voluntariamente los terminales de venta en las otras ramas de la cadena, o se arriesgaban a que fuera un mal funcionamiento y dejaban que los terminales de venta de las demás sucursales siguieran funcionando correctamente?

Ciberataque versus incidente cibernético: derivar conocimientos del ejercicio a partir del escenario

El extenso título de este apartado tiene como objetivo diferenciar entre el ángulo desde el que la División de Administración observa los detalles del escenario y el ángulo desde el que los practicantes los ven. Dado que construyó el escenario, la División de Administración sabe por qué y cómo sucedió todo en él. En cambio, los practicantes ven solamente los eventos del ejercicio, que no representan más que los resultados (efectos) visibles de la cadena de eventos que la División de Administración ha construido. De esta manera, por ejemplo, si bien la División de Administración sabe que uno de esos efectos es un incidente de ruido (y no un ciberataque), los practicantes pueden interpretar las señales como si fuera un evento de ciberseguridad.

La diferencia entre estas dos perspectivas es una característica esencial de la acción práctica y refleja, a su manera, la diferencia inherente entre la visión del atacante y la del defensor. Con base en esto, al derivar un conocimiento práctico del escenario, es extremadamente importante asegurarse de que la información que se transmite refleje de la mejor manera lo que los practicantes habrían sabido si las cosas hubieran sucedido en la realidad. En el recuadro A2.2 se presenta un ejemplo para ilustrar este punto.

En el ejemplo, el boletín en cuestión no puede en sí mismo indicar que el origen del problema es un ciberataque contra el sistema de pago digital, por lo que los practicantes tienen la responsabilidad de investigar lo que está sucediendo para averiguarlo. Por supuesto, la dinámica aquí descrita es exactamente lo que la División de Administración buscaba provocar, es decir, motivar a los practicantes a actuar de una determinada manera, preservando la naturaleza realista y auténtica del hecho.

Derivar conocimientos del ejercicio a partir del escenario es el primer paso (de dos) para realizar el componente de simulación en el ejercicio. Este paso se lleva a cabo antes de realizar el ejercicio. El segundo paso es gestionar el proceso de transmisión de la información a los practicantes y tiene lugar durante el ejercicio. De hecho, es el núcleo de ocupación de la División de Administración en este marco. Más información al respecto en el apéndice 3.

Recuadro A2.2. Ejemplo: derivar conocimiento práctico a partir del escenario

Como parte de una práctica del sistema de transporte público terrestre, en la que también participaron los actores políticos relevantes, la División de Administración construyó un ciberataque a la infraestructura de pago digital que lo sostiene. Como resultado, los sistemas de compensación en autobuses y estaciones de tren dejaron de detectar los medios de pago digitales en poder de los pasajeros, lo que provocó graves perturbaciones en el funcionamiento del transporte público.

Para aprovechar los eventos del ejercicio derivados de este ataque, la División de Administración examinó la secuencia de este incidente: los conductores de autobús y los trabajadores en las estaciones de tren serían, presumiblemente, los primeros en notar la ocurrencia anormal. A su vez, se espera que los viajeros muestren un gran resentimiento por lo que está sucediendo y, en la era actual, esto pronto encontrará un eco generalizado en las redes sociales. A partir de ahí, también llegará muy rápidamente a los medios de comunicación masiva.

Al mismo tiempo, es probable que este resentimiento dé lugar a diversas manifestaciones de violación del orden público, por lo que la policía también se verá involucrada. Este proceso de derivación, basado en la lógica simple de una cosa lleva a la otra, condujo a la División de Administración a generar informes sobre los conductores en los centros de operaciones de las compañías de autobuses, información paralela sobre la infraestructura ferroviaria y noticias de los medios que informan sobre la interrupción, así como sobre los disturbios y el alboroto que se está extendiendo entre el público en general.

Adicionalmente, la División de Administración agregó un evento con una solicitud de la policía a los funcionarios del gobierno con respecto a la aclaración de los detalles del incidente y cómo proceder con su tratamiento.

