ANÁLISIS PROSPECTIVO No. 3

FEBRERO
2026

ESCENARIOS Y RIESGOS PARA MÉXICO EN EL MARCO DE LA COPA MUNDIAL DE FUTBOL FIFA-2026 CANADA, MEXICO, USA

SAPIENS INTELLIGENCE CONSULTING GROUP
DIVISIÓN DE INTELIGENCIA ESTRATÉGICA.

MÉXICO, Febrero 2026

ESCENARIOS Y RIESGOS PARA MÉXICO EN EL MARCO DE LA COPA MUNDIAL DE FUTBOL FIFA-2026 CANADA, MEXICO, USA

Análisis Prospectivo

Este documento constituye un análisis técnico independiente y no representa posición oficial de ninguna institución gubernamental o académica.

ÍNDICE GENERAL

I. RESUMEN EJECUTIVO

El Mundial FIFA 2026 representa un evento de alcance global que transformará cualitativamente el perfil de amenazas de México durante el período enero-julio 2026. La convergencia de cuatro factores estructurales configura un escenario de riesgo complejo: (1) concentración masiva de personas en tres sedes metropolitanas con perfiles de riesgo diferenciados —Ciudad de México, Guadalajara y Monterrey—; (2) visibilidad mediática internacional que amplificará exponencialmente cualquier incidente de seguridad; (3) infraestructura crítica sometida a estrés operacional sostenido; y (4) un entorno criminal estructural caracterizado por fragmentación territorial y competencia entre organizaciones delictivas.

Hallazgos principales:

La amenaza de mayor probabilidad identificada es la violencia criminal oportunista, incluyendo depredación patrimonial, fraude y extorsión dirigidos a visitantes internacionales en corredores turísticos y logísticos de las tres sedes (probabilidad: 80-90%).

La amenaza de mayor impacto potencial corresponde a un incidente de violencia dirigida con motivación ideológica o terrorista, perpetrado por actor solitario radicalizado o célula pequeña, cuya probabilidad es media-baja (25-35%) pero cuyas consecuencias serían críticas para la reputación internacional del país.

El riesgo estratégico central no radica en un evento catastrófico aislado, sino en la acumulación de incidentes de seguridad que, en conjunto, degraden la narrativa de gobernanza efectiva ante la audiencia global. Esta tesis operativa orienta las recomendaciones hacia la prevención, detección temprana y capacidad de respuesta coordinada.

La ventana de máximo riesgo se concentra en la fase de grupos del torneo (11-26 de junio de 2026), cuando las tres sedes operarán simultáneamente con máxima dispersión geográfica de recursos. El partido inaugural en el Estadio Azteca (11 de junio, México vs. Sudáfrica) representa el momento de mayor simbolismo para las sedes mexicanas y, por tanto, de particular atractivo para actores amenazantes. Nota: la final del torneo (19 de julio) se celebrará en MetLife Stadium, Nueva Jersey, Estados Unidos.

Recomendación estratégica:

Se recomienda la implementación de un Centro de Fusión interinstitucional con gobernanza RACI claramente definida (Anexo D), sistema de Indicadores y Alertas Tempranas calibrado por sede (Anexo A), plan de colecciones de inteligencia multi-fuente (Anexo B), ejercicios de simulación previos al evento (Anexo C), reporteo estructurado diario y semanal (Anexos E-F), y protocolo de comunicación de crisis con vocería técnica preaprobada.

II. NOTAS METODOLÓGICAS

II.1 Enfoque analítico

El presente informe adopta un enfoque de inteligencia estratégica orientado a la anticipación de amenazas y la planificación de respuestas. No constituye un documento de inteligencia operativa ni describe tácticas, técnicas o procedimientos (TTPs) que pudieran ser explotados por actores adversarios. El análisis se fundamenta en la triangulación de fuentes abiertas, inferencia estructurada y aplicación de técnicas analíticas reconocidas en la comunidad de inteligencia.

II.2 Técnicas analíticas empleadas

II.2.1 Análisis de Hipótesis Competidoras (ACH)

Se aplicó la metodología ACH desarrollada por Richards J. Heuer Jr. (1999) para evaluar hipótesis alternativas sobre intenciones y capacidades de actores amenazantes, particularmente en escenarios de alta incertidumbre como la violencia dirigida de motivación ideológica. Esta técnica permite reducir sesgos cognitivos mediante la evaluación sistemática de evidencia a favor y en contra de cada hipótesis.

II.2.2 Indicadores y Alertas Tempranas (I&W)

El sistema I&W se diseñó conforme a los principios establecidos por Cynthia Grabo (2004) para la detección anticipada de amenazas. Los indicadores seleccionados cumplen criterios de: (a) observabilidad directa, (b) relevancia para las amenazas identificadas, (c) capacidad de calibración con línea base local, y (d) accionabilidad para la toma de decisiones.

II.2.3 Matriz Probabilidad/Impacto

La priorización de amenazas emplea una matriz P/I no lineal que integra, además de la probabilidad de ocurrencia y magnitud del impacto, variables adicionales: frecuencia esperada de incidentes, manejabilidad institucional, recursos de preparación requeridos, y consecuencias de segundo orden (Kaplan & Garrick, 1981).

II.2.4 Análisis de escenarios

Se desarrollaron tres escenarios prospectivos (bajo, medio y alto impacto) como herramientas de planificación, no como predicciones. La metodología sigue los principios de scenario planning aplicados a contextos de seguridad (Schwartz, 1991; van der Heijden, 2005).

II.3 Fuentes de información

El análisis se sustenta en las siguientes categorías de fuentes:

- Fuentes académicas y especializadas: Literatura revisada por pares sobre seguridad en eventos masivos, terrorismo, crimen organizado transnacional y gestión de crisis.
- Documentos institucionales: Publicaciones oficiales de FIFA, gobiernos anfitriones de Mundiales previos, y organismos internacionales de seguridad.
- Reportes de inteligencia de fuentes abiertas (OSINT): Análisis de medios, redes sociales y bases de datos especializadas.
- Precedentes históricos: Lecciones documentadas de eventos deportivos internacionales previos y sus incidentes de seguridad.

II.4 Supuestos estructurales

El análisis opera bajo los siguientes supuestos, cuya invalidación activaría una revisión inmediata del documento:

1. Las sedes mexicanas completan los preparativos logísticos y de seguridad con fricciones manejables dentro de los parámetros normales de coordinación interinstitucional.
2. El entorno criminal mantiene continuidad estructural sin reconfiguración mayor (fusiones, escisiones o escalamiento territorial significativo) en el horizonte de análisis.
3. La coordinación trinacional México–Estados Unidos–Canadá opera con tensiones diplomáticas normales, pero sin ruptura de cooperación en materia de seguridad.
4. No emerge un conflicto geopolítico mayor que afecte la participación de selecciones nacionales o genere boicots al evento.
5. La dimensión reputacional amplificará cualquier incidente de seguridad, independientemente de su magnitud física real.

II.5 Niveles de confianza

Las estimaciones de probabilidad expresan juicio analítico informado, no certeza estadística. Se emplean los siguientes niveles de confianza:

Nivel	Descripción	Criterio
Alto	Alta certeza en la estimación	Evidencia consistente, múltiples fuentes independientes, patrones históricos claros
Medio	Certeza moderada	Evidencia parcial, algunas fuentes contradictorias, variables inciertas
Bajo	Incertidumbre significativa	Evidencia limitada, escenarios sin precedente claro, alta dependencia de supuestos

II.6 Limitaciones del análisis

- El informe se basa en fuentes abiertas e inferencia analítica estructurada; no incorpora inteligencia clasificada que pudiera modificar sustancialmente las estimaciones.
- El horizonte de seis meses implica incertidumbre significativa sobre la evolución de variables políticas, económicas y criminales.
- Las probabilidades asignadas constituyen rangos estimados, no valores precisos.
- Los escenarios prospectivos son herramientas de planificación, no predicciones del futuro.

II.7 Gaps de inteligencia identificados.

Vacío de información	Impacto en el análisis	Requerimiento de colección
Intenciones actuales de liderazgos de organizaciones criminales respecto al evento	Incertidumbre en amenazas de extorsión y control territorial	Inteligencia humana focalizada (HUMINT)
Estado de radicalización de individuos en territorio nacional	Incertidumbre en amenaza de violencia dirigida	Coordinación con socios internacionales, monitoreo de canales extremistas
Capacidad real de respuesta CBRN en cada sede	Incertidumbre en preparación para eventos de cola	Evaluación técnica independiente de capacidades
Vulnerabilidades específicas de proveedores tecnológicos del evento	Incertidumbre en amenazas cibernéticas	Auditoría de ciberseguridad de terceros críticos

III.1 Panorama Estratégico: Por qué el Mundial cambia el perfil de amenaza

III.1.1 Factores de amplificación del riesgo

Amplificación mediática y simbolismo. El Mundial FIFA 2026 generará una audiencia acumulada estimada de más de cinco mil millones de espectadores a nivel global (FIFA, 2023). Esta exposición mediática sin precedentes implica que cualquier incidente de seguridad, independientemente de su escala física, escalará a crisis reputacional en cuestión de horas. El Estadio Azteca, sede del partido inaugural del torneo y recinto con carga simbólica histórica (finales de 1970 y 1986), representa el punto de máxima visibilidad inicial para México. Nota: la final del torneo se celebrará en MetLife Stadium, Nueva Jersey, Estados Unidos (19 de julio de 2026).

Concentración de blancos de alto valor. Se estima la llegada de más de 500,000 visitantes internacionales durante el período del torneo, incluyendo delegaciones oficiales de 48 países participantes, personalidades públicas, ejecutivos corporativos y medios de comunicación globales. Las Fan Zone's, hoteles sede y corredores de transporte concentrarán objetivos de alto valor simbólico y económico para actores amenazantes diversos.

Movilidad como centro de gravedad operacional. La dependencia de rutas y nodos específicos —aeropuertos internacionales, estaciones de transporte masivo, accesos a estadios— configura una fragilidad estructural ante bloqueos, fallas técnicas o eventos de pánico. El colapso de la movilidad constituye un multiplicador de cualquier otro incidente.

Superficie digital ampliada. Los sistemas de ticketing, reservaciones hoteleras, pagos electrónicos, transmisiones y comunicación pública expanden significativamente la superficie de ataque para ciberamenazas, fraude digital y campañas de desinformación.

Complejidad de coordinación institucional. El Mundial 2026 es el primer torneo trinacional en la historia, lo que implica tres marcos legales, tres culturas organizacionales y múltiples niveles de gobierno. En México, la coordinación federal-estatal-municipal presenta capacidades asimétricas entre sedes.

III.1.2 Análisis diferenciado por sede

Sede	Perfil de riesgo	Factores agravantes	Factores mitigantes
Ciudad de México (Estadio Azteca)	Mayor concentración poblacional; complejidad urbana extrema; sede del partido inaugural del torneo	Sistema de transporte saturado en condiciones normales; presencia de múltiples organizaciones criminales; historial de movilizaciones sociales	Mayor capacidad institucional federal; experiencia acumulada en eventos masivos internacionales
Monterrey (Estadio BBVA)	Proximidad a frontera internacional; presencia de organizaciones criminales con capacidad de alto impacto	Principal corredor de tráfico hacia Estados Unidos; tensiones recientes entre grupos criminales	Sector privado con capacidad de coordinación; infraestructura urbana moderna
Guadalajara (Estadio Akron)	Dinámica criminal propia; nodo logístico de alcance nacional	Presencia dominante del CJNG; historial de violencia de alto impacto en la región	Experiencia reciente en eventos internacionales (Juegos Panamericanos 2011)

III.1.3 Cronograma de concentración de riesgo

Fase	Fechas	Nivel de riesgo	Justificación
Pre-evento	Enero-Mayo 2026	Medio	Período de preparación, pruebas de estrés y acumulación de indicadores de alerta temprana
Fase de grupos	11-26 Junio 2026	Alto	Máxima dispersión geográfica de partidos; tres sedes operando simultáneamente; mayor volumen de visitantes en tránsito
Fase eliminatoria	27 Junio-6 Julio 2026	Medio-Alto	Reducción de sedes activas; intensificación de atención mediática en partidos decisivos
Semifinales y Final	9-19 Julio 2026	Crítico (para-EE.UU.)	Concentración máxima de atención global; semifinales y final en Estados Unidos. Para México: riesgo residual de incidentes con aficionados en tránsito

III.2 Tipología de Amenazas

III.2.1 Amenaza 1: Violencia criminal oportunista y depredación

Descripción. Incremento de delitos patrimoniales y contra personas, aprovechando la concentración de víctimas de alto valor económico (turistas internacionales) y la saturación temporal de capacidades policiales.

Modalidades identificadas: - Robo con violencia en corredores turísticos y zonas de hospedaje - Secuestro exprés en traslados aeropuerto-hotel-estadio - Fraude (boletos falsos, hospedaje fantasma, transporte pirata) - Clonación de tarjetas y fraude financiero - Estafas digitales mediante sitios web fraudulentos

Actores probables: Delincuencia común no organizada; células criminales oportunistas; estructuras de crimen organizado operando funciones de control territorial (“cobro de piso”).

Evaluación: Probabilidad ALTA (80-90%) | Impacto individual BAJO-MEDIO | Impacto agregado MEDIO-ALTO

III.2.2 Amenaza 2: Extorsión y control territorial de economías del evento

Descripción. Organizaciones criminales buscando capturar rentas de la economía temporal generada por el Mundial, incluyendo proveedores, comercio, transporte y servicios.

Modalidades identificadas: - Cobro de piso a negocios temporales en zonas de afluencia - Control de estacionamientos informales - Extorsión a transportistas y prestadores de servicios - Infiltración de cadenas de suministro del evento

Actores probables: Estructuras locales de crimen organizado con control territorial establecido en las zonas de sede.

Evaluación: Probabilidad ALTA (70-80%) | Impacto MEDIO

III.2.3 Amenaza 3: Disrupción social y protestas con escalamiento

Descripción. Movilizaciones sociales que aprovechen la visibilidad mediática del evento para posicionar demandas, con riesgo de escalamiento hacia violencia o bloqueo de operaciones críticas.

Modalidades identificadas: - Protestas pacíficas con efecto disruptivo en zonas de afluencia - Bloqueos de vialidades y accesos - Infiltración de grupos violentos en movilizaciones - Vandalismo y sabotaje menor

Actores probables: Colectivos sociales diversos; grupos anarquistas; oportunistas con agenda política.

Demandas potenciales: Comunidades desplazadas por obras de infraestructura; trabajadores afectados por el evento; activistas de derechos humanos; grupos ambientalistas.

Evaluación: Probabilidad ALTA (75-85%) | Impacto BAJO-MEDIO (variable según escalamiento)

III.2.4 Amenaza 4: Disrupción de movilidad e infraestructura urbana

Descripción. Acciones deliberadas o fallas sistémicas que colapsen sistemas de transporte y servicios críticos durante ventanas de máxima demanda operacional.

Modalidades identificadas: - Bloqueos coordinados de accesos a estadios y zonas de afluencia - Saturación inducida de nodos de transporte - Explotación de fallas técnicas existentes - Interrupción de servicios básicos (agua, electricidad, telecomunicaciones)

Actores probables: Grupos de presión; crimen organizado demostrando capacidad de disrupción; fallas sistémicas sin actor intencional.

Evaluación: Probabilidad MEDIA (40-50%) | Impacto ALTO

III.2.5 Amenaza 5: Ciberataques y fraude digital

Descripción. Ataques a la infraestructura digital del evento o explotación de la superficie digital ampliada para fraude masivo y disrupción de operaciones.

Modalidades identificadas: - Ataques DDoS contra sistemas críticos (ticketing, transmisiones) - Ransomware dirigido a proveedores del evento - Compromiso de sistemas de seguridad física - Campañas de phishing masivo temático - Fraude en sistemas de pago

Actores probables: Cibercriminales con motivación financiera; hacktivistas; actores estatales hostiles (operaciones de influencia).

Evaluación: Probabilidad ALTA (70-80%) para intentos | MEDIA (40-50%) para éxito significativo | Impacto MEDIO-ALTO

III.2.6 Amenaza 6: Desinformación e influencia

Descripción. Campañas coordinadas o espontáneas de información falsa que amplifiquen percepción de caos, generen pánico o dañen la reputación del evento y del país.

Modalidades identificadas: - Alertas falsas de ataques terroristas o incidentes graves - Videos manipulados presentados como incidentes reales - Narrativas de colapso de seguridad - Atribución falsa de responsabilidades - Polarización política inducida

Actores probables: Actores estatales hostiles; oportunistas políticos domésticos; amplificación algorítmica sin actor centralizado. Evaluación: Probabilidad ALTA (80-90%) | Impacto MEDIO (puede escalar a ALTO si genera pánico físico)

III.2.7 Amenaza 7: Violencia dirigida de alto impacto (baja probabilidad)

Descripción. Acto de violencia con motivación política, ideológica o terrorista, buscando impacto simbólico máximo y cobertura mediática global.

Modalidades plausibles: - Ataque de actor solitario radicalizado - Dispositivo explosivo improvisado en zona de concentración - Ataque vehicular contra multitudes - Ataque dirigido contra delegación nacional específica

Actores potenciales: Actor solitario radicalizado (espectro ideológico diverso); célula pequeña inspirada por grupos terroristas internacionales; extremistas domésticos.

Evaluación agregada: Probabilidad de algún incidente de violencia dirigida MEDIA-BAJA (25-35%) | Impacto CRÍTICO

III.2.8 Amenaza 8: Eventos de cola — Pánico masivo y amenazas CBRN

Descripción. Escenarios de muy baja probabilidad, pero impacto potencialmente catastrófico, incluyendo amenazas químicas, biológicas, radiológicas o nucleares (CBRN) y fallas de gestión de multitudes con fatalidades masivas.

Modalidades: - Estampida por pánico (detonada por falsa alarma o incidente real) - Amenaza CBRN empleada como mecanismo de terror psicológico - Incidente de aplastamiento (crowd crush) en accesos o durante evacuaciones

Consideración crítica. El impacto de estos escenarios es principalmente psicológico y reputacional. La preparación institucional debe enfocarse en: (1) prevención del pánico mediante comunicación efectiva, (2) protocolos de evacuación certificados según estándares internacionales, (3) capacidad de respuesta CBRN orientada a contención y comunicación de crisis, no necesariamente a respuesta ante ataque masivo real.

Lecciones de precedentes internacionales: - Seúl 2022 (Halloween): Incidente de aplastamiento con más de 150 fatalidades por falla en gestión de multitudes - Manchester 2017: Atentado terrorista en evento masivo con pánico secundario significativo - Boston 2013: Respuesta coordinada efectiva que limitó el impacto secundario del atentado

Evaluación: Probabilidad MUY BAJA (5-10%) | Impacto CRÍTICO

Análisis de Hipótesis Competidoras (ACH):

Hipótesis	Evidencia a favor	Evidencia en contra	Probabilidad estimada
H1: No ocurrirá atentado	México no es blanco histórico de terrorismo internacional; barreras operativas significativas para grupos extranjeros; ausencia de indicadores actuales	Precedentes globales de ataques en eventos deportivos masivos; propaganda terrorista ha mencionado Mundiales como objetivos simbólicos	65%
H2: Atentado de actor solitario	Patrón global creciente de ataques de "lobos solitarios"; baja barrera de entrada; máxima recompensa simbólica; extrema dificultad de detección previa	Menor prevalencia de violencia política individual en México comparado con otras regiones	22%
H3: Atentado de célula organizada	Capacidad demostrada de grupos terroristas internacionales; México como blanco simbólico por conexión con Estados Unidos	Ausencia de infraestructura terrorista conocida en territorio mexicano; barreras logísticas significativas	10%
H4: Atentado sofisticado/masivo	Impacto máximo en evento de esta escala justificaría inversión de recursos	Requiere capacidades no detectadas actualmente; alta dificultad operativa; alta probabilidad de detección durante preparación	3%

III.3 Escenarios Prospectivos (Enero–Julio 2026)

III.3.1 Escenario 1: Bajo Impacto

Probabilidad estimada: 25-30%

Descripción narrativa. El Mundial 2026 transcurre con incidentes menores que son manejados efectivamente por las autoridades. La narrativa internacional sobre México es predominantemente positiva o neutral, enfocada en los aspectos deportivos y culturales del evento.

Características del escenario: - Delincuencia común se mantiene en niveles controlados, sin casos de alto perfil mediático internacional - Protestas sociales se desarrollan de forma pacífica y son contenidas sin escalamiento - Incidentes cibernéticos menores son detectados y contenidos en cuestión de horas - No se materializa ningún ataque de violencia dirigida - Gestión de multitudes opera sin fatalidades ni incidentes graves

Indicadores de trayectoria hacia este escenario: - Baja actividad sostenida en indicadores de alerta temprana - Coordinación interinstitucional efectiva demostrada en eventos de prueba - Ausencia de amenazas creíbles detectadas por sistemas de inteligencia

Resultado. México refuerza su imagen de capacidad organizativa y se posiciona favorablemente para futuros eventos internacionales. Éxito reputacional significativo.

III.3.2 Escenario 2: Medio Impacto (Más Probable)

Probabilidad estimada: 50-55%

Descripción narrativa. Ocurren múltiples incidentes de seguridad que generan cobertura mediática negativa significativa, pero sin disrupción mayor de las operaciones del torneo. El evento se completa según lo programado con daño reputacional moderado pero manejable.

Características del escenario: - 10-20 casos documentados de delincuencia contra turistas con cobertura en medios internacionales - Al menos una protesta social con escalamiento menor (bloqueo temporal, enfrentamiento limitado con autoridades) - Incidente de gestión de multitudes con heridos (decenas, no fatalidades masivas) - Ciberataques logran afectación parcial de servicios (horas de interrupción) - Campañas de desinformación activas que requieren respuesta institucional sostenida - Posible amenaza terrorista que no se materializa o intento frustrado que se hace público - Al menos un incidente de violencia en estadio (confrontación entre aficiones)

Indicadores de trayectoria hacia este escenario: - Activación de múltiples indicadores de alerta temprana sin alcanzar umbrales críticos - Fricción observable en coordinación interinstitucional, pero sin colapso operativo - Narrativa mediática mixta con cobertura tanto de incidentes como de respuesta efectiva

Resultado. El evento se completa con daño reputacional moderado. Se documentan lecciones aprendidas significativas para futuros eventos.

Nota: El Anexo C contiene un ejercicio de simulación (TTX) diseñado específicamente para preparar la respuesta institucional ante este escenario.

III.3.3 Escenario 3: Alto Impacto

Probabilidad estimada: 15-20% Descripción narrativa. Ocurre al menos un evento grave que domina la cobertura mediática del Mundial y genera una crisis de gestión que trasciende el ámbito deportivo.

Posibles eventos detonadores: - Atentado terrorista con víctimas (cualquier escala) - Incidente de gestión de multitudes con fatalidades múltiples - Ataque de alto perfil de crimen organizado - Secuestro de figura pública (deportista, funcionario, periodista internacional) - Ciberataque que paralice infraestructura crítica por período extendido - Acumulación de incidentes menores que colapsen la capacidad de respuesta institucional

Indicadores de trayectoria hacia este escenario: - Múltiples indicadores de alerta temprana en umbral crítico (rojo) - Fallas significativas en coordinación durante eventos de prueba previos sin remediación - Amenazas creíbles detectadas, pero no neutralizadas

Resultado. Daño reputacional severo y duradero para México. Crisis diplomática probable con países de ciudadanos afectados. Consecuencias políticas domésticas significativas. Revisión profunda de protocolos para futuros eventos.

III.4 Matriz Probabilidad/Impacto y Priorización

Prioridad	Amenaza	Probabilidad	Impacto	Justificación de priorización
1	Violencia criminal oportunista	Alta (85%)	Medio	Alta frecuencia esperada; efecto acumulativo en narrativa internacional
2	Ciberincidentes + fraude digital	Alta (75%)	Medio-Alto	Casi certeza de intentos múltiples; potencial de impacto sistémico
3	Desinformación e influencia	Alta (85%)	Medio	Efecto multiplicador sobre todos los demás riesgos
4	Disrupción social/protestas	Alta (80%)	Bajo-Medio	Muy probable, pero con precedentes de manejo efectivo
5	Extorsión economías del evento	Alta (75%)	Medio	Afecta ecosistema de servicios; difícil detección
6	Disrupción movilidad/infraestructura	Media (45%)	Alto	Impacto operacional directo sobre el evento
7	Violencia en estadios/crowd management	Media (50%)	Medio-Crítico	Precedentes internacionales claros; requiere preparación específica
8	Violencia dirigida simbólica	Media-Baja (30%)	Crítico	Baja probabilidad compensada por máximo impacto; justifica preparación máxima
9	Eventos de cola (CBRN/pánico)	Muy Baja (7%)	Crítico	Preparación enfocada en manejo de pánico, no en materialización de amenaza

Nota metodológica. La priorización integra múltiples variables más allá de la función simple de probabilidad por impacto (P×I): frecuencia esperada de incidentes, manejabilidad institucional, recursos de preparación requeridos, tiempo de respuesta necesario, y consecuencias de segundo orden.

III.5 Indicadores y Alertas Tempranas (I&W)

Esta sección presenta los indicadores en formato analítico. Para la implementación operativa con sistema de semáforos, umbrales calibrados, responsables asignados y acciones preaprobadas, consultar el Anexo A: Tablero I&W.

Principio operativo. Todos los umbrales deben calibrarse con línea base local específica para cada sede, considerando estacionalidad y patrones históricos. Los indicadores son señales observables; los umbrales son específicos del contexto operacional.

III.5.1 Dominio CRIM/EXT — Violencia criminal oportunista

Indicador	Fuente de colección	Umbral sugerido
Variación porcentual en denuncias y llamadas 911 en corredores turísticos	C5, Fiscalías estatales	>30% respecto a línea base mensual
Detección de redes organizadas de fraude temático (boletos, hospedaje)	Monitoreo digital, denuncias	Cualquier red con >10 víctimas identificadas
Reportes consulares sobre victimización de extranjeros	Embajadas, SRE	>3 casos con modus operandi similar
Señales de vigilancia criminal (“halconeo”) en zonas de afluencia	Inteligencia policial	Detección confirmada
Incremento de secuestro exprés en rutas aeropuerto-centro	Fiscalías, reportes	Cualquier caso con víctima extranjera

III.5.2 Dominio SOC — Disrupción social y protestas

Indicador	Fuente de colección	Umbral sugerido
Convocatorias verificadas en fechas/lugares sensibles	Monitoreo de redes sociales	>1,000 confirmaciones de asistencia
Comunicados públicos anunciando “acciones directas”	Medios alternativos, comunicados	Cualquier amenaza específica contra el evento
Señales de infiltración en movilizaciones sociales	Inteligencia	Patrón identificado con evidencia
Tensiones laborales en servicios críticos del evento	Sindicatos, medios	Amenaza de paro en sector clave
Conflictos comunitarios por obras con escalamiento	Medios locales	Escalamiento a cobertura mediática nacional

III.5.3 Dominio MOB/INF — Movilidad e infraestructura

Indicador	Fuente de colección	Umbral sugerido
Bloqueos cortos/intermitentes en nodos críticos (“pruebas”)	Reportes viales, C5	>2 incidentes en misma ruta en 7 días
Incidentes menores repetitivos en sistemas de transporte	Operadores	Patrón sin causa técnica identificable
Saturaciones recurrentes sin causa técnica clara	Monitoreo de flujos	Anomalías inexplicadas sostenidas
Coordinación multi-actor para colapsar rutas	Inteligencia	Cualquier evidencia verificable
Fallas de continuidad en operadores sin remediación	Auditorías técnicas	Falla no corregida en >48 horas

III.5.4 Dominio CYB — Ciberincidentes y fraude digital

Indicador	Fuente de colección	Umbral sugerido
Incremento de escaneos/intentos de acceso a proveedores críticos	SOC, logs de seguridad	>200% respecto a línea base
Registro de dominios typosquatting relacionados con el evento	Monitoreo DNS	>10 dominios sospechosos activos
Compromisos confirmados en terceros (hotelería, pagos, transporte)	Alertas de industria	Cualquier compromiso confirmado
Picos de fraude digital temático	Denuncias, monitoreo	>50 casos en una semana
Ofertas de accesos/datos en foros underground	Threat intelligence	Cualquier oferta verificada relacionada

III.5.5 Dominio INFO — Desinformación e influencia

Indicador	Fuente de colección	Umbral sugerido
Narrativas coordinadas con amplificación artificial	Monitoreo de redes	Detección de patrones de coordinación
Viralización de contenido manipulado como “incidente real”	Fact-checkers, monitoreo	>100,000 interacciones
Llamados a violencia asociados al evento	Análisis de sentimiento	Tendencia creciente sostenida >72 horas
Fugas selectivas que erosionen confianza institucional	Medios, redes	Patrón de filtración dirigida
Mensajes contradictorios de voceros oficiales	Monitoreo de comunicación	Cualquier contradicción pública documentada

III.5.6 Dominio LOW-P/HIGH-I — Violencia dirigida

Indicador	Fuente de colección	Umbral sugerido
Amenazas específicas contra sedes o delegaciones	Inteligencia, monitoreo	Cualquier amenaza evaluada como creíble
Radicalización acelerada de individuos con fijación en el evento	Inteligencia, reportes de socios	Cualquier caso identificado
Vigilancia sospechosa en rutas o perímetros de seguridad	Seguridad pública/privada	Cualquier incidente confirmado
Propaganda terrorista mencionando Mundial/México	Monitoreo de canales extremistas	Cualquier mención específica
Adquisición anómala de materiales restringidos	FININT, controles comerciales	Cualquier patrón sospechoso

III.5.7 Dominio HOOL — Violencia en estadios y hooliganismo

Indicador	Fuente de colección	Umbral sugerido
Grupos de hooligans de riesgo viajando a México	Europol, Interpol, cooperación bilateral	Cualquier grupo identificado
Comunicaciones de grupos de aficionados sobre confrontaciones	Inteligencia policial, monitoreo	Cualquier plan específico detectado
Incidentes de violencia en partidos previos del torneo	Reportes FIFA, seguridad	Cualquier incidente documentado
Armas/objetos prohibidos detectados en filtros de acceso	Seguridad de estadios	>50% incremento respecto a línea base
Sobreventa o boletos falsos generando aglomeraciones	Control de accesos	Cualquier incidente de sobrecupo

III.6 Recomendaciones Accionables

III.6.1 Nivel Estratégico (Tomadores de decisión)

R1. Establecimiento del Centro de Fusión. Constituir un Centro de Fusión dedicado al Mundial con representación de los tres niveles de gobierno, proveedores críticos del sector privado, y enlaces internacionales permanentes (FBI, Europol, agencias de inteligencia de países participantes). Activación recomendada: 90 días antes del inicio del evento. Implementar estructura de gobernanza conforme a matriz RACI (Anexo D).

R2. Umbrales de decisión preaprobados. Documentar y aprobar formalmente umbrales para: activación de niveles de alerta, escalamiento de recursos, activación de protocolos de comunicación de crisis, y coordinación diplomática/consular. Validar mediante ejercicios de simulación antes de mayo 2026. Sistema de semáforo detallado en Anexo A.

R3. Sistema de reporteo estructurado. Implementar cadena de reporteo con Daily 1-Pager para nivel operativo (Anexo E) y Weekly Executive Brief para tomadores de decisión (Anexo F).

R4. Certificación de capacidades de crowd management. Verificar que cada sede cuente con certificación de capacidades conforme a estándares FIFA y mejores prácticas internacionales incorporando lecciones de incidentes recientes (Seúl 2022).

R5. Presupuesto de contingencia. Etiquetar presupuesto de contingencia con mecanismos de contratación de emergencia pre-autorizados. Objetivo: eliminar improvisación durante crisis.

R6. Protocolo de coordinación trinacional. Formalizar protocolo con Estados Unidos y Canadá que incluya: intercambio de inteligencia en tiempo real, respuesta conjunta ante incidentes que afecten ciudadanos de los tres países, y comunicación coordinada.

III.6.2 Nivel Operacional (Mandos de seguridad)

R7. Sistema I&W operativo. Implementar tablero de indicadores por sede con actualización diaria y umbrales de activación automática. Asignar responsable por cada indicador conforme a matriz RACI (Anexo D). Plan de colecciones detallado en Anexo B.

R8. Ejercicios de mesa (TTX). Conducir ejercicios de simulación para escenarios 2 y 3 antes de abril 2026, involucrando cadena completa de mando y coordinación. Utilizar guion de Anexo C como base y documentar brechas identificadas.

R9. Protocolos de movilidad resiliente. Desarrollar rutas alternativas pre-planificadas, capacidad de redireccionamiento en tiempo real, protocolos de comunicación directa con usuarios, y planes de control de nodos críticos.

R10. Ciberresiliencia de proveedores. Verificar planes de continuidad de negocio (BCP) de todos los proveedores críticos, incluyendo tiempos de recuperación declarados (RTO/RPO). Conducir ejercicios de respuesta a incidentes con coordinación público-privada.

R11. Equipos especializados por amenaza. Constituir equipos focalizados en: (a) inteligencia criminal sobre economías del evento, (b) monitoreo de radicalización y actores solitarios, (c) ciberamenazas, (d) detección y respuesta a desinformación.

R12. Capacidad CBRN. Verificar capacidad de respuesta CBRN en cada sede, con énfasis en detección, comunicación de crisis y manejo de pánico. El objetivo no es responder a un ataque masivo sino gestionar la percepción y el pánico.

R13. Cooperación internacional sobre aficiones de riesgo. Establecer coordinación con policías europeas para identificación y seguimiento de grupos de hooligans conocidos. Implementar protocolos de separación de aficiones en estadios.

III.6.3 Nivel Comunicación Pública

R14. Protocolo de vocería única. Designar voceros con autoridad técnica (no figuras políticas en funciones electorales) con mensajes preaprobados por escenario. Responsabilidad asignada a D/COMMS conforme a RACI (Anexo D).

R15. Unidad de verificación rápida. Establecer capacidad de detección y desmentido de desinformación en <2 horas, coordinada con plataformas digitales y medios de comunicación.

R16. Campaña preventiva para visitantes. Desarrollar campaña multilingüe con: información sobre riesgos reales, medidas de precaución, canales oficiales de emergencia, y aplicación móvil con alertas geolocalizadas.

R17. Narrativa de resiliencia. Preparar comunicación que no niegue incidentes sino demuestre capacidad de respuesta efectiva. Desarrollar mensajes para escenarios adversos, no solo para escenario de éxito.

R18. Coordinación con medios internacionales. Establecer expectativas realistas sobre contexto de seguridad con corresponsales y medios internacionales previo al evento. Evitar tanto alarmismo como minimización.

III.7 Riesgos de Segundo Orden

Dimensión	Riesgo	Mecanismo de activación	Mitigación recomendada
Reputación internacional	Incidente menor percibido como falla sistémica	Amplificación mediática desproporcionada; comparación desfavorable con otras sedes	Narrativa proactiva de capacidad de respuesta; comunicación oportuna y transparente
Impacto económico	Cancelaciones masivas, incremento de costos de seguridad, litigios	Percepción de inseguridad generalizada; incidentes con turistas de alto perfil	Seguros de contingencia; protocolos de respuesta rápida a víctimas; comunicación diferenciada
Relaciones diplomáticas	Crisis bilateral por incidentes con extranjeros	Ciudadanos de países específicos afectados; respuesta institucional percibida como inadecuada	Protocolos consulares predefinidos; comunicación directa con embajadas; rol de ENL/INTL en RACI
Derechos humanos	Excesos en control de protestas; detenciones arbitrarias; uso desproporcionado de fuerza	Presión institucional por "éxito" del evento; tensión entre seguridad y libertades	Protocolos de uso de fuerza con supervisión independiente; rol de D/LEGAL-DDHH en RACI; observadores
Política interna	Instrumentalización del evento; polarización por atribución de responsabilidades	Contexto político doméstico; oposición buscando capitalizar incidentes	Despolitización de estructura de seguridad; comunicación institucional no partidista
Precedente criminal	Crimen organizado percibe impunidad o debilidad institucional	Falta de respuesta efectiva ante extorsión o violencia durante el evento	Demostración de capacidad del Estado sin escalamiento contraproducente

III.8 Disparadores de Actualización

Este análisis debe someterse a revisión inmediata si ocurre cualquiera de los siguientes eventos:

1. Reconfiguración mayor del mapa criminal en cualquiera de las tres sedes (ruptura de treguas entre organizaciones, fusiones, o escalamiento territorial significativo)
2. Incidente de seguridad grave en evento deportivo internacional que demuestre nuevos patrones de ataque o inspire emulación
3. Fallas significativas en eventos de prueba (partidos preparatorios, ejercicios de movilidad) que no sean remediadas verificablemente
4. Evidencia creíble de amenaza específica contra sedes mexicanas, delegaciones participantes, o el evento en general
5. Emergencia de movimiento social organizado que adopte el Mundial como objetivo central de protesta sostenida
6. Cambio significativo en contexto político de México (crisis institucional, ruptura de coordinación con socios internacionales)
7. Detección de capacidades cibernéticas ofensivas nuevas o no anticipadas dirigidas específicamente al evento
8. Información de inteligencia proveniente de socios internacionales que invalide supuestos clave de este análisis

Cadencia de actualización programada: - Revisión mensual de indicadores de alerta temprana y tablero I&W - Actualización formal trimestral del análisis completo - Actualización inmediata ante cualquier disparador identificado.

IV. CONCLUSIONES

IV.1 Síntesis del análisis

El Mundial FIFA 2026 representa simultáneamente una oportunidad histórica y un desafío de seguridad sin precedentes para México. El análisis prospectivo presentado identifica un perfil de riesgo caracterizado no por una amenaza singular catastrófica, sino por la potencial acumulación de incidentes que, en conjunto, podrían degradar la narrativa de gobernanza efectiva ante una audiencia global de miles de millones de espectadores.

La tesis central de este informe sostiene que el riesgo dominante es de naturaleza acumulativa: la convergencia de criminalidad oportunista, disrupciones de movilidad, incidentes cibernéticos y campañas de desinformación tiene mayor probabilidad de materializarse que un evento catastrófico único. Esta caracterización del riesgo tiene implicaciones directas para la estrategia de preparación: se requiere un enfoque sistémico de detección temprana, respuesta coordinada y comunicación efectiva, más que la concentración exclusiva de recursos en escenarios de baja probabilidad.

IV.2 Hallazgos principales

Primero. Las tres sedes mexicanas presentan perfiles de riesgo diferenciados que requieren estrategias de preparación específicas. Ciudad de México enfrenta el mayor desafío de movilidad y concentración; Monterrey presenta la mayor exposición a dinámicas de crimen organizado fronterizo; Guadalajara combina riesgos de conflictividad social y presencia criminal consolidada.

Segundo. La fase de grupos del torneo (11-26 de junio) constituye la ventana de máximo riesgo operacional por la dispersión simultánea de partidos en las tres sedes. El partido inaugural en el Estadio Azteca (11 de junio) representa el punto de mayor simbolismo para las sedes mexicanas. Nota: la final del torneo se celebrará en Estados Unidos (MetLife Stadium, 19 de julio), por lo que las fases eliminatorias avanzadas no representan riesgo operativo directo para México, aunque sí riesgo reputacional indirecto.

Tercero. El sistema de indicadores y alertas tempranas propuesto permite la detección anticipada de escalamiento en las principales categorías de amenaza. Su efectividad dependerá de la calibración rigurosa con líneas base locales y la disciplina en el reporteo estructurado.

Cuarto. La gobernanza del Centro de Fusión, articulada mediante la matriz RACI, proporciona claridad sobre responsabilidades y cadenas de decisión que resultan críticas en situaciones de crisis donde la ambigüedad institucional puede ser tan dañina como la amenaza misma.

IV.3 Recomendaciones prioritarias

La implementación efectiva de las recomendaciones contenidas en este informe requiere acción inmediata en tres frentes:

1. Gobernanza (febrero 2026). Constituir formalmente el Centro de Fusión con la estructura de roles propuesta, validar la matriz RACI con todos los actores involucrados, y establecer los canales de comunicación y escalamiento.

2. Capacidades (marzo-abril 2026). Conducir los ejercicios de simulación, verificar las capacidades de los proveedores críticos, calibrar el sistema de indicadores con líneas base reales, y posicionar los recursos de contingencia.

3. Coordinación (mayo 2026). Activar el reporteo estructurado diario/semanal, realizar los ajustes finales basados en las pruebas de estrés, y confirmar los protocolos de comunicación de crisis con todos los voceros designados.

IV.4 Consideración final

El éxito en la gestión de seguridad del Mundial 2026 no se medirá por la ausencia total de incidentes —expectativa que sería irrealista dado el perfil de riesgo identificado— sino por la capacidad institucional de anticipar, prevenir cuando sea posible, y responder efectivamente cuando la prevención no sea suficiente. La preparación rigurosa, la coordinación efectiva y la comunicación transparente constituyen los pilares sobre los cuales México puede convertir este desafío en una demostración de capacidad institucional ante el mundo.

El presente análisis y sus instrumentos operativos asociados proporcionan el marco analítico y las herramientas prácticas para esta preparación. Su valor dependerá, en última instancia, de la voluntad institucional para implementarlos con rigor y sostenerlos con disciplina a lo largo de los próximos seis meses.

“La seguridad de un evento no se mide por la ausencia de incidentes, sino por la capacidad de anticiparlos, prevenirlos cuando es posible, y responder efectivamente cuando no lo es.”

V. REFERENCIAS BIBLIOGRÁFICAS

Fuentes académicas y especializadas

Crenshaw, M. (2011). *Explaining terrorism: Causes, processes and consequences*. Routledge.

Grabo, C. M. (2004). *Anticipating surprise: Analysis for strategic warning*. Center for Strategic Intelligence Research, Joint Military Intelligence College.

Heuer, R. J., Jr. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). Columbia University Press.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1), 11-27.

Schwartz, P. (1991). *The art of the long view: Planning for the future in an uncertain world*. Currency Doubleday.

Silke, A. (Ed.). (2014). *Prisons, terrorism and extremism: Critical issues in management, radicalisation and reform*. Routledge.

van der Heijden, K. (2005). *Scenarios: The art of strategic conversation* (2nd ed.). John Wiley & Sons.

Documentos institucionales y reportes oficiales

Europol. (2023). *EU terrorism situation and trend report 2023 (TE-SAT)*. European Union Agency for Law Enforcement Cooperation.

FIFA. (2023). *FIFA World Cup 2026 bid evaluation report*. Fédération Internationale de Football Association.

FIFA. (2024). *Stadium safety and security regulations* (2024 ed.). Fédération Internationale de Football Association.

Global Terrorism Database. (2023). *National Consortium for the Study of Terrorism and Responses to Terrorism (START)*. University of Maryland.

International Centre for Sport Security. (2022). *Securing major sporting events: A framework for organizers*. ICSS.

U.S. Department of Homeland Security. (2024). *Homeland threat assessment 2024*. DHS.

U.S. Department of State. (2023). *Country reports on terrorism 2022*. Bureau of Counterterrorism.

Análisis de precedentes y lecciones aprendidas

Altheide, D. L. (2017). *Terrorism and the politics of fear* (2nd ed.). Rowman & Littlefield.

Boyle, M. J. (2013). The costs and consequences of drone warfare. *International Affairs*, 89(1), 1-29.

Giulianotti, R., & Klauser, F. (2010). Security governance and sport mega-events: Toward an interdisciplinary research agenda. *Journal of Sport and Social Issues*, 34(1), 49-61.

Korean National Police Agency. (2023). *Itaewon crowd crush incident: Investigation report and recommendations*. Government of the Republic of Korea.

Manchester Arena Inquiry. (2023). *Report of the public inquiry into the attack on Manchester Arena on 22nd May 2017* (Vols. 1-3). UK Government.

Spaaij, R. (2014). Sports crowd violence: An interdisciplinary synthesis. *Aggression and Violent Behavior*, 19(2), 146-155.

Fuentes sobre crimen organizado y seguridad en México

Astorga, L. (2015). *¿Qué querían que hiciera? Inseguridad y delincuencia organizada en el gobierno de Felipe Calderón*. Grijalbo.

Dudley, S. S. (2022). *MS-13: The making of America's most notorious gang* (Updated ed.). Hanover Square Press.

Grillo, I. (2016). *Gangster warlords: Drug dollars, killing fields, and the new politics of Latin America*. Bloomsbury Press.

Instituto Nacional de Estadística y Geografía. (2024). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2024*. INEGI.

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2024). *Informe de víctimas de homicidio, secuestro, extorsión y robo de vehículos 2023*. SESNSP.

Ciberseguridad y amenazas digitales

FireEye Mandiant. (2023). *M-Trends 2023: Special report*. Mandiant.

Recorded Future. (2024). *Threat landscape for major sporting events*. Insikt Group.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. WEF.

ANEXOS

ANEXO A: TABLERO I&W

TRINITY-MEX2026-001-IW (v1.0)

Propósito: Anticipar escalamiento y activar decisiones preaprobadas mediante monitoreo sistemático de indicadores observables.

Cadencia operativa: - Actualización diaria: nivel operativo - Corte semanal: nivel decisor - Alerta inmediata: ante activación de umbrales

Cobertura geográfica: CDMX, Guadalajara, Monterrey

Ventana temporal del evento: 11 junio – 19 julio 2026

A.1 Dominios I&W y Sistema de Semáforo

Nota metodológica. Los umbrales presentados son sugerencias iniciales que deben calibrarse con línea base local (3-6 meses previos) y ajustarse por estacionalidad y contexto específico de cada sede.

Dominio 1: CRIM/EXT — Crimen depredador y extorsión

KPIs núcleo: - Variación porcentual en denuncias/llamadas 911 en corredores turísticos y nodos de transporte - Casos confirmados de targeting a extranjeros (hoteles/consulados) - Señales de cobro de piso a proveedores/comercio temporal - Incidentes de fraude temático (tickets/hospedaje/transportes)

Umbrales de activación: - 🟡 ÁMBAR: +20-30% vs línea base sostenido por 2 semanas, O 2+ casos de alto perfil con cobertura internacional - 🔴 ROJO: Patrón sostenido + incidentes contra delegación oficial/funcionario/medios con viralización global

Owner: Centro de Fusión (CRIMINT + FININT + enlaces hotelería/cámaras)

Dominio 2: SOC — Disrupción social y protestas

KPIs núcleo: - Convocatorias verificadas en fechas/lugares sensibles del evento - Evidencia de escalamiento (ultimátums públicos, anuncios de acciones directas, infiltración detectada) - Tensiones laborales en servicios críticos (movilidad, limpieza, salud, operación de estadios) - Bloqueos “de prueba” (intermitentes) en nodos críticos. Umbrales de activación: - 🟡 ÁMBAR: Convocatoria con tracción verificable + intención disruptiva declarada, O amenaza de paro en servicio crítico.

🔴 ROJO: Bloqueos coordinados en múltiples nodos, O violencia sostenida que comprometa rutas/servicios esenciales

Owner: D/GOV (Gobernabilidad) + Seguridad Pública + Protección Civil

Dominio 3: MOB/INF — Movilidad e infraestructura urbana

KPIs núcleo: - Saturación recurrente sin causa técnica identificable - Fallas repetidas en sistemas de transporte/telecom/energía con remediación incompleta - Incidentes menores repetitivos (vandalismo/sabotaje menor) en nodos críticos

Umbrales de activación: - 🟡 ÁMBAR: Interrupciones parciales repetidas por >48-72 horas sin corrección verificable - 🔴 ROJO: Caída prolongada de servicio crítico, O colapso de rutas primarias en día de partido

Owner: D/MOB + Operadores + SOC técnico

Dominio 4: CYB — Ciberincidentes y fraude digital

KPIs núcleo: - Picos de escaneo/ataques contra proveedores críticos del evento - Campañas de phishing temático y dominios engañosos activos - Incidentes en terceros (hotelería/pagos/transportistas) con potencial de spillover - Estado de integridad/continuidad (backups verificados, RTO/RPO probados)

Umbrales de activación: - 🟡 ÁMBAR: Campaña dirigida detectada + evidencia de compromiso parcial, O caída de servicio <6 horas - 🔴 ROJO: Interrupción significativa >6-12 horas, O afectación a sistemas de información al público/ticketing

Owner: D/CYB + CERT/SOC conjunto público-privado

Dominio 5: INFO — Desinformación y pánico

KPIs núcleo: - Narrativas coordinadas de “ataque/colapso/encubrimiento” con patrones de amplificación artificial - Reuso de material manipulado presentado como “incidente en sede” - Mensajes oficiales contradictorios (indicador interno crítico de vulnerabilidad)

Umbrales de activación: - 🟡 ÁMBAR: Rumor viral con tracción significativa + confusión institucional observable - 🔴 ROJO: Pánico físico observable (aglomeraciones/evacuaciones espontáneas), O pérdida de control narrativo a nivel internacional

Owner: D/COMMS + Célula de Comunicación de Crisis + Unidad de Verificación 24/7

Dominio 6: LOW-P/HIGH-I — Violencia dirigida

KPIs núcleo: - Amenazas específicas persistentes con elementos de trazabilidad - Vigilancia sospechosa confirmada en perímetros/rutas de seguridad - Incidentes precursores (falsas alarmas repetidas) con patrón identificable

Umbrales de activación: - 🟡 ÁMBAR: Amenaza específica evaluada como potencialmente creíble + al menos un precursor verificable - 🔴 ROJO: Convergencia de 2-3 señales independientes + elevación de credibilidad por análisis de inteligencia

Owner: D/INT + Contrainteligencia/Protección + Centro de Fusión

A.2 Protocolo de Acciones por Semáforo

Estado	Acciones preaprobadas
🟢 VERDE	Operación normal; calibración continua de línea base; preparación y conducción de TTX; monitoreo de rutina
🟡 ÁMBAR	Activar célula de fusión ampliada; desplegar refuerzo focalizado en área afectada; emitir comunicación preventiva; ejecutar pruebas de continuidad; notificar a ENL/INTL y LNO/PRIV
🔴 ROJO	Activar protocolo de crisis completo; establecer mando único por incidente; implementar comunicación “una sola voz”; activar coordinación consular/diplomática; autorizar medidas extraordinarias con supervisión de D/LEGAL-DDHH

ANEXO B: PLAN DE COLECCIONES

TRINITY-MEX2026-001-COLL (v1.0)

Objetivo: Alimentar el sistema I&W con cobertura multi-fuente optimizada, evitando saturación de información.

Principio rector: “Colección mínima viable” + “calidad sobre volumen”

B.1 Capas de Colección (Aplicables a todas las sedes)

Capa	Fuentes principales	Propósito analítico
OSINT local y georreferenciado	Prensa local, redes sociales, aplicaciones de transporte, cámaras empresariales, reportes de organizadores	Contexto general, tendencias de percepción, detección temprana de anomalías
CRIMINT/Seguridad pública	Línea 911, fiscalías, reportes de patrullaje, estadísticas por cuadrante (agregadas)	Indicadores de amenaza criminal, patrones de victimización
FININT (alto nivel)	UIF, señales de extorsión, flujos de efectivo atípicos, intermediación sospechosa en cadenas de suministro	Indicadores de control territorial y economía criminal
CYB Threat Intelligence	SOC, CERT, proveedores críticos, indicadores de compromiso compartidos	Amenazas digitales, vulnerabilidades emergentes
Infraestructura/Operadores	Energía, agua, telecomunicaciones, movilidad, estadios, hotelería	Estado de continuidad operativa, detección de fallas
Gobernabilidad/Conflict mapping	Agenda social, sindicatos, colectivos, calendario electoral local, conflictos por obras	Indicadores de disrupción social potencial

B.2 Prioridades de Colección por Sede

Ciudad de México

Prioridad	Dominio	Justificación
1	MOB/INF	Red de movilidad masiva y nodos multimodales representa el principal riesgo sistémico
2	INFO	Mayor amplificación mediática nacional e internacional; criticidad de “una sola voz”
3	CRIM/EXT	Corredores turísticos extensos, zonas de hospedaje dispersas, múltiples rutas de traslado

Guadalajara

Prioridad	Dominio	Justificación
1	SOC	Historial de protestas y agenda social activa; necesidad de gobernabilidad preventiva
2	CRIM/EXT	Presión documentada a proveedores y comercio en zona metropolitana
3	CYB	Concentración de proveedores del evento y sector servicios digitales

Monterrey

Prioridad	Dominio	Justificación
1	CRIM/EXT	Economía del evento y cadenas de suministro como objetivos de extorsión
2	MOB/INF	Accesos limitados, riesgo de congestión severa, dependencia de operadores específicos
3	CYB	Superficie corporativa amplia y terceros con integración digital

B.3 Productos de Inteligencia y Cadencia

Producto	Frecuencia	Audiencia	Contenido	Plantilla
Daily 1-Pager	Diario (am)	Nivel operativo	Semáforo del día + 5 cambios relevantes + acciones recomendadas	Anexo E
Weekly Executive Brief	Semanal (lunes)	Tomadores de decisión	Tendencias + riesgos de segundo orden + decisiones pendientes	Anexo F
Alerta Roja	Inmediato	Todos los niveles	Estructura: Hecho → Impacto → Acción requerida	N/A (formato libre)

ANEXO C: GUION TTX — ESCENARIO 2

TRINITY-MEX2026-001-TTX-S2 (v1.0)

Denominación del ejercicio: “Disruptivo Multimodal”

Propósito: Validar gobernanza, coordinación interinstitucional, continuidad operativa y comunicación de crisis. El ejercicio NO evalúa tácticas operativas.

Duración: 4-6 horas (tiempo simulado)

C.1 Objetivos de Aprendizaje

1. Validar funcionamiento de mando y coordinación (federal-estatal-municipal + sector privado)
2. Probar ciclo completo del tablero I&W: detección → análisis → decisión → acción
3. Evaluar continuidad de movilidad/servicios/ciber bajo presión simultánea
4. Probar protocolo de comunicación de crisis: distinción rumor vs. hecho; disciplina de vocería única
5. Verificar controles de legalidad y DDHH en manejo de protestas y decisiones de seguridad

C.2 Participantes Requeridos (Mínimo Viable)

Conforme a roles definidos en matriz RACI (Anexo D):

- COM (Coordinador General del Centro de Fusión)
- D/INT (Dirección de Inteligencia)
- D/OPS (Dirección Operacional)
- D/CYB (Ciberseguridad)
- D/MOB (Movilidad e Infraestructura)
- D/COMMS (Comunicación de Crisis)
- D/GOV (Gobernabilidad)
- D/LEGAL-DDHH (Legalidad y Derechos Humanos)
- ENL/INTL (Enlace Internacional/Consular)
- LNO/PRIV (Enlace Sector Privado)

C.3 Supuestos del Escenario

El ejercicio simula un día de partido en fase de grupos con los siguientes elementos convergentes:

1. Incremento sostenido de delitos depredadores en corredores turísticos
2. Convocatoria activa a protesta con intención disruptiva cerca de zona de afluencia
3. Incidente cibernético que degrada servicio informativo al público (app/portal)
4. Campaña de desinformación viral sobre supuesto "ataque" (falso/no verificado)
5. Disrupciones parciales de movilidad por combinación de congestión y bloqueo puntual

C.4 Línea de Tiempo (Injects)

Tiempo	#	Injects	Descripción	Decisión requerida	Responsable RACI
T0 (08:00)	1	I&W Ámbar CRIM	Aumento sostenido de reportes de robo/fraude temático; dos casos confirmados con víctimas extranjeras	¿Qué refuerzo focalizado se despliega? ¿Qué mensaje preventivo se emite?	A: COM / R: D/OPS, D/COMMS
T+45 min	2	SOC Ámbar	Convocatoria verificada a protesta cerca de estadio; mensajes en redes anuncian bloqueo	¿Se activa mesa de gobernabilidad? ¿Cuál es la ruta de negociación/contención?	A: D/GOV / R: D/OPS
T+90 min	3	CYB Ámbar	Portal/app informativa presenta degradación parcial; rumores en redes de "hackeo total"	¿Quién comunica y qué dice? ¿Cómo se coordina con proveedor?	A: D/CYB / R: CERT/SOC
T+120 min	4	INFO Ámbar→Rojo	Contenido viral (posible fake) afirma "ataque terrorista en sede"; comienza pánico digital	Activar célula de verificación; emitir mensaje "rumor vs. hecho"; controlar vocerías	A: D/COMMS / R: Verificación
T+150 min	5	MOB Ámbar	Disrupción de movilidad por congestión agravada + bloqueo puntual; tiempos de traslado se disparan	Activar rutas alternativas; coordinar con operadores; comunicar a usuarios	A: D/MOB / R: Operadores
T+210 min	6	Escalamiento internacional	Medio internacional solicita postura oficial; embajada pide confirmación sobre ciudadano supuestamente afectado	Activar canal diplomático; designar vocero único; articular narrativa de resiliencia	A: ENL/INTL / R: D/COMMS
T+270 min	7	Control DDHH	Tensión entre necesidad de contención y riesgo de uso excesivo de fuerza; cámaras de medios graban intervención	Verificar reglas de enfrentamiento; activar supervisión; documentar acciones	A: D/LEGAL-DDHH / R: D/OPS
T+330 min	8	Cierre	Servicio digital restablecido; protesta dispersada; persiste percepción de riesgo en narrativa	Definir plan de 72 horas: refuerzo, comunicación, investigación, documentación de lecciones	A: COM / R: Todos

C.5 Criterios de Evaluación (Scorecard)

Criterio	Indicador de éxito	Peso
Tiempo de ciclo I&W→decisión	<30 minutos desde detección hasta decisión documentada	20%
Consistencia de vocería	Cero contradicciones públicas entre voceros	20%
Continuidad de servicios	RTO alcanzado según lo declarado por operadores	15%
Coordinación con privados	Comunicación efectiva documentada con LNO/PRIV	15%
Manejo de protesta	Proporcionalidad verificable; cero incidentes graves de DDHH	15%
Capacidad de desmentido	<2 horas desde detección de fake hasta comunicación correctiva efectiva	15%

C.6 Productos Obligatorios del Ejercicio

1. Minuta de decisiones y responsables — Formato RACI, documentando cada decisión tomada
2. Lista priorizada de brechas identificadas — Clasificadas P0 (crítica) / P1 (alta) / P2 (media)
3. Plan de remediación — Con hitos a 30, 60 y 90 días
4. Propuesta de ajustes al tablero I&W — Modificaciones a umbrales y/o indicadores basadas en aprendizajes

ANEXO D: MATRIZ RACI — CENTRO DE FUSIÓN

TRINITY-MEX2026-001-RACI (v1.0)

Propósito: Eliminar ambigüedad en la asignación de responsabilidades, acelerar la toma de decisiones, y evitar el "diseño por comité" que paraliza la respuesta en situaciones de crisis.

D.1 Definición de Roles Funcionales

Código	Denominación	Función principal
COM	Coordinador General del Centro de Fusión	Dirección estratégica; decisión final en situaciones de ambigüedad; representación institucional
D/INT	Dirección de Inteligencia	Análisis de amenazas; aplicación de ACH; síntesis de información; priorización diaria
D/OPS	Dirección Operacional	Coordinación de despliegues; enlace con fuerzas de seguridad; ejecución de decisiones (sin TTPs)
D/CYB	Dirección de Ciberseguridad	Operación de CERT/SOC; continuidad digital; respuesta a incidentes cibernéticos
D/MOB	Dirección de Movilidad e Infraestructura	Coordinación con operadores críticos; continuidad de transporte y servicios
D/COMMS	Dirección de Comunicación de Crisis	Vocería única; verificación de información; protocolo anti-rumor
D/GOV	Dirección de Gobernabilidad	Gestión de conflictos sociales; enlace político-administrativo; negociación con actores
D/LEGAL-DDHH	Dirección de Legalidad y DDHH	Control de legalidad; supervisión de uso de fuerza; documentación; enlace con observadores
ENL/INTL	Enlace Internacional	Coordinación trilateral; comunicación con embajadas; gestión de incidentes con extranjeros
LNO/PRIV	Enlace Sector Privado	Coordinación con estadios, hotelería, transporte privado, operadores de pago

Nota estructural. En cada sede (CDMX, Guadalajara, Monterrey) puede constituirse una célula espejo con los mismos roles funcionales, subordinada operativamente al COM nacional.

D.2 Leyenda RACI

- R (Responsible): Ejecuta la tarea o función
- A (Accountable): Responsable final de que la tarea se complete; autoridad de decisión
- C (Consulted): Debe ser consultado antes de la decisión; comunicación bidireccional
- I (Informed): Debe ser informado después de la decisión; comunicación unidireccional

Regla fundamental: Cada función tiene exactamente un Responsable final. Sin Responsable definido, no hay ejecución autorizada.

D.3 Asignación RACI por Función Crítica

Función 1: Activación de nivel de alerta (Verde/Ámbar/Rojo)

Rol	Asignación
COM	A
D/INT	R (lectura de indicadores)
D/OPS	R (preparación de acciones)
D/COMMS	R (preparación de mensaje)
D/CYB, D/MOB, D/GOV, D/LEGAL-DDHH	C
ENL/INTL, LNO/PRIV	I

Función 2: Priorización diaria de amenazas (Top 3 por sede)

Rol	Asignación
COM	A
D/INT	R
D/OPS, D/MOB, D/CYB, D/GOV	C
D/COMMS, ENL/INTL, LNO/PRIV, D/LEGAL-DDHH	I

Función 3: Respuesta a disrupción de movilidad

Rol	Asignación
D/MOB	A
Operadores + D/OPS	R
D/INT, D/COMMS, D/LEGAL-DDHH	C
COM, ENL/INTL, LNO/PRIV	I

Función 4: Respuesta a ciberincidente con impacto público

Rol	Asignación
D/CYB	A
CERT/SOC + proveedor afectado	R
D/INT, D/COMMS, D/MOB (si afecta transporte), D/LEGAL-DDHH	C
COM, ENL/INTL, LNO/PRIV	I

Función 5: Manejo de protesta y gobernabilidad

Rol	Asignación
D/GOV	A
D/OPS + enlace local	R
D/INT, D/COMMS, D/LEGAL-DDHH	C
COM, ENL/INTL, LNO/PRIV	I

Función 6: Comunicación pública (incidente/rumor/pánico)

Rol	Asignación
D/COMMS	A
Equipo de verificación + vocería designada	R
COM, D/INT, D/OPS, D/LEGAL-DDHH	C
ENL/INTL, LNO/PRIV, D/MOB, D/CYB	I

Función 7: Coordinación consular/diplomática

Rol	Asignación
ENL/INTL	A
Enlace SRE/consular + D/COMMS	R
COM, D/INT, D/OPS, D/LEGAL-DDHH	C
D/MOB, D/CYB, LNO/PRIV	I

Función 8: Control de legalidad y DDHH

Rol	Asignación
D/LEGAL-DDHH	A
Supervisión + documentación + revisión	R
COM, D/OPS, D/COMMS	C
D/INT, ENL/INTL, D/GOV	I

D.4 Reglas de Mando

1. Una decisión = un Responsable final. Sin Responsable designado no hay autoridad para ejecutar.
2. Consulta en ventana definida. Los roles C tienen 15-30 minutos para responder en situación de crisis; sin respuesta se procede.
3. Información sin debate. Los roles I reciben reporte breve; no participan en la decisión.
4. Escalamiento claro. Si el A no puede decidir en el tiempo requerido, la decisión escala automáticamente a COM.
5. Post-mortem obligatorio. Toda decisión P0/P1 requiere revisión documentada dentro de 24-72 horas.

ANEXO E: PLANTILLA DAILY 1-PAGER

TRINITY-MEX2026-001-DAILY (v1.0)

Tiempo de lectura objetivo: 90-120 segundos

Cadencia: Emisión diaria (matutina) | Consolidación semanal para decisores

Responsable de emisión: D/INT

TRINITY DAILY — [FECHA]

Clasificación: RESERVADO (uso restringido) **Sedes:** CDMX | Guadalajara | Monterrey

SEMÁFORO GLOBAL: [🟢 VERDE / 🟡 ÁMBAR / 🔴 ROJO]
NIVEL DE CONFIANZA: [ALTO / MEDIO / BAJO]

1. TOP 3 RIESGOS DEL DÍA

#1 _____ | Prob: _____ % | Impacto: _____ | [Estable/Escalando]
#2 _____ | Prob: _____ % | Impacto: _____ | [Estable/Escalando]
#3 _____ | Prob: _____ % | Impacto: _____ | [Estable/Escalando]

2. CAMBIOS CLAVE (últimas 24 horas)

- **CRIM/EXT:** _____
- **CYB:** _____
- **SOC:** _____
- **INFO:** _____
- **MOB/INF:** _____
- **LOW-P/HIGH-I:** _____

3. INDICADORES I&W ACTIVADOS

🟡 **Ámbar:** _____ 🔴 **Rojo:** _____

Tendencia general: [MEJORANDO / ESTABLE / DETERIORANDO]

4. ACCIONES RECOMENDADAS (próximas 24-72h)

- Acción 1: _____ | A/R: _____ | Plazo: ___ h
- Acción 3: _____ | A/R: _____ | Plazo: ___ h

5. COMUNICACIÓN PÚBLICA

Mensaje recomendado: _____
Riesgo de desinformación: [BAJO / MEDIO / ALTO]
Vocero designado: _____

6. RIESGOS DE SEGUNDO ORDEN

- **Reputación internacional:** [BAJO / MEDIO / ALTO]
- **Derechos/legitimidad:** [BAJO / MEDIO / ALTO]
- **Diplomacia/consulares:** [BAJO / MEDIO / ALTO]
- **Economía/continuidad:** [BAJO / MEDIO / ALTO]

7. DISPARADORES DE RE-EVALUACIÓN INMEDIATA

⚠ _____
⚠ _____
⚠ _____

FIN — TRINITY DAILY

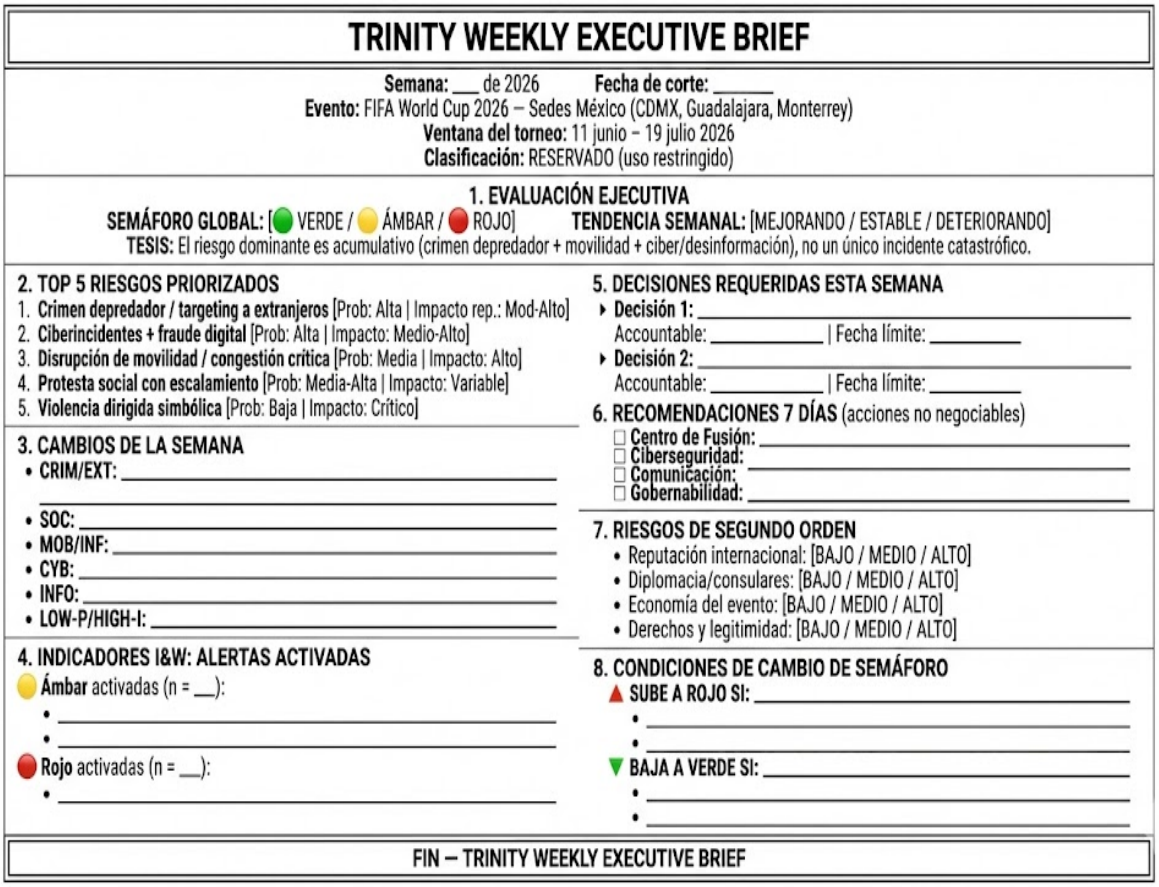
ANEXO F: PLANTILLA WEEKLY EXECUTIVE BRIEF

TRINITY-MEX2026-001-WEEKLY (v1.0)

Audiencia: Tomadores de decisión de nivel estratégico

Cadencia: Emisión semanal (lunes)

Responsable de emisión: D/INT + COM



TRINITY WEEKLY EXECUTIVE BRIEF

Semana: ___ de 2026 **Fecha de corte:** _____
Evento: FIFA World Cup 2026 – Sedes México (CDMX, Guadalajara, Monterrey)
Ventana del torneo: 11 junio – 19 julio 2026
Clasificación: RESERVADO (uso restringido)

1. EVALUACIÓN EJECUTIVA

SEMÁFORO GLOBAL: [VERDE / ÁMBAR / ROJO] **TENDENCIA SEMANAL:** [MEJORANDO / ESTABLE / DETERIORANDO]
TESIS: El riesgo dominante es acumulativo (crimen depredador + movilidad + ciber/desinformación), no un único incidente catastrófico.

2. TOP 5 RIESGOS PRIORIZADOS

1. **Crimen depredador / targeting a extranjeros** [Prob: Alta | Impacto rep.: Mod-Alto]
2. **Ciberincidentes + fraude digital** [Prob: Alta | Impacto: Medio-Alto]
3. **Disrupción de movilidad / congestión crítica** [Prob: Media | Impacto: Alto]
4. **Protesta social con escalamiento** [Prob: Media-Alta | Impacto: Variable]
5. **Violencia dirigida simbólica** [Prob: Baja | Impacto: Crítico]

3. CAMBIOS DE LA SEMANA

- **CRIM/EXT:** _____
- **SOC:** _____
- **MOB/INF:** _____
- **CYB:** _____
- **INFO:** _____
- **LOW-P/HIGH-I:** _____

4. INDICADORES I&W: ALERTAS ACTIVADAS

Ámbar activadas (n = __):
- _____
- _____

Rojo activadas (n = __):
- _____

5. DECISIONES REQUERIDAS ESTA SEMANA

- **Decisión 1:** _____
  Accountable: _____ | Fecha límite: _____
- **Decisión 2:** _____
  Accountable: _____ | Fecha límite: _____

6. RECOMENDACIONES 7 DÍAS (acciones no negociables)

- ☐ **Centro de Fusión:** _____
- ☐ **Ciberseguridad:** _____
- ☐ **Comunicación:** _____
- ☐ **Gobernabilidad:** _____

7. RIESGOS DE SEGUNDO ORDEN

- Reputación internacional: [BAJO / MEDIO / ALTO]
- Diplomacia/consulares: [BAJO / MEDIO / ALTO]
- Economía del evento: [BAJO / MEDIO / ALTO]
- Derechos y legitimidad: [BAJO / MEDIO / ALTO]

8. CONDICIONES DE CAMBIO DE SEMÁFORO

▲ **SUBE A ROJO SI:** _____
- _____
- _____

▼ **BAJA A VERDE SI:** _____
- _____
- _____

FIN – TRINITY WEEKLY EXECUTIVE BRIEF

ANEXO G: GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

G.1 Acrónimos institucionales y operativos

Acrónimo	Significado	Descripción
ACH	Analysis of Competing Hypotheses	Técnica analítica estructurada para evaluar hipótesis alternativas minimizando sesgos cognitivos
BCP	Business Continuity Plan	Plan de continuidad de negocio que establece procedimientos para mantener operaciones críticas durante y después de una disrupción
C5	Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano	Centros de monitoreo y coordinación de emergencias en entidades federativas de México
CBRN	Chemical, Biological, Radiological, Nuclear	Categoría de amenazas que involucran agentes químicos, biológicos, radiológicos o nucleares
CERT	Computer Emergency Response Team	Equipo de respuesta a emergencias informáticas
COM	Command / Coordinador General	Rol de mando en el Centro de Fusión
CRIMINT	Criminal Intelligence	Inteligencia criminal; información procesada sobre actividades delictivas
DDoS	Distributed Denial of Service	Ataque cibernético que busca saturar servicios mediante múltiples solicitudes simultáneas
D/COMMS	Dirección de Comunicación	Rol responsable de comunicación de crisis en el Centro de Fusión
D/CYB	Dirección de Ciberseguridad	Rol responsable de seguridad digital en el Centro de Fusión
D/GOV	Dirección de Gobernabilidad	Rol responsable de gestión de conflictos sociales en el Centro de Fusión

Acrónimo	Significado	Descripción
D/INT	Dirección de Inteligencia	Rol responsable de análisis en el Centro de Fusión
D/LEGAL-DDHH	Dirección de Legalidad y DDHH	Rol responsable de supervisión legal y derechos humanos
D/MOB	Dirección de Movilidad	Rol responsable de infraestructura y transporte en el Centro de Fusión
D/OPS	Dirección Operacional	Rol responsable de coordinación operativa en el Centro de Fusión
ENL/INTL	Enlace Internacional	Rol de coordinación con entidades extranjeras
FIFA	Fédération Internationale de Football Association	Federación Internacional de Fútbol