Metodología para ejercicios de simulación de respuesta ante incidentes de ciberseguridad

Resumen. Este trabajo presenta una metodología para llevar a cabo ejercicios de simulación específicos de respuesta ante incidentes de ciberseguridad. Se basa en una combinación de mejores prácticas de la industria, y experiencia en la realización de estos ejercicios. El objetivo es permitir que organizaciones de cualquier tamaño y complejidad puedan planificar, diseñar y ejecutar simulaciones de forma ordenada, repetible y eficiente, que permitan evaluar su capacidad para responder a incidentes, identificar áreas de mejora y desarrollar planes de acción para aumentar sus capacidades de respuesta. La metodología se divide en varias etapas que van desde la planificación y preparación hasta la ejecución y evaluación de la actividad. Adicionalmente, se proporciona orientación práctica sobre cómo abordar cada etapa de manera efectiva, y una propuesta de métricas orientadas a la mejora continua.

1 Introducción

Los ejercicios de simulación de escritorio, también conocidos como “tabletop exercises” (TTX) permiten a las organizaciones simular situaciones críticas o de emergencia en un entorno controlado y seguro. Esto les da la oportunidad de evaluar su capacidad de respuesta y preparación ante posibles crisis, identificar áreas de mejora y tomar medidas preventivas para minimizar los riesgos. Además, pueden ayudar a mejorar la comunicación y la coordinación entre los miembros del equipo, así como a fortalecer su capacidad para tomar decisiones efectivas en situaciones de alta presión. También pueden ayudar a las organizaciones a cumplir con los requisitos regulatorios y normativos, y a mantener su reputación y credibilidad en caso de una crisis[1].

En el caso particular de la respuesta ante incidentes de ciberseguridad, son una herramienta clave para mejorar las capacidades para enfrentar amenazas. Un TTX bien diseñado y ejecutado puede ayudar a identificar brechas en procesos relacionados con la respuesta ante incidentes, mejorar la capacidad para gestionar situaciones críticas y ajustar los planes de acción. Ante ciberataques cada vez más sofisticados y frecuentes, la necesidad de una respuesta eficiente aumenta, y estos ejercicios deben planificarse de manera adecuada para garantizar que las organizaciones obtengan el máximo beneficio. Los TTX deben ser realistas y que estar alineados con escenarios que tengan sentido para el contexto y objetivos de cada organización. Todo esto hace que sea importante contar con una metodología sólida para garantizar que se esté obteniendo información valiosa y útil[2]. En este trabajo se presenta una metodología para la planificación, diseño y ejecución de ejercicios TTX, diseñada para dar un enfoque estructurado para estas pruebas, siendo la primera de su tipo específico.

2 Metodología

Para el desarrollo de un ejercicio de simulación de respuesta ante incidentes se propone una metodología iterativa basada en cuatro fases, en un marco de mejora continua que puede ser aplicado a cualquier proceso, área o tecnología dentro de la organización. Esto proporciona un marco estructurado y sistemático para el diseño, implementación y evaluación de estos ejercicios, a través del cual las organizaciones pueden asegurarse de que sean adecuados, relevantes y desafiantes, permitiendo mejorar su capacidad de respuesta ante posibles amenazas de ciberseguridad. Además, la metodología proporciona una guía para el equipo encargado de llevar adelante el proyecto, y está alineada con trabajos de referencia que presentaron la terminología y la estructura general de estos ejercicios[3].