Apéndice 3.
Directrices para llevar a cabo un ejercicio de simulación y un juego organizacional de ciberseguridad

Panorama general

La diferencia entre el método teórico y el práctico se percibe de manera notable en la diferencia entre los métodos de ejecución reales de los ejercicios realizados de acuerdo con estos dos métodos. Así, este apéndice se ocupará de la realización de un TTX y un juego organizacional y el apéndice 4, de la realización de un ejercicio operativo. Aunque los puntos que se presentan a continuación están dirigidos a un nivel práctico, las limitaciones comprensibles de la extensión de esta guía requieren enfocarse solo en los puntos clave, y no deben verse como una receta que se puede aplicar de manera directa.

Marco temporal

La duración total de un TTX no debe exceder el medio día (por lo general, un período de una hora y media a tres horas puede ser suficiente). También es recomendable llevarlo a cabo en la primera parte del día.

Entorno de práctica

En su configuración clásica un TTX se realiza alrededor de una sola mesa. Esto significa que los practicantes se sientan en esta mesa, ya que es importante asegurarse de que todos se vean. De ahí que sea habitual denominar mesa redonda al ejercicio de este tipo. Pero la mesa no tiene necesariamente que ser redonda y, en cualquier caso, tiene un punto final o, más exactamente, una cabecera, que es una zona de asientos diseñada para el **facilitador del ejercicio** (véase el apartado: Coordinación del ejercicio).

En la práctica, debido a las limitaciones involucradas en la forma de ejecución física del ejercicio, es posible que no haya espacio alrededor de la mesa **para todos los practicantes**. Esto ocurre cuando al menos algunas de las funciones ejercidas no están representadas por un solo funcionario, sino por un equipo de varios funcionarios. En tal caso, se puede colocar un círculo adicional de asientos (el segundo círculo), que rodeará desde el exterior esta mesa y sus asientos (el primer círculo).

De esta manera, el funcionario de más alto rango (o el principal, en términos de objetivos y temas del ejercicio) del equipo estará sentado en el primer círculo, y todos los demás se colocarán en el segundo círculo, detrás de él y junto a él. El segundo círculo también está destinado para miembros de la División de Administración del Ejercicio (es costumbre que el jefe administrativo se siente en el primer círculo), incluidos los funcionarios y veedores.

Cabe destacar que la comunicación del ejercicio debe tener lugar, al menos mayormente, entre los ocupantes del **primer círculo**. Por lo tanto, para asegurar la efectividad y eficiencia de la comunicación en torno a la mesa, es importante asegurarse de que el número total de personas sentadas en el primer círculo sea, **como máximo, de entre 20 y 30**. Sin embargo, el número total de practicantes puede ser mayor y, debido a eso, es necesario ajustar el tamaño de la sala donde se realiza el ejercicio al número total de participantes.

Como ya se explicó, por regla general, llevar a cabo un ejercicio de simulación se caracteriza por la unidad de tiempo y espacio. Por lo tanto, este formato de práctica es particularmente apropiado para cualquier situación en la que, por ejemplo, no se presenten consideraciones de privilegios de divulgación de información o mandatos que surgen de una estructura organizacional, que pueden requerir la segmentación interna de practicantes los unos de los otros. Alternativamente, los objetivos del ejercicio pueden ser tales que para alcanzarlos los planificadores del ejercicio elijan eliminar dichas particiones de manera deliberada.

Sin embargo, a veces es correcto y necesario tener una segmentación interna de los practicantes con el fin de realizar la práctica. El caso típico y común es el del **juego organizacional**. En tales circunstancias, la práctica no se puede llevar a cabo en un espacio común y, por lo tanto, los practicantes se dividen en equipos, cada uno de los cuales se ubica en una sala separada (o en una misma sala pero a una distancia adecuada del otro equipo).

Dado que cualquier equipo de este tipo opera en condiciones de unidad de tiempo y espacio, todo lo que se ha escrito anteriormente en relación a esto se aplica a dichas condiciones. Además, incluso en un juego organizacional probablemente será necesario reunir de vez en cuando a todos los practicantes en un espacio (plenario).

