Ejercicios de Ciber Crisis: El camino a seguir

INFORME

JULIO 2026

Contenido

1

Ciberresiliencia

En el entorno operativo actual, las organizaciones ya no pueden depender únicamente de los enfoques tradicionales de ciberseguridad, centrados principalmente en la prevención y la protección. Aunque estos controles siguen siendo esenciales, ya no son suficientes por sí solos. El entorno tecnológico moderno es complejo y está caracterizado por sistemas interconectados, infraestructuras heredadas y amenazas cibernéticas en constante evolución, lo que exige que las organizaciones pasen de una mentalidad centrada en la seguridad a una mentalidad centrada en la resiliencia.

La ciberresiliencia va mucho más allá de prevenir ataques; refleja la capacidad de una organización para resistir, recuperarse y adaptarse a las perturbaciones externas provocadas por riesgos cibernéticos. Las interrupciones ocurrirán incluso frente a las defensas más avanzadas. Como se define en la literatura especializada, la ciberresiliencia es "la capacidad de seguir ofreciendo el resultado previsto a pesar de la ocurrencia de eventos cibernéticos adversos".[1]

La ciberresiliencia es importante porque está fundamentalmente ligada a la confianza.

La ciberresiliencia es importante porque está intrínsecamente vinculada a la confianza de clientes, socios, reguladores y del ecosistema en general. Una resiliencia eficaz garantiza la continuidad operativa, mantiene la confianza de las partes interesadas y minimiza el impacto a largo plazo de los incidentes cibernéticos. En última instancia, una organización resiliente no solo sobrevive a una disrupción; aprende, se adapta y emerge fortalecida.

El Centro Europeo de Ciberresiliencia de Mastercard

En toda Europa y alrededor del mundo, las amenazas cibernéticas se han vuelto más frecuentes, más automatizadas y cada vez más coordinadas. Los atacantes actúan con mayor rapidez, se dirigen a infraestructuras críticas y explotan la interconexión de nuestra economía digital. Existe un amplio consenso entre gobiernos, reguladores e industria en que la ciberresiliencia es una responsabilidad colectiva.

La resiliencia no se puede construir en compartimentos aislados.

Es en este contexto que **Mastercard creó el Centro Europeo de Ciberresiliencia (ECRC) en 2024. Diseñado para fortalecer nuestra capacidad de proteger a Mastercard, nuestra red, nuestros clientes y, en última instancia, a los consumidores,** el ECRC también responde a las expectativas de gobiernos, responsables políticos y organismos reguladores de toda Europa.

El ECRC reúne a más de 30 equipos de toda la organización, permitiéndonos acelerar nuestra capacidad de respuesta y recuperación, manteniendo al mismo tiempo un fuerte enfoque regional en Europa. También refuerza un principio fundamental: la resiliencia no puede construirse en silos. Las amenazas cibernéticas no respetan fronteras, y nuestra respuesta tampoco debe hacerlo. El Centro fortalece la colaboración público-privada, mejora la conciencia situacional y apoya la defensa colectiva en todo el ecosistema de pagos.

En esencia, el ECRC se basa en el principio **de seguridad a través de la unidad**. Trabajamos estrechamente con instituciones financieras líderes, altos directivos de Mastercard, reguladores, fuerzas del orden, bancos centrales e instituciones europeas. Seguimos ampliando este ecosistema, incorporando socios de gobiernos, industria y organizaciones internacionales como parte de un compromiso compartido con la resiliencia.

El ECRC desempeña un papel fundamental en la respuesta a incidentes, la coordinación de acciones y la colaboración con las

partes interesadas para garantizar una respuesta eficaz. Al mismo tiempo, **el ECRC mira más allá del horizonte inmediato, analizando escenarios de baja probabilidad pero alto impacto** que podrían afectar a Mastercard o al ecosistema en general. Este enfoque prospectivo impulsa actividades como la planificación de contingencias, ayudando a la organización a prepararse tanto para los mejores como para los peores escenarios, así como a desarrollar estrategias de mitigación eficaces. De forma similar, el evento "Threatcasting", celebrado en octubre de 2025, reunió a expertos de la industria, el mundo académico, organismos gubernamentales, entidades reguladoras y organizaciones no gubernamentales para explorar tecnologías emergentes y desarrollar estrategias de mitigación antes de que los riesgos futuros lleguen a materializarse (con un horizonte de entre 5 y 10 años).