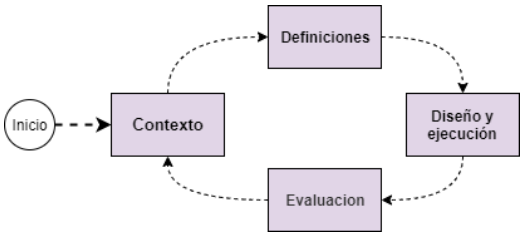

Fig. 1. Esquema general de fases

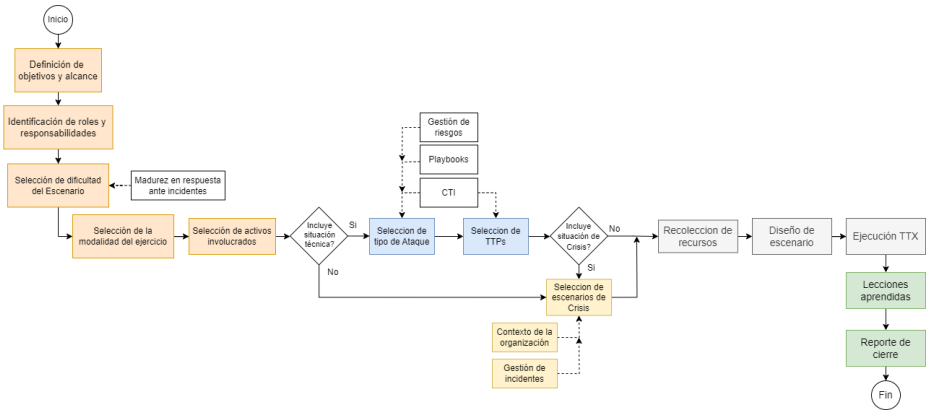

Fig. 2. Esquema detallado

2.1 Fase de contexto

En la primera fase se trabaja sobre el contexto del ejercicio, y se divide en cinco etapas. La primera consiste en definir los objetivos y alcance del ejercicio, es decir, qué se quiere lograr y cuáles son las limitaciones y alcances de este. La segunda etapa implica identificar los roles y responsabilidades de cada uno de los miembros del equipo involucrado en el ejercicio. La tercera etapa implica seleccionar la dificultad del ejercicio, lo que permitirá definir el nivel de complejidad y desafío que enfrentará el equipo. La

cuarta etapa se refiere a la selección de la modalidad del ejercicio, que variará según el tipo de interacción y las herramientas utilizadas. Finalmente, la quinta etapa implica la selección de los activos involucrados en el ejercicio.

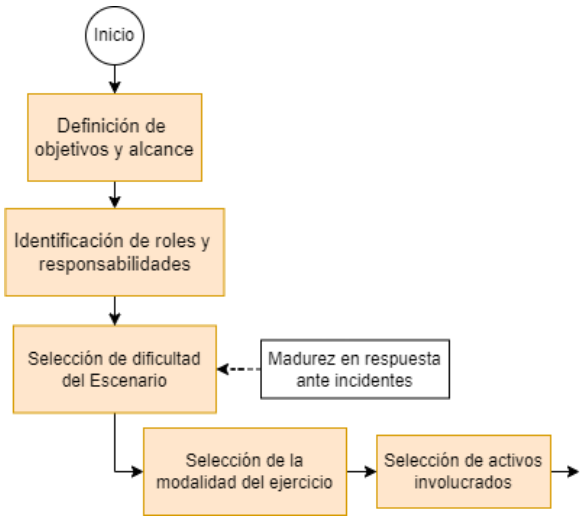

Fig. 3. Esquema de fase de definición de contexto

C1: Definición de objetivos y alcance. La definición de todas las decisiones de diseño del escenario de simulación será estructurada en base a uno o varios objetivos, que funcionarán como guía para dirigir las acciones posteriores. Ejemplos de objetivos pueden ser la identificación de brechas entre un procedimiento recientemente actualizado y su conocimiento real, ejercitar un proceso de respuesta ante un incidente derivado de una amenaza especialmente relevante para la industria o sector, y reconocer dificultades operativas de un procedimiento específico formalizado.

Otro de los elementos que atraviesa las definiciones del escenario es el alcance, en donde se establecen cuáles serán los activos de la organización involucrados. En el alcance podemos encontrar por ejemplo servicios internos, áreas o procesos específicos que quieran evaluarse dentro de la simulación.

En base a la definición de objetivos y al alcance podremos determinar adicionalmente si el ejercicio contendrá elementos técnicos y/o relacionados con la gestión de crisis. En esta etapa también se definirá la fecha simulada del ejercicio, que es el momento ficticio en el cual transcurrirán los eventos. Según los objetivos, podría ser de importancia evaluar la respuesta en distintos escenarios definiendo diferentes horarios, días o meses simulados que tengan características particulares para las operaciones de la organización. Por último, se establecerá de ser posible una duración del incidente simulado (en días) que luego podrá ser ajustada en relación con el tipo de ataque, las técnicas o los eventos propuestos.

C2: Identificación de roles y responsabilidades. Cada participante del ejercicio tendrá un rol específico y definido desde el inicio de las definiciones del escenario. Los roles posibles son los siguientes:

Jugadores: Personas que tienen un rol activo en el contexto del ejercicio, debatiendo o desempeñando sus propias funciones en la organización. Los jugadores debaten o inician acciones en respuesta al escenario simulado. Solo tienen participación durante la ejecución del ejercicio.

Equipo de coordinación: Personas encargadas llevar adelante las actividades del ejercicio. También participan en el diseño del escenario junto al equipo de preparación de la organización. El equipo de coordinación se compone de tres roles:

- Líder de proyecto: gestiona el proceso completo desde la reunión inicial hasta la entrega y presentación del informe final.
- Coordinadores: dirigen el ejercicio supervisando el flujo de eventos, y gestionando los debates que surgen del escenario.
- Monitores: registran y documentan los debates, interacciones, y acciones realizadas por los jugadores para cada evento, para facilitar la generación de los informes.