La reunión plenaria se utiliza principalmente con el propósito de realizar un mapa de situación, que permite a los practicantes y a la División de Administración comprender el panorama general del ejercicio. Por supuesto, el resumen del juego organizacional y su investigación inicial también se realizarán en el plenario.

Coordinación del ejercicio

Como se ha mencionado, el área de asientos en la parte superior de la mesa está asignada al facilitador del ejercicio. Su trabajo es coordinar la comunicación del ejercicio (la División de Administración, en cambio, despliega el escenario), pasando la información al primer círculo para ayudarlo a lograr los objetivos planteados. El facilitador puede ser también un practicante (y en este caso, su verdadero rol organizacional tiene una clara importancia directiva en el ejercicio). Alternativamente, puede ser un miembro de la Junta (pero generalmente no el director de la misma). Puede haber casos en los que su rol sea de naturaleza puramente directiva (es decir, no desempeñará ningún rol de cliente dentro de la organización y tendrá una afinidad directa y práctica con los temas y propósitos del ejercicio). Por tanto, el facilitador debe:

01

Tener experiencia gerencial básica, que incluye la habilidad de facilitar discusiones.

02

Conocer la organización entrenada.

03

Motivar la comunicación de acuerdo a los temas y objetivos del ejercicio, y según el reloj del ejercicio. Todo ello, a la vez que controla la dinámica de la discusión.

04

Mantener una cultura de discusión adecuada.

Si el facilitador es también un practicante, no está expuesto al escenario, y la lógica que impulsa su funcionamiento proviene de la definición de su responsabilidad organizacional y de la forma en que se espera que la implemente con base en las circunstancias del escenario. En este caso, la responsabilidad de la División de Administración es asegurarse en todo momento de que la acción del facilitador realmente cumpla su propósito según se requiera. Por el contrario, si el facilitador es miembro de la División de Administración, debe estar familiarizado con los procesos y procedimientos organizativos involucrados en el ejercicio (metódicamente). Dado que conoce los detalles del escenario, la necesidad de ser orientado por la División de Administración es menos probable.

Para evitar dudas, el jefe administrativo es el único autorizado para tomar las decisiones concluyentes con respecto al momento de la práctica (establecer su hora de inicio real, establecer descansos o cancelarlos, acelerar o ralentizar la velocidad de lanzamiento del escenario y establecer la hora de su finalización).

En un juego organizacional se designará un facilitador para cada equipo de practicantes (además de un facilitador para el plenario). En este caso, es típico y aceptable que el facilitador sea uno de los miembros del equipo, sin embargo, esta no es una norma estricta. Debido a la mayor complejidad administrativa que existe aquí, la División de Administración debe usar a sus veedores no solamente para documentar las actividades del equipo de manera continua, sino también para ayudarse a monitorear las actividades de todo el personal y dirigirlas a los objetivos del ejercicio.

Preparación técnica y logística del entorno de práctica

En la guía ya se ha hecho referencia a los aspectos técnicos y logísticos comunes de los métodos teóricos y prácticos. Los siguientes son los aspectos especiales de la parte teórica:

01

La preparación del espacio de práctica debe completarse el día anterior a la fecha del ejercicio.

02

Es recomendable colocar sobre la mesa de ejercicios un juego de herramientas de escritura para cada uno de los ocupantes del primer círculo (bloc o libreta y bolígrafo). Esto los animará a poner sus pensamientos por escrito y ayudará a aclarar los problemas que trata el ejercicio. Además, las anotaciones podrán ayudar a los practicantes a llevar a cabo la investigación inicial y la posterior investigación interna. Como regla general, las notas de un practicante son su propiedad personal y únicamente él tiene el derecho de acceso para escribir en ellas. Si un practicante decide no llevarse sus notas al final del ejercicio, la División de Administración tiene la responsabilidad de destruirlas.

03

El día del ejercicio se recomienda adjuntar a los medios que se ponen a disposición de los ocupantes del primer círculo documentos que contengan información sobre los temas del ejercicio (procesos de trabajo, procedimientos, etcétera) y recopilar estos documentos al final del ejercicio.