Gestión de crisis en Mastercard

Las crisis son situaciones anormales, inestables y complejas que representan una amenaza seria para la reputación y la existencia de una organización. Una crisis ocurre cuando los procesos establecidos han fallado o no pueden abordar plenamente la magnitud o la urgencia de un evento. En estos momentos, los procedimientos normales de gobierno corporativo y respuesta a incidentes no son suficientes.

En Mastercard definimos la gestión de crisis como el proceso estructurado de predecir, prevenir, prepararse para, responder a y recuperarse de eventos que tienen el potencial de afectar significativamente a una organización. La gestión de crisis es esencial porque toda organización, independientemente de su tamaño o nivel de madurez, enfrentará inevitablemente una crisis en algún momento. Ninguna organización es demasiado grande para fracasar y los incidentes importantes pueden escalar rápidamente sin un liderazgo coordinado. La gestión de crisis proporciona la estructura necesaria para coordinar la toma de decisiones bajo

presión y evitar respuestas reactivas o mal fundamentadas.

Ejercicios de Ciber Crisis

El ejercicio de cibercrisis es lo que convierte en práctica los planes de resiliencia.

Los Ejercicios de Ciber Crisis son lo que transforma los planes de resiliencia en una práctica real. Las políticas y los planes por sí solos no son suficientes; los ejercicios los convierten en acciones concretas al poner a prueba el desempeño de los equipos bajo presión y ayudarles a comprender cómo responder cuando se produce una interrupción. Realizar ejercicios en tiempos de normalidad permite a las organizaciones identificar brechas, comprender mejor sus desafíos y evaluar si los procesos actuales son adecuados para su propósito.

Uno de los principales beneficios de los ejercicios de crisis es **el desarrollo de memoria operativa**. Trabajar con escenarios realistas ayuda a los equipos a recordar información con rapidez, actuar con confianza y tomar mejores decisiones bajo presión. En última instancia, un plan es tan sólido como su ensayo. Los Ejercicios de Ciber Crisis garantizan que los equipos de respuesta no solo sepan qué está escrito, sino cómo aplicarlo cuando la situación sea compleja o inesperada.

Es importante equilibrar los ejercicios internos, que permiten probar procesos propios, con ejercicios externos o sectoriales, que ayudan a mejorar la coordinación con el ecosistema en general. Estos ejercicios pueden realizarse de forma presencial o virtual, dependiendo de su alcance, recursos y objetivos.

Existen varios tipos de ejercicios, cada uno con una finalidad diferente:

1. **Ejercicios de revisión guiada** son sesiones basadas en discusión diseñadas para familiarizar a los equipos con los planes, funciones y responsabilidades. Ayudan a identificar brechas de alto nivel y garantizar que todos comprendan los fundamentos del proceso de respuesta.

2. **Ejercicios de tabletop**, el formato más común, guían a los equipos a través de un escenario de crisis simulado

que evoluciona paso a paso, requiriendo que los participantes analicen decisiones y acciones. Son una forma práctica de probar la coordinación en un entorno seguro.

3. **Ejercicios en vivo**, también conocidos como Cyber Ranges, van un paso más allá al activar procedimientos, sistemas y personal reales en tiempo real. Estos ejercicios validan la preparación operativa, ponen a prueba herramientas y tecnologías y generan una mayor confianza en los equipos responsables de la respuesta.

La selección del tipo de ejercicio adecuado depende de la madurez, capacidad y perfil de riesgo de la organización. Un enfoque basado en riesgos ayuda a determinar qué escenarios deben priorizarse, ya que ninguna organización puede probar todas las situaciones posibles.

También es importante reconocer que los equipos de respuesta ante crisis tienen distintos niveles de experiencia y confianza. El formato, la dificultad y el contenido de los ejercicios deben adaptarse a los participantes involucrados.

Lecciones Aprendidas de los Ejercicios de Ciber Crisis

Las lecciones aprendidas convierten los ejercicios de crisis en cambios accionables.