Equipo de preparación: Personas encargadas de la planificación del proceso y diseño del escenario, incluyendo objetivos, alcance, y definiciones técnicas. Durante la ejecución del ejercicio su participación debe ser mínima, dado que conocen los detalles del escenario, y deben limitar su interacción a las cuestiones previamente definidas.

Observadores: Personas que están presentes durante el ejercicio, pero no participan activamente, y solo pueden intervenir en la fase final, luego del cierre de la presentación del ejercicio. Este rol está relacionado con las funciones de auditores, o personas vinculadas a la organización que puedan estar interesadas en el desarrollo y resultado del ejercicio.

C3: Selección de la dificultad del ejercicio. La dificultad del ejercicio será definida en base a la madurez de la organización en relación con su gestión del riesgo y sus procesos de ciberseguridad. El objetivo de conocer este nivel es el de plantear un escenario desafiante que lleve a los distintos equipos a un espacio en el que puedan generar mejoras en sus procesos. Para definir la escala para la dificultad se toman como referencia los cuatro niveles (tiers) del Cybersecurity Framework v1.1 del NIST (National Institute of Standards and Technologies)[4] y se adicionan componentes derivados de la experiencia en diseño y ejecución de ejercicios:

Dificultad básica (Tier 1: Partial): En este nivel de madurez se recomienda la realización de ejercicios simples basados en escenarios típicos de la industria de la organización, el objetivo principal será identificar los elementos básicos a incorporar dentro proceso de respuesta ante incidentes. El escenario tendrá una historia lineal y cada elemento estará claramente definido.

Dificultad media (Tier 2: Risk Informed): En este nivel de madurez se recomienda la realización de ejercicios que se alineen con los riesgos de ciberseguridad de mayor relevancia para la organización, con el objetivo principal de identificar las posibles mejoras a los procesos de respuesta ante incidentes. El escenario tendrá una historia lineal, elementos distractores, y algunos elementos con información incompleta (no toda la información será revelada durante el ejercicio).

Dificultad alta (Tier 3: Repeatable): En este nivel de madurez se recomienda la realización de ejercicios rutinarios que se alineen con los riesgos de la organización, con el objetivo principal de identificar las posibles mejoras dentro de los procesos de respuesta ante incidentes, la comunicación entre los diferentes equipos y la generación de posibles ajustes a los procedimientos involucrados. El escenario tendrá una historia lineal, elementos distractores, y algunos elementos con información incompleta (no toda la información será revelada durante el ejercicio).

Dificultad exhaustiva (Tier 4: Adaptive): En este nivel de madurez se recomienda la realización de ejercicios rutinarios que se alineen con los riesgos de la organización y además incorporen información de ciber inteligencia en relación con las amenazas actuales. El objetivo principal será identificar las posibles mejoras sutiles dentro de los diferentes procesos definidos con relación a los incidentes de ciberseguridad. El escenario tendrá una historia que podrá variar en base a las decisiones de los jugadores, contará con elementos distractores, y elementos incompletos. Adicionalmente, se recomienda la realización de ejercicios específicos para cada área.

C4. Selección de la modalidad del ejercicio. La modalidad se compone de dos aspectos, que son la forma de interacción y las herramientas de comunicación, y se selecciona de acuerdo con tres criterios principales: la madurez de la organización en términos de ciberseguridad, la experiencia previa en el tipo de ejercicios, y la cantidad de participantes y áreas.

Forma de interacción. Podrá ser seleccionado de acuerdo con la operatoria típica de los distintos equipos participantes, o bien según la modalidad esperada por la organización. Las opciones de interacción son:

- Virtual (online): haciendo uso de servicios de videollamadas o distintas plataformas de comunicación.
- Presencial: dentro de una sala de debate (también "sala de guerra" o "war room").
- Híbrida: parte de los participantes se encontrará virtual y parte presencial. Esta es la forma más utilizada en los últimos años.

Herramientas de comunicación. Durante la ejecución debe definirse además el modo en que los participantes reciben la información de los eventos, y para esto hay dos opciones.

- Modalidad clásica: llamada también tradicional, estará conformada por una presentación en la que los participantes reciben al mismo tiempo los distintos eventos y situaciones que conforman el escenario. Esta modalidad podría ser más efectiva

para los ejercicios específicos con público reducido, para las organizaciones que no hayan realizado ejercicios de simulación anteriormente o para los ejercicios de formato plenamente presencial.
- Modalidad basada en plataforma: conformada por una plataforma de mensajería, mediante la cual cada equipo recibirá distintos tipos de eventos según su función, asemejándose más a una situación de la vida real, y se establecerán momentos particulares para la interacción en vivo a través de videollamadas o "war room" según el formato elegido. Esta modalidad implica la complejidad de diseñar múltiples tipos de eventos según las áreas involucradas como si se tratasen de hilos de ejecución que luego convergen en distintos momentos y se basan en la misma historia.