04

Se recomienda colocar sobre la mesa de ejercicios un cartel de identificación de los miembros del primer círculo (nombre completo, afiliación organizacional y cargo). Esto les facilitará sentarse alrededor de la mesa y reconocerse entre sí.

05

También es importante realizar un proceso de registro de los participantes al inicio del día de ejercicio. Además, cada uno de ellos debe poseer una tarjeta de identificación personal. Esto no solo ayudará a la División de Administración a monitorear la composición real de los participantes, sino también a prevenir la entrada de personas que no deben participar en el ejercicio en el espacio de práctica. Después de esto, y ciertamente en los casos en los que se trata de cuestiones delicadas de práctica, debe haber un control constante de quienes ingresan al espacio de práctica hasta el final del ejercicio.

06

Es muy beneficioso mostrar los eventos del ejercicio en monitores instalados en el espacio de ejercicio. Este beneficio aumenta a medida que se incrementa el número de practicantes. En cualquier caso, es recomendable entregar manualmente, al menos a los ocupantes del primer círculo, una copia impresa de cada evento presentado, para que puedan esbozar por sí mismos la secuencia de desarrollo del escenario.

07

En caso de que la duración del ejercicio no supere las dos horas, es recomendable evitar establecer pausas durante el mismo, ya que esto puede perjudicar la tensión del ejercicio y su dinámica general. Para un ejercicio más prolongado, se recomienda conformarse con un solo descanso.

Apéndice 4. Directrices para llevar a cabo un ejercicio operativo de ciberseguridad

Marco temporal

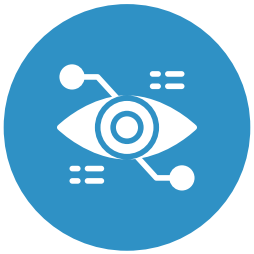
La duración total de un ejercicio operativo puede variar de uno a varios días. En general, es directamente proporcional tanto a la disponibilidad y alcance del personal y sectores entrenados, como al nivel de complejidad organizativa del ejercicio.

Entorno de práctica

Como se mencionó anteriormente, es de gran importancia que en el entorno de práctica del tipo operativo se reflejen la mayoría de los componentes del entorno real. Más allá de los componentes blandos, como los métodos de operación y procedimientos, también debe incluirse el medio de comunicación que la organización utiliza en tiempo real (y con énfasis en situaciones de crisis), por ejemplo.

En la práctica operativa a nivel técnico-táctico, la unidad del lugar generalmente se mantiene: incluso si hay varios equipos practicando en paralelo, cada uno ubicado en una sala o incluso en un edificio separado, estos espacios de práctica probablemente serán adyacentes entre sí. Como ya se mencionó, la efectividad de este tipo de ejercicio depende de manera crucial de una representación adecuada de las diversas infraestructuras corporativas (TI y OT), así como de los ciberataques de diferente tipo dirigidos a las mismas.

Es de esperar que este sea un campo de práctica profesional y de uso intensivo de recursos, cuya implementación requiere infraestructura, medios y mano de obra exclusivos, que generalmente traslada el ejercicio del espacio físico de la organización a varias instalaciones externas que brindan dicho servicio. De hecho, hay varios en Israel y en todo el mundo.[42]



Esta característica distingue la práctica técnico-táctica de la de otros niveles de la organización, ya que implica importantes consideraciones logísticas y económicas.[43] Al mismo tiempo, la distancia entre el ejercicio y la formación es bastante pequeña, por lo que se puede incluir en este nivel la necesidad de formación dentro de las necesidades de práctica de la organización y de esta forma ahorrar recursos considerables.

De esta manera, por ejemplo, en el caso de un ejercicio operativo de varias plantas manufactureras agrupadas bajo un mismo asunto (cuya gestión también se entrena), es posible que el ejercicio se lleve a cabo simultáneamente en sitios repartidos en una gran área del país.