Las lecciones aprendidas convierten los ejercicios de crisis en mejoras concretas y accionables. El objetivo es permitir que todos los equipos participantes reflexionen sobre lo que funcionó correctamente durante la respuesta simulada y dónde se necesitan mejoras para evitar repetir los mismos errores durante un incidente real. Las lecciones aprendidas impulsan actualizaciones de manuales operativos, clarifican funciones y responsabilidades, refinan rutas de escalamiento y optimizan procesos, fortaleciendo así la preparación ante crisis en toda la organización.

Es importante evitar un error habitual: **las lecciones deben analizarse de forma integral**. Si una brecha aparece en una

región o departamento, podría existir en otros. Si un rol es ambiguo en un manual, esa misma ambigüedad podría estar presente en procesos similares. Las mejoras identificadas deben aplicarse de manera consistente en toda la organización para garantizar la alineación y fortalecer la resiliencia colectiva.

2

Solución de Ejercicios de Ciber Crisis

Cyber Crisis Exercise: una solución de ejercicios de tabletop basada en datos e inteligencia.

En un documento publicado previamente por Mastercard[2], el equipo de Cybersecurity Solutions explicó cómo el entorno operativo actual y la realidad del ecosistema descritos anteriormente, combinados con la experiencia y el liderazgo intelectual de Mastercard, crearon una oportunidad para colaborar con líderes de la industria de simulación de ciberseguridad y ofrecer a los clientes de Mastercard una solución orientada a fomentar la validación de sus planes de resiliencia mediante ejercicios periódicos, utilizando las lecciones aprendidas para promover mejores prácticas de preparación de la fuerza laboral en materia de ciberseguridad y fortalecer la ciberresiliencia. El resultado de esta colaboración es Ejercicios de Ciber Crisis, una solución de ejercicios de mesa impulsada por datos e inteligencia, impartida por los expertos de Cybersecurity Advisory de Mastercard para apoyar la toma de decisiones y respaldada por Immersive, una plataforma líder en simulación de crisis y uno de los socios tecnológicos de Mastercard.

La oferta de Ejercicios de Ciber Crisis complementa el portafolio integrado de soluciones de ciberseguridad de Mastercard, enfocado en evaluar la exposición al riesgo al ritmo del negocio, proteger frente a amenazas mediante inteligencia avanzada y **fortalecer la confianza del ecosistema mediante** la mejora continua de la ciberseguridad a nivel global. La solución aborda directamente el factor humano de la ciberresiliencia, destacando que la tecnología y los procesos solo son tan eficaces como las capacidades de las personas que los utilizan.

Desde su lanzamiento en 2024, Ejercicios de Ciber Crisis ha evolucionado en respuesta a las necesidades y desafíos del mercado. Aunque inicialmente fue diseñado como un servicio prestado exclusivamente por consultores con el apoyo de los

asesores de ciberseguridad de Mastercard, la interacción con los clientes dejó claro que las organizaciones tienen ritmos y requisitos distintos en relación con la frecuencia de los ejercicios, determinados en muchos casos por su tamaño, complejidad y los marcos regulatorios aplicables. Como respuesta, en 2025 la solución incorporó una modalidad de **Autoejercicios**, permitiendo a los clientes acceder a la plataforma Immersive y ejecutar simulaciones cibernéticas a su propio ritmo a partir de un catálogo de escenarios de crisis impulsados por inteligencia artificial e inteligencia de amenazas. Estos escenarios son seleccionados y adaptados por los asesores de Mastercard en función del panorama de amenazas y de los vectores de ataque más probables para cada organización. Gracias a esta nueva capacidad, las instituciones de mayor tamaño y aquellas que constituyen objetivos prioritarios para los atacantes pueden poner a prueba sus planes de resiliencia de forma trimestral, en línea con las recomendaciones de mejores prácticas de Mastercard.

Laboratorios de Capacitación como método para implementar las lecciones aprendidas tras un ejercicio.