C5. Selección de activos involucrados. En esta etapa se debe hacer el relevamiento de los activos que estarán involucrados en el escenario, y los procesos de negocio que los mismos sustentan. En este punto podemos encontrar:
- Servicios, aplicaciones, servidores, centros de datos que dan soporte al activo sobre el que quiere simular el incidente.
- Personas, áreas, proveedores, y otras entidades del ecosistema de la organización que estén involucradas en alguna parte de la operación y funcionamiento del activo afectado y también quienes estén involucrados en la toma de decisiones de un incidente ya sea técnico o de crisis.
- Procesos, runbooks, playbooks, políticas, y otra documentación útil para la respuesta ante un incidente.

2.2 Fase definiciones

En esta fase se definen las especificaciones del ejercicio, y tiene a su vez dos sub-fases que corresponden a las deficiones de estadio técnico y de crisis. La primera contiene dos etapas, una de selección del tipo de ataque, que permitirá establecer los objetivos específicos, y otra de selección de las TTPs (Tácticas, Técnicas y Procedimientos) que se utilizarán en el ataque. La segunda sub-fase permite determinar el alcance del incidente en caso de que trascienda los efectos técnicos, y derive por diseño en una situación de crisis, y cuenta con dos etapas, la selección de la repercusión, y la selección de los efectos colaterales (daños secundarios que pueden ocurrir como resultado). En cuanto al proceso de esta fase, se puede visualizar en el flujograma que se muestra a continuación:

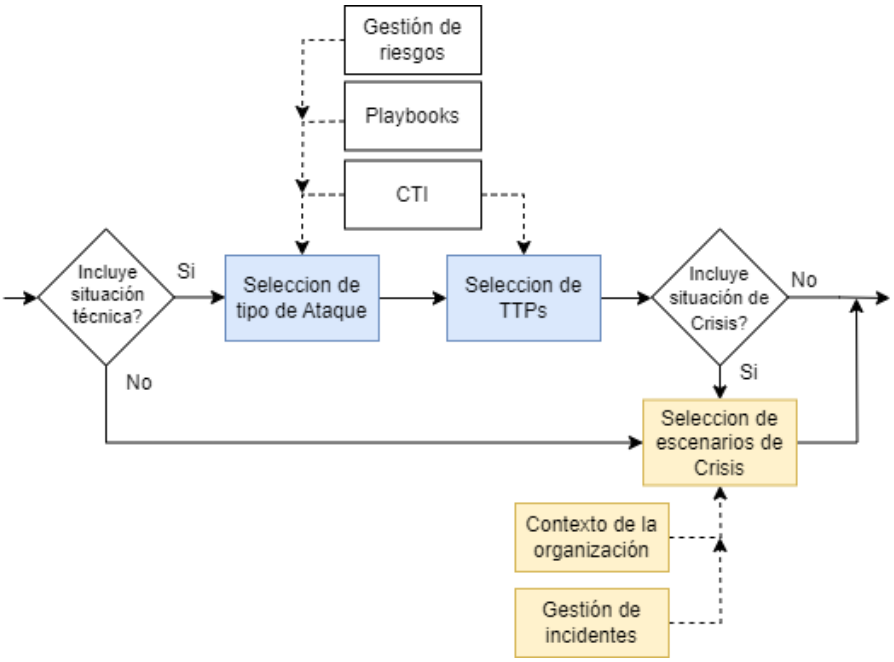

Fig. 4. Esquema de fase de definiciones

T1. Selección del tipo de ataque: En esta etapa se seleccionará el tipo de amenaza que desea considerarse para el diseño del escenario técnico, esta definición podrá incluir uno o varios tipos de amenazas en relación con los objetivos del ejercicio. Esto puede estar definido por la gestión de riesgos, o los reportes de ciber inteligencia de amenazas (internos, externos, o alineados con el sector al que pertenece la organización). El tipo de amenazas servirá de guía principal para las distintas tácticas, técnicas y procedimientos seleccionados en la próxima etapa. Los tipos más comunes son: Ransomware, Denegación de Servicio, Atacantes internos, Fuga de información, Ingeniería social, Ataque a cadena de suministros, y Disrupción física.

T2. Selección de TTPs: Para la selección de las tácticas, técnicas y procedimientos (TTPs) simuladas durante el ataque se tomará como referencia el tipo de amenaza elegido y los reportes de ciber inteligencia. En esta metodología se realiza la selección en base al modelo del framework MITRE ATT&CK[5] que es la principal referencia de la industria. Esta selección además tendrá consideración sobre el alcance y los activos involucrados durante el ejercicio de simulación.