A diferencia de la práctica teórica, en este caso no existe un límite preestablecido en el número de practicantes. La única condición limitante es la capacidad de la División de Administración para controlar el curso del ejercicio y, en el caso de un ejercicio técnico-táctico, la capacidad de la infraestructura de simulación que respalda la práctica.

Coordinación del ejercicio

Para ejercer un control adecuado sobre los movimientos de un ejercicio operativo a nivel operativo y estratégico, la División de Administración debe primero establecer un **centro de control del ejercicio (CCE)**, donde y a través del cual se llevará a cabo el ejercicio en la práctica. Al mismo tiempo, la División de Administración colocará veedores en las áreas de práctica, que le servirán de ojos y oídos.

Además de lo ya mencionado sobre las limitaciones del componente de simulación en el ejercicio práctico, es importante enfatizar que el objeto de estudio de los veedores es la actividad humana (de funcionarios y personal) y no la funcionalidad de sistemas e infraestructuras. Es decir, las declaraciones verbales de los funcionarios en su día a día y en diversos foros, y cualquier información adicional disponible, accesible en monitores o mediante documentos escritos.

42. Los ejercicios operativos que se realizan en esas instalaciones suelen tener un carácter similar al de un juego organizacional o más precisamente al de la competencia entre equipos. Un ejemplo bien conocido de esto es el ejercicio Locked Shields de la Organización del Tratado del Atlántico Norte (OTAN), que se realiza una vez al año en su Cooperative Cyber Defence Centre of Excellence (CCDCOE) en Tallin, Estonia.

43. Si bien la capacidad intraorganizacional puede desarrollarse en esta área, debido a los costos involucrados en el desarrollo, uso diario y mantenimiento a largo plazo, en contraposición con los costos de la subcontratación, es claro que este esfuerzo solo vale la pena para organizaciones particularmente grandes (y, como es de esperar, organizaciones estatales y varios organismos de seguridad).

Los veedores estarán en contacto permanente y cercano con el CCE. A su vez, la División de Administración utilizará sus informes para evaluar la condición del ejercicio (y no la condición de la organización, que es lo que realizan los practicantes) siempre que parezca que el ritmo y la dirección en la que avanza la práctica no está en consonancia con lo previsto.

En general, sería correcto ubicar al veedor asignado para monitorear un espacio de actividad particular en un centro neurálgico que domine la actividad de ese espacio. Por ejemplo, en el contexto de la práctica de la compañía presentada en el recuadro A1.1, sería correcto colocar al veedor de la alta dirección en el sitio donde la Gerencia realiza sus evaluaciones de situación. También es posible que la División de Administración coloque veedores en posiciones de control sobre la infraestructura de producción de las fábricas.

Debido a la dispersión física de los practicantes, y también con el fin de asegurar el control de los ejercicios, es aconsejable transferir la información del ejercicio de manera computarizada.[44] Con base en lo anterior, y asumiendo de manera razonable que la organización no cuenta con una infraestructura TI exclusiva para este propósito, sería ideal utilizar un sistema de mensajería que sirva para la comunicación entre los practicantes y entre ellos y la División de Administración durante el ejercicio.

Solo es necesario asegurarse de que la infraestructura en cuestión permita la transmisión tanto de mensajes escritos como de archivos multimedia (audio y videos). Se recomienda configurar en el sistema elegido cuentas de usuario exclusivas para el ejercicio, que representen a todos los practicantes y que serán utilizadas para la comunicación entre ellos y con la División de Administración, a fin de que esta pueda transmitirles la información del ejercicio.

Durante el ejercicio, la División de Administración puede realizar una acción conocida como parada metódica del ejercicio. Esto es detener el proceso de transmisión de la información a los practicantes durante un cierto período de tiempo y, como resultado directo de esto, congelar el proceso de desarrollo del escenario durante este período. Esta acción puede tener dos propósitos. Uno es permitir que los practicantes realicen una evaluación de la situación sin limitaciones de tiempo y enfrenten nuevos desafíos para los que el escenario está diseñado.