Además, la solución se ha vuelto más accionable mediante la incorporación de Laboratorios de Capacitación como mecanismo para implementar las lecciones aprendidas después de cada ejercicio. Estos laboratorios prácticos, disponibles en la plataforma Immersive y personalizados por los asesores, están alineados con las rutas de ataque utilizadas en los escenarios de crisis del ejercicio original. Asimismo, funcionan como una herramienta de capacitación especializada para aquellos participantes —equipos o individuos— cuyo desempeño durante la simulación evidenció brechas de conocimiento o preparación. Los Laboratorios de Capacitación permiten a los clientes de Mastercard desarrollar y medir habilidades específicas de su personal de ciberseguridad como parte de un **ciclo continuo de validación y mejora**, utilizado para construir programas permanentes de ejercicios y fortalecer la resiliencia con el tiempo. En otras palabras, se "valida" la preparación mediante ejercicios, se "mejora" a través de los laboratorios y posteriormente se vuelve a "validar" el progreso en ejercicios futuros.

El siguiente paso para Ejercicios de Ciber Crisis en 2026 será aprovechar la experiencia de Corporate Security y del Centro Europeo de Ciberresiliencia de Mastercard, junto con las mejores prácticas de gestión de crisis, para ofrecer a los clientes **ejercicios cibernéticos en vivo** o Simulacros Cibernéticos más completos. Estos ejercicios incorporarán Cyber Ranges técnicos combinados con simulaciones estratégicas de mesa dirigidas a niveles ejecutivos. Esta nueva categoría de solución adoptará un modelo similar, aunque de menor escala, al utilizado en los Ejercicios de Ciberdefensa de Mastercard (CDX), descritos en la siguiente sección. Los Simulacros Cibernéticos permitirán a los clientes de Mastercard reducir de forma medible la duración y el costo de los incidentes mediante la validación y optimización de la eficacia colectiva de sus equipos —tácticos, operativos y estratégicos/ejecutivos— frente a ataques realistas. Asimismo, impulsarán programas de gestión de crisis centrados en resultados, garantizarán la alineación entre los ejercicios cibernéticos y otras iniciativas de seguridad, y ayudarán a preparar a las organizaciones para los desafíos futuros mediante una mayor ciberresiliencia.

3

¿Qué es CDX?

El CDX ha evolucionado con el tiempo para centrarse en la capacitación y la realización de ejercicios que ponen a prueba los componentes tácticos, operativos y estratégicos que conforman una organización del sector privado.

El Ejercicio de Ciberdefensa de Mastercard (CDX) fue creado en 2016 con el objetivo de fomentar alianzas dentro de la industria y fortalecer las relaciones entre organizaciones. Esta iniciativa reúne a entidades públicas y privadas para mejorar la resiliencia y los planes de respuesta, **contribuyendo a la protección de infraestructuras críticas y la seguridad nacional**. Con el paso del tiempo, CDX ha evolucionado para centrarse en la capacitación y el entrenamiento de los componentes tácticos, operativos y estratégicos que conforman una organización.

El ejercicio táctico se desarrolla en el Cyber Range de Mastercard, que proporciona entornos técnicos simulados y prácticos para poner a prueba las defensas en tiempo real. Este ejercicio se complementa con un ejercicio de mesa colaborativo, basado en la discusión, que guía a los participantes a través de procesos de respuesta a incidentes, comunicación y toma de decisiones. Ambos ejercicios tienen como objetivo identificar brechas y fortalecer la resiliencia.

Uno de los Ejercicios de Ciberdefensa más recientes de Mastercard fue organizado por el Centro Europeo de Ciberresiliencia (ECRC) en octubre de 2025 como una iniciativa multisectorial europea. El ejercicio reunió a equipos técnicos y altos directivos de los sectores financiero y de telecomunicaciones en una simulación en tiempo real, tipo fuerza contra fuerza, que replicó un ciberataque sofisticado y complejo. Ante el incremento de las amenazas cibernéticas en Europa, el CDX del ECRC demostró cómo el sector privado, impulsado por la colaboración, puede liderar el fortalecimiento de las defensas mediante modelos escalables y repetibles de colaboración cibernética que pueden implementarse en distintos sectores y regiones geográficas. Descubra la historia completa aquí.[3]

¿Cuáles son los objetivos de CDX?

El Ejercicio de Ciberdefensa persigue tres objetivos principales:

1. **Fortalecer la preparación para la ciberdefensa en entornos reales.** Mejorar la capacidad de la organización para detectar, analizar y responder a ciberataques complejos y multivectoriales en un entorno realista y de alta presión.

2. **Mejorar la coordinación interfuncional e interorganizacional.** Impulsar una colaboración y comunicación más sólidas entre equipos internos de seguridad, unidades de negocio, liderazgo ejecutivo y socios externos durante incidentes cibernéticos de gran escala.

3. **Validar la resiliencia de la infraestructura crítica, los procesos y la tecnología.** Evaluar el desempeño de sistemas críticos —incluidas redes, aplicaciones, entornos en la nube, sistemas ICS/OT e integraciones con terceros— cuando son sometidos a escenarios de ataque persistentes y dirigidos. Toda esta actividad se registra para su análisis y elaboración de informes con el fin de apoyar una revisión estructurada posterior al ejercicio, comúnmente conocida como Informe Posterior a la Acción (After-Action Report o AAR), que documenta las tareas, decisiones, desafíos y resultados asociados al cumplimiento de estos objetivos.

¿Cómo se organiza el CDX?

Los recursos necesarios para desarrollar un evento dinámico y exitoso incluyen equipos rojos, equipos azules, responsables de respuesta a incidentes y líderes organizacionales, que conforman un equipo y participan junto con otros equipos con capacidades similares.

El ejercicio está diseñado para escalar progresivamente el escenario de incidente cibernético e involucrar a todos los niveles de la organización, desde el **nivel táctico** (equipos azules), pasando por el **nivel operativo** (equipos de respuesta a incidentes), hasta el **nivel estratégico** (liderazgo organizacional).

Desde una perspectiva técnica, el CDX está diseñado para simular redes empresariales pequeñas y medianas que reproducen cargas de trabajo típicas de productividad empresarial, así como aplicaciones orientadas a clientes con dependencias integradas.

- **Equipos Azules**: tienen la responsabilidad de defender redes que contienen vulnerabilidades de seguridad, configuraciones incorrectas y amenazas internas. Para ello, utilizan plataformas de código abierto que les permiten mantenerse independientes de proveedores específicos y les obligan a apoyarse en los fundamentos y principios básicos de la ciberseguridad para proteger sus entornos y responder a los ataques dirigidos contra sus redes.

- **Equipos Rojos**: son responsables de ejecutar operaciones ofensivas contra las redes de los Equipos Azules. Su objetivo es atacar aplicaciones e infraestructura de red para comprometer completamente los entornos objetivo, establecer persistencia y exfiltrar información durante sus campañas.

- **Equipos de Respuesta a Incidentes**: representan la capa operativa y de negocio de la organización. Su función es analizar el impacto empresarial asociado a los incidentes que los Equipos Azules gestionan en el ejercicio táctico. Esta parte del programa se desarrolla mediante un ejercicio de mesa (tabletop) y permite plantear objetivos específicos para evaluar cómo distintas áreas interesadas —como los equipos legales, de privacidad de datos o de comunicaciones externas— responderían ante una cibercrisis.

- **Liderazgo o Participantes Estratégicos**: participan en el ejercicio de mesa cuando los responsables de respuesta a incidentes elevan situaciones que requieren decisiones de carácter estratégico. Aspectos como las respuestas materiales al incidente, la gestión de la marca y la reputación, la comunicación con el consejo de administración o la coordinación con organismos gubernamentales y entidades públicas forman parte de los desafíos que deben abordar durante el CDX.

- **Socios**:
    - Mastercard selecciona a las organizaciones participantes a través de sus relaciones comerciales actuales y de su base de clientes, incluyendo bancos, emisores y adquirentes.
    - También se incorporan organizaciones pertenecientes a sectores de infraestructura crítica, especialmente de energía y telecomunicaciones.
    - Socios tecnológicos: WWT, Dell, Intel e Immersive.

- **Plataformas**:
    - La plataforma Cyber Range utilizada durante el ejercicio es proporcionada y respaldada por Mastercard.
    - Diseñada para replicar una red empresarial pequeña o mediana, esta infraestructura dedicada está optimizada para ofrecer resiliencia, estabilidad y rendimiento durante todo el evento. Los entornos de ataque y defensa también han sido diseñados y desarrollados por Mastercard y se ejecutan dentro de su Cyber Range.
    - La plataforma Immersive Crisis Exercise se utiliza para gestionar y ejecutar la parte de ejercicio de tabletop del programa.

4

De Simulacros Puntuales a una Resiliencia Continua

La mayoría de las organizaciones han aceptado una realidad difícil del panorama actual de amenazas: unas defensas sólidas reducen el riesgo, pero no lo eliminan. Cuando ocurre un incidente grave, los resultados dependen de la resiliencia; es decir, de la capacidad para mantener operativos los servicios críticos, tomar decisiones claras bajo presión, recuperarse rápidamente y adaptarse a medida que evolucionan los acontecimientos.

Este cambio también se refleja en la forma en que los reguladores, auditores y marcos de referencia de la industria abordan la preparación organizacional. En muchos sectores, se espera ahora que las organizaciones realicen simulaciones de incidentes de forma recurrente, no solo para "demostrar" su preparación, sino para mejorar continuamente la coordinación, los procesos de escalamiento y las comunicaciones.

En la práctica, la mayor brecha rara vez es la ausencia de un documento. El verdadero desafío suele encontrarse en el elemento humano y organizacional: quién reúne a quién, con qué rapidez se toman las decisiones, qué información es relevante, cómo se evalúan los compromisos y cómo la respuesta técnica se alinea con las prioridades del negocio. Por eso, el futuro de los ejercicios de crisis se está alejando de los ejercicios de mesa anuales realizados únicamente para cumplir requisitos, evolucionando hacia una práctica continua y medible que genera un verdadero ritmo operativo.

Cuando los ejercicios están bien diseñados, crean una memoria operativa efectiva. Las personas aprenden a actuar en situaciones de incertidumbre, a escalar incidentes en el momento adecuado y a comunicarse con claridad. Por el contrario, cuando los ejercicios son demasiado simples,

excesivamente guionizados o poco frecuentes, existe el riesgo de generar el efecto opuesto: una falsa sensación de confianza y planes que parecen sólidos sobre el papel, pero que fracasan bajo presión.

La próxima generación de Ejercicios de Ciber Crisis estará definida por tres características fundamentales:

1. Realismo, que obligue a los equipos a reaccionar como lo harían ante una situación real.
2. Frecuencia, que evite la pérdida de capacidades y el deterioro de las habilidades con el tiempo.
3. Integración, que conecte la respuesta técnica con la toma de decisiones ejecutivas.

El objetivo no es la simulación por sí misma. El objetivo es la preparación operativa y una cultura en la que la práctica sea habitual, las lecciones aprendidas se registren y las mejoras se implementen de manera efectiva.

Muchas organizaciones ya están combinando entornos de simulación realistas con facilitación experta para crear experiencias prácticas que reproduzcan de forma fiel la presión de un incidente real.

El objetivo no es la simulación por sí misma. El objetivo es la preparación operativa y una cultura en la que la práctica sea habitual, las lecciones aprendidas se registren y las mejoras se implementen de manera efectiva.

Un Modelo de Mejores Prácticas para un Programa Continuo de Ejercicios de Ciber Crisis

En lugar de tratar las simulaciones como eventos aislados, las organizaciones obtienen mejores resultados cuando implementan un programa continuo que crea un ciclo permanente de mejora: probar, aprender, capacitar, volver a probar e institucionalizar las mejoras. A continuación, se presenta un ciclo práctico de cuatro pasos.

PASO	DESCRIPCIÓN	FRECUENCIA RECOMENDADA	VALOR APORTADO
1. Simulacro Cibernético Inicial (Dirigido por Asesores)	Un ejercicio integral de cibercrisis dirigido por asesores que combina una simulación realista de incidentes con un taller de gestión de crisis para líderes, con el fin de evaluar la capacidad actual de respuesta y establecer una línea base.	Anual	Prueba de estrés realista de personas, procesos y tecnología. Establece indicadores y observaciones de preparación inicial. Identifica brechas en los planes de respuesta a incidentes, controles técnicos, claridad de funciones, procesos de escalamiento y toma de decisiones ejecutivas.
2. Capacitación Dirigida y Laboratorios	Programas de capacitación y talleres enfocados en abordar las debilidades identificadas durante el simulacro inicial. Pueden incluir laboratorios técnicos prácticos, ejercicios de comunicación de crisis, talleres de gestión de incidentes y ejercicios de ejecución de manuales operativos.	Continua (por ejemplo, mensualmente como parte de un programa de formación)	Cierra brechas específicas de habilidades y procesos. Refuerza las mejores prácticas y mantiene a los equipos actualizados. Fortalece la confianza y las capacidades en el uso de herramientas, flujos de trabajo y manuales operativos bajo presión.
3. Simulaciones Trimestrales Autogestionadas	Simulaciones periódicas realizadas internamente por la organización mediante una plataforma o escenarios previamente preparados. Generalmente tienen una duración de 60 a 120 minutos. Involucran a equipos técnicos de respuesta, continuidad de negocio, comunicaciones, áreas legales y liderazgo ejecutivo, según corresponda.	Trimestral	Mantiene la memoria operativa mediante la repetición. Valida que las mejoras implementadas funcionan en condiciones realistas. Fortalece una cultura de preparación continua y evita una mentalidad de cumplimiento basada en ejercicios puntuales.
4. Actualización de Planes de Continuidad y Manuales Operativos	Institucionaliza las lecciones aprendidas mediante la actualización de los Planes de Continuidad del Negocio (BCP), planes de respuesta a incidentes, rutas de escalamiento y manuales operativos tras ejercicios relevantes o cambios significativos.	Al menos una vez al año y después de ejercicios importantes o cambios significativos	Convierte las lecciones aprendidas en prácticas documentadas y repetibles. Cierra el ciclo entre los ejercicios y la mejora operativa. Garantiza que los planes permanezcan alineados con la manera en que los equipos responden realmente ante incidentes.

Consideraciones para el Futuro

Los Ejercicios de Ciber Crisis están evolucionando para ser cada vez más inmersivos y adaptativos. El diseño de escenarios continúa mejorando, las simulaciones son más fáciles de ejecutar para equipos distribuidos geográficamente y las plataformas digitales permiten escalar la repetición de ejercicios sin necesidad de una facilitación intensiva en cada ocasión.

Sin embargo, la tecnología no sustituirá el requisito fundamental: las personas deben practicar juntas. Las herramientas pueden hacer que los escenarios sean más realistas y facilitar la participación remota, pero la resiliencia sigue dependiendo de cómo los equipos se coordinan, toman decisiones, se comunican y ejecutan acciones bajo presión.

Las organizaciones que establecen un programa continuo de ejercicios hacen mucho más que simplemente sobrevivir a los incidentes. Se vuelven más ágiles, más serenas y más consistentes en su respuesta, y esa confiabilidad se traduce en confianza por parte de clientes, socios y reguladores.

Descubra cómo las soluciones de Ciberseguridad Empresarial de Mastercard, incluidos los Ejercicios de Ciber Crisis, pueden fortalecer la resiliencia de su organización. Conéctate con nuestro equipo para obtener más información.

Referencias

1. Björk, Fredrik, Henkel, M, Stirna, Janis, and Zdravkovic, J. (2015), "Cyber resilience – Fundamentals for a definition", in Rocha, Alvaro, Correia, Anna Maria, Costanzo, Sandra, and Reis, Luis Paulo (eds.), New contributions in information systems and technologies, Springer, London, pp. 311-316. doi: 10.1007/978-3-319-16486-1_31

2. Fail to Prepare, Prepare to Fail: Cyber Crisis Exercising for Operational Resilience Paper

3. Europe | Mastercard Newsroom

Colaboradores

Yonatan Israel Garzon
Director, Gestión de Producto, Riesgos y Resiliencia
Mastercard

Gokhan Demirel
Director, Gestión de Producto, Riesgos y Resiliencia
Mastercard

Fadwa Rachi
Director, Monitorización y Respuesta de Seguridad
Mastercard

Aaron Gomez
Director de Ingeniería de Seguridad de la Información
Mastercard

Coordinador

Eda Boltürk
Director, Desarrollo de Producto
Mastercard