Cr1. Selección de la repercusión de la crisis. En esta etapa se definirá la situación de crisis que incluirá el escenario, que estará relacionada con los objetivos y el alcance del

mismo. En esta definición se puede encontrar el impacto en forma de repercusión sobre: clientes, proveedores, empleados, partes interesadas, redes sociales, medios de prensa.

Cr2. Selección de los efectos colaterales. Con el objetivo de detallar la orientación del impacto provocado por el incidente se definen en esta etapa los efectos concretos para la repercusión. Entre algunos ejemplos de efectos podemos encontrar: caída de las acciones, disminución de operaciones, pérdida de licencias de operación, pérdida de contratos con terceros, cierre de operaciones, multas o acciones judiciales.

2.3 Fase de diseño y ejecución

En esta fase se comienza a trabajar sobre el armado del escenario en sí, a través del proceso de diseño, y finaliza con la ejecución, correspondiente al día del ejercicio. La primera etapa implica la recolección de recursos, lo que puede incluir herramientas, software y hardware necesarios para llevar a cabo el ejercicio. La segunda etapa implica el diseño del escenario, que puede variar según las definiciones tomadas. La tercera etapa implica la ejecución del ejercicio, lo que permite poner en práctica los planes y protocolos establecidos.

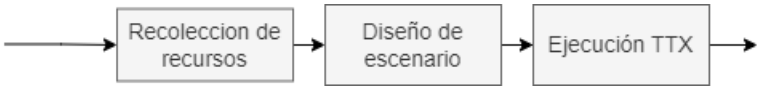

Fig. 5. Esquema de fase de diseño y ejecución

D1. Recolección de recursos. Antes de comenzar con el diseño del escenario simulado se recopilan los elementos adicionales vinculados a los activos definidos en el alcance y relacionados con las definiciones técnicas y/o de crisis. Entre estos podemos encontrar: normas de aplicación, reportes de incidentes relacionados, referencias a situaciones de crisis transitadas por terceros, documentación de proveedores, y más.

D2. Diseño de escenario. En esta etapa se realiza el diseño del escenario propiamente dicho. Esto se conforma por dos perspectivas, en primera instancia se elaborará una historia (storyline) que dará estructura y consistencia al escenario, y posteriormente se trabajará sobre la "vista del participante" la cual estará conformada por elementos de la historia.

Diseño de historia: Este proceso comienza con la confección de una línea de tiempo que incluirá el escenario completo de ataque simulado según el alcance y los objetivos, desde el vector de acceso inicial, técnicas utilizadas, y los activos involucrados. Esta línea de tiempo no se reducirá a la cadena del ataque desde el punto de vista técnico, sino que deberá incluir, en caso de que corresponda, la ruta hasta el impacto y los distintos tipos de repercusiones. Este diseño de la historia es crucial para permitir la fluidez en la ejecución del ejercicio, ya que una simulación de incidente que no se alinee con

alguno de los aspectos recolectados anteriormente podrá ser interpretado por los participantes como ficticio y entorpecer la dinámica de participación.

Diseño de la vista de participantes: El material preparado en este diseño será el utilizado para guiar la ejecución del escenario, estará basado en la historia y en las capacidades de detección de la organización. Si el ejercicio se realiza en la modalidad tradicional esta vista de participantes será unificada, salvo que la complejidad del ejercicio, la cantidad de participantes o una división de los roles lo requieran, en ese caso la ejecución será dividida en partes y cada parte tendrá su propia "vista de participantes". Para el caso de la modalidad asistida por plataforma, toda la vista de los participantes será preparada específicamente para cada rol. Los distintos eventos serán agrupados en un archivo de eventos conocido como MSEL (Master Scenario Event List). Los distintos eventos por presentar podrán contener información sobre una situación relevada en un sistema (recibida por un tercero o de cualquier otra fuente), opciones de decisión explícita, en los que se requerirá la elección de una elección taxativa para una situación, o información adicional sobre el avance del incidente, por ejemplo, el resultado de una evaluación forense, la respuesta de un tercero involucrado, o una definición de un participante no presente en el ejercicio.

Para la elaboración de cada uno de estos diseños se propone la utilización de alguna herramienta que permita diagramar los distintos momentos del incidente simulado, lo que permite visualizar con mayor facilidad el escenario completo, agregar elementos o detectar inconsistencias en el ejercicio. La organización MITRE, a través del “Engenuity Center for Threat-Informed Defense” provee “Attack Flow”[6], una herramienta de libre uso que permite crear diagramas de flujo y referenciar las distintas técnicas ofensivas a lo largo de un ataque, y puede ser usada para el diseño.

Adicionalmente, se prepara para los participantes un documento estilo presentación que funciona como introducción al ejercicio, y se recomienda hacer llegar a los participantes durante los días anteriores a la fecha de ejercicio. Este documento podrá contener información como ser: objetivos, alcance, reglas de la dinámica, consideraciones asumidas y ficticias, y modalidad de la actividad. También puede contener otros elementos informativos para contextualizar el ejercicio, como ser disparadores, fecha simulada, activos involucrados, tipo de amenaza, áreas involucradas, y requisitos.

D3. Ejecución del ejercicio. Para la ejecución se convoca a los participantes el día programado para el ejercicio. Se recomienda evitar llegar a la hora precisa de comienzo, aunque este tiempo de espera y preparación conviene que se tome como parte del ejercicio y se incluya en la agenda como período de recepción. Según la modalidad, el espacio de encuentro podrá ser una o varias salas virtuales, o bien una sala de reuniones con participantes conectados de forma virtual.

Para comenzar con las actividades se realizará una revisión de documento de introducción, previamente enviado a los participantes, para repasar los objetivos, la dinámica, las reglas y algunas decisiones de diseño que hayan sido planificadas para revelar en la etapa inicial. En el caso de la modalidad basada en plataforma el encuentro se realizará en una sala virtual con cualquier servicio de videollamadas.

Es importante reforzar a los participantes que cualquier comunicación dirigida a algún participante por un canal distinto a los propuestos por el ejercicio, debe ser precedida por un texto de referencia a la simulación (por ejemplo: ejercicio, ejercicio, ejercicio). Esto es para evitar generar confusiones con posibles situaciones reales que estén ocurriendo.

Modalidad tradicional. Durante el encuentro se muestra una presentación a todos los participantes con los eventos según lo planificado. La distribución física de los participantes en la sala será fundamental para incentivarlos a entablar conversaciones, generar debates y estimular la toma de decisiones, dejando la comunicación con el coordinador solo para definir cuáles son las acciones que serán realizadas para cada evento. Puede usarse una disposición de tipo herradura, o agrupados en mesas según las distintas áreas. Los observadores en cambio pueden distribuirse alrededor de los distintos participantes teniendo cercanía con las áreas que más afinidad tengan según las tareas desarrolladas.

El coordinador proporciona un tiempo indeterminado para que se converse sobre cada evento según corresponda, y guía los debates para obtener de cada evento una serie de decisiones claras sobre el posible avance o resolución de la situación planteada. Ante el avance de los días simulados, el coordinador podrá considerar como "no ejecutadas" las acciones que no hayan sido claramente mencionadas el día correspondiente (por ejemplo, dar aviso a un regulador, utilizar un procedimiento, lanzar una tarea de restauración, etc.). Si fuera el caso de una ejecución presencial dividida en dos partes (técnica y ejecutiva) se realizará primero la etapa técnica con el equipo correspondiente, y al finalizar esta, uno de los participantes deberá informar el estado de situación al equipo siguiente para dar comienzo con la etapa de crisis.

Modalidad basada en plataforma. Luego de la introducción, se dará inicio al envío de una serie de eventos según lo planificado y volcado en el MSEL. Cada equipo recibirá a través del canal de mensajería correspondiente los eventos particulares relacionados con el avance del incidente en relación con las áreas en las que desarrollan sus actividades habituales. Los participantes de los equipos pueden interactuar por el mismo canal de mensajería o a través de salas virtuales según prefieran o según se haya definido por diseño. A su vez cada equipo recibe instrucciones específicas sobre la forma en la que deberán registrar las tareas ejecutadas en una especie de bitácora de equipo. Si fuera requerido conectar con una persona fuera del equipo, puede realizarse por los canales destinados para tal fin y en los tiempos indicados por el ejercicio.

2.4 Fase de Evaluación

Esta fase corresponde al cierre de la actividad completa. La primera etapa comprende el período inmediatamente siguiente al ejercicio, e implica la identificación de lecciones aprendidas en caliente, lo que permitirá identificar los problemas y debilidades durante el ejercicio. La segunda etapa corresponde a un momento posterior, e implica la generación de un reporte de cierre, que puede incluir recomendaciones y mejoras para futuros ejercicios de simulación de respuesta ante incidentes de ciberseguridad.

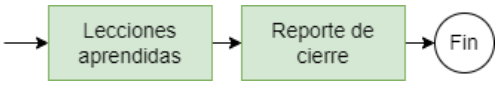

Fig. 5. Esquema de fase de evaluación

E1. Lecciones aprendidas en caliente. Esta etapa se realiza a continuación de la ejecución del escenario dentro del mismo encuentro (o videollamada si corresponde), a fin de relevar tanto las lecciones derivadas de la autocrítica, como las sensaciones subjetivas de los participantes acerca de la toma de decisiones. Estos ayudan a la construcción posterior del reporte, que podrá contener elementos discutidos en este momento. Este cierre "en caliente" puede basarse en una serie de preguntas como ser: ¿Qué hicimos bien? ¿Qué podríamos haber hecho mejor? ¿Qué capacidades no utilizamos o utilizamos de menos? ¿Qué brechas encontramos en nuestra comunicación? ¿Qué sería útil realizar en futuros ejercicios? Estas preguntas tienen como objetivo abrir un debate autocrítico sobre lo realizado y como fue realizado. A su vez ponen en común lo experimentado por los participantes. En esta etapa pueden compartir sus apreciaciones también los participantes observadores y otros participantes asistentes.

E2. Reporte de cierre. El reporte de cierre está conformado típicamente por dos secciones, un resumen ejecutivo y un informe detallado. Como paso opcional, se puede realizar una versión en modo de presentación para ser mostrada al directorio o gerencia de la organización como resultado de la actividad.

Resumen ejecutivo: esta sección tiene como objetivo presentar de manera resumida los resultados del ejercicio de simulación y las lecciones aprendidas durante el mismo. Está dirigido a los directivos y tomadores de decisiones de la organización, por lo que debe ser claro y conciso, presentando los aspectos más importantes del ejercicio y las recomendaciones principales para mejorar la preparación ante posibles incidentes de ciberseguridad. Debe incluir información sobre la definición del contexto y los objetivos del ejercicio, así como los resultados obtenidos y los principales desafíos enfrentados durante el mismo. También es importante incluir las recomendaciones y mejoras identificadas para fortalecer la preparación de la organización ante futuros incidentes de ciberseguridad. Puede contener información sobre antecedentes, modalidad de trabajo adoptada, fortalezas y áreas de mejora detectadas.

Informe detallado: este aportará los detalles para dar mayor contexto sobre los resultados relevados del ejercicio, adicionalmente estos detalles serán consultados en próximos procesos de auditorías o ejercicios similares. Esta sección tiene como objetivo presentar de manera exhaustiva los hallazgos y recomendaciones identificados durante la evaluación en caliente del ejercicio. Se proporciona información detallada sobre los aspectos que funcionaron bien durante el ejercicio, así como las áreas de mejora y las lecciones aprendidas que se deben tener en cuenta para fortalecer la preparación de la organización ante posibles incidentes de ciberseguridad. Debe incluir una descripción más específica de los resultados obtenidos en cada parte del ejercicio, así como una

evaluación de la eficacia de los planes de respuesta. También es importante incluir información sobre los desafíos enfrentados durante el ejercicio y las recomendaciones para mejorar la preparación de la organización ante posibles incidentes de ciberseguridad a futuro. Se deben incluir los objetivos del ejercicio, listado de participantes, explicación del escenario simulado y observaciones sobre el mismo, y el listado de eventos mostrados durante la ejecución junto con un resumen de la respuesta y decisiones registradas por los participantes para cada evento. Sobre cada área de mejora detectada se realiza una recomendación para su resolución o mejora.

3 Métricas para la mejora continua

Bajo la hipótesis de que los ejercicios de simulación como los descritos permiten mejorar las capacidades de respuesta ante incidentes, se debe tener una referencia en base a métricas que permitan las comparaciones entre diferentes momentos. Los puntos de referencia en este caso se establecen antes y después del ejercicio, y se recomienda que él después no sea inmediato, sino que se realice luego de un período tras el cual puedan asimilar los aprendizajes derivados del ejercicio.

En este sentido, y a fin de poder determinar métricas precisas que reflejen el nivel de madurez en las capacidades de respuesta ante incidentes, es conveniente utilizar un estándar de referencia. Para este caso, utilizamos el framework de madurez de CSIRT[7] creado por la agencia ENISA, basado en el SIM3 (Security Incident Management Maturity Model). De esta manera, en caso de que se requiera la medición precisa del efecto de estos ejercicios en el contexto de las organizaciones, debe agregarse el proceso inicial y posterior, sumando esto al dimensionamiento de los esfuerzos para la realización del ejercicio en sí.

El modelo de madurez consta de 45 parámetros (la lista detallada se encuentra como apéndice de este trabajo) que se miden en función de la madurez, y cada uno pertenece a una de las siguientes categorías: O (Organización), H (Humano), T (Herramientas) y P (Procesos). Estas categorías se han elegido de forma que los parámetros que las componen sean lo más independientes posible entre sí, y lo que se miden son los niveles de cada parámetro. El conjunto de niveles definido para todos los parámetros de todas las categorías es el siguiente:

- 0 = no disponible / indefinido / desconocido
- 1 = implícito (conocido/considerado, pero no escrito)
- 2 = explícito, interno (escrito, pero no formalizado)
- 3 = explícito, formalizado bajo autoridad y publicado
- 4 = explícito, evaluado regularmente por la autoridad superior

Si bien este proceso puede resultar en tiempos más prolongados y esfuerzos superiores que exceden el ejercicio, son recomendables para tener referencias sólidas a la hora de comprender el rol de los ejercicios de simulación en la mejora de capacidades de respuesta ante incidentes.

4 Conclusiones

Considerando que el uso de una metodología proporciona un marco estructurado para la realización de actividades, ayudando a garantizar el alcance de objetivos de manera eficiente y efectiva, las simulaciones de respuesta ante incidentes de ciberseguridad pueden beneficiarse de adoptar un enfoque metodológico para lograr resultados consistentes. Este trabajo cumple con proporcionar un conjunto de conceptos, herramientas y técnicas para realizar estas tareas específicas de manera sistemática, permitiendo a los equipos lograr resultados predecibles y repetibles. La definición de los pasos necesarios para la realización de un ejercicio TTX facilita trabajar de manera más organizada y colaborativa, al tiempo que proporciona una forma de medir el progreso y éxito del proyecto, ayudando a mantener el foco en los objetivos y en la toma de decisiones informadas.

Es posible a futuro integrar esta metodología en un conjunto mayor de marcos de trabajo para las organizaciones, que permita modularizar las actividades de ejecución de los distintos tipos de pruebas relacionadas con la gestión de incidentes y de crisis, como pueden ser pruebas de resiliencia, recuperación ante desastres, o emulación técnica de ataques de ciberseguridad.

Cabe destacar que el desarrollo de esta metodología se encuentra limitado a la experiencia de los autores en empresas y organizaciones diversas, aunque mayormente centrada en Argentina y otros países de Latinoamérica, y que podría no ser aplicable de manera directa en otro tipo de entornos como ser el ámbito gubernamental y militar, sin la previa adaptación correspondiente.

Referencias

1. Brilingaitė, A., Bukauskas, L., Krinickij, V., & Kutka, E. (2017, October). Environment for cybersecurity tabletop exercises. In ECGBL 2017 11th European Conference on Game-Based Learning (pp. 47-55). Academic Conferences and publishing limited.
2. Pacheco, F., 2022, septiembre. Simulación de respuesta ante incidentes de ciberseguridad para aprendizaje en organizaciones y en el aula. 2022 IEEE Congreso bienal (ARGENCON) (pp. 1-8). IEEE.
3. Kick, Jason. Cyber exercise playbook. MITRE Corp., (2014).
4. NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (2018). https://doi.org/10.6028/nist.cswp.04162018.
5. MITRE ATT&CK. Homepage, https://attack.mitre.org.
6. MITRE Attack Flow. Homepage, https://center-for-threat-informed-defense.github.io/attack-flow/
7. ENISA CSIRT Maturity Framework. Homepage, https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework

Apéndice

ID	Descripción	ID	Descripción
O-1	Mandato	T-6	Mensajería resiliente
O-2	Circunscripción	T-7	Acceso a Internet resiliente
O-3	Autoridad	T-8	Herramientas de prevención de incidentes
O-4	Responsabilidad	T-9	Herramientas de detección de incidentes
O-5	Descripción del servicio	T-10	Herramientas de resolución de incidentes
O-6	Política de medios de comunicación	P-1	Escalada al nivel de gobernanza
O-7	Nivel de servicio Descripción	P-2	Escalada a la función de prensa
O-8	Clasificación de los incidentes	P-3	Escalada a la función jurídica
O-9	Integración en sistemas CSIRT	P-4	Proceso de prevención de incidentes
O-10	Marco organizativo	P-5	Proceso de detección de incidentes
O-11	Política de seguridad	P-6	Proceso de resolución de incidentes
H-1	Código de conducta/práctica/ética	P-7	Procesos específicos de incidentes
H-2	Resiliencia del personal	P-8	Proceso de auditoría y retroalimentación
H-3	Descripción del conjunto de competencias	P-9	Proceso de accesibilidad en caso de emergencia
H-4	Desarrollo del personal	P-10	Mejores prácticas de presencia en Internet
H-5	Formación técnica	P-11	Proceso seguro de tratamiento de la información
H-6	Formación en competencias interpersonales	P-12	Fuentes de información Proceso
H-7	Redes externas	P-13	Proceso de divulgación
T-1	Activos informáticos y configuraciones	P-14	Proceso de elaboración de informes de gobernanza
T-2	Lista de fuentes de información	P-15	Proceso de notificación de circunscripciones
T-3	Sistema de mensajería consolidado	P-16	Proceso de reunión
T-4	Sistema de seguimiento de incidentes	P-17	Proceso de colaboración entre iguales
T-5	Llamadas de voz resilientes		