44. El uso de medios de comunicación automatizados permitirá documentar de manera confiable, conveniente y accesible la información que fluye durante el ejercicio entre la División de Administración y los practicantes y entre los propios practicantes. De esta manera, la base de información resultante servirá como primera fuente de datos para investigar el ejercicio.

El otro es permitir que la División de Administración saltee una serie de ejercicios que aún no se han transmitido a los practicantes porque entiende que ya se ha logrado un subobjetivo de ejercicio particular que se pretendía alcanzar, o para fomentar de manera proactiva el desarrollo de un escenario de ejercicio, si este ha progresado a un ritmo más lento de lo planeado.

Preparación técnica y logística del entorno de práctica

En la guía ya se hizo referencia a los aspectos técnicos y logísticos comunes de los métodos teóricos y prácticos. Asimismo, al comienzo de este apéndice se mencionó este asunto en el contexto de un ejercicio operativo a nivel técnico-táctico. Por lo tanto, los siguientes son los aspectos especiales de un ejercicio práctico a nivel operativo y estratégico:

01

Al igual que en el ejercicio teórico, el principal esfuerzo técnico y logístico de la División de Administración en el ejercicio práctico se concentra en establecer y preparar un sitio: el CCE. A diferencia del ejercicio teórico, en el práctico los practicantes deben invertir sus propios esfuerzos de preparación con el fin de establecer su entorno de práctica. Se enfatiza que esta responsabilidad recae en los practicantes y no en la División de Administración.

02

La determinación de la ubicación del CCE y la planificación de su organización funcional y preparación física se realizan como parte del proceso de preparación general de la División de Administración para el ejercicio, y deben completarse en un momento que permita al CCE alcanzar su capacidad funcional completa, a más tardar dos días antes de que comience el ejercicio.

03

Tanto en el TTX y el juego organizacional como en un ejercicio operativo, los participantes deben registrarse cuando se abre el ejercicio (esto es válido para todas las áreas de práctica, incluido el CCE), y continuar controlando a quienes ingresan a los espacios de práctica hasta el final del ejercicio. Cada participante debe tener una credencial de identificación personal.

04

A diferencia del ejercicio teórico, en el práctico no tiene mucho sentido tomar descansos por iniciativa de la División de Administración, ya que cada uno de los practicantes funciona en este marco de manera similar, en la medida de lo posible, a la forma en que actúa en la realidad.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos.

Como resultado de esta realidad, la preparación organizacional en el ciberespacio es un asunto dinámico y, por lo tanto, debe examinarse con regularidad. Una de las principales herramientas con las que cuenta una organización para este fin es la práctica, diseñada para promover la competencia y preparación de los individuos de una organización, a través de cualidades que requieren una construcción gradual, mantenimiento continuo y promoción de acuerdo a un plan definido.

Como en otros contextos, la realización de prácticas en el mundo cibernético es muy importante para preservar y promover la resiliencia organizacional. Esta guía inicial y única está destinada a ser utilizada por las organizaciones económicas como una herramienta básica para construir ciberejercicios, realizarlos y extraer lecciones de ellos de manera ordenada.

Nitzan Amar
Jefe Senior de la División de Resiliencia Infraestructural

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

- **A.01** Metodología de Ciberdefensa para Organizaciones Versión 1.0
- **A.02** Metodología de Ciberdefensa para Organizaciones Versión 2.0
- **A.03** Uso de servicios en la nube: Adenda a la Metodología de Ciberdefensa para Organizaciones
- **A.04** Recomendaciones de defensa: La amenaza interna
- **A.05** Preparación organizacional para una crisis cibernética
- **A.06** Cadena de suministro
- **A.07** Preguntas de orientación para formuladores de políticas cibernéticas
- **A.08** Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas
- **A.09** Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones
- **A.10** Gestión de riesgos cibernéticos en entornos de tecnologías operativas (OT)
- **A.11** Plantilla de evaluación de riesgo en el sector minorista
- **A.12** Práctica cibernética: creación de planes de concientización para organizaciones

Volumen B: Un enfoque técnico

Volumen C: Desarrollo seguro de *software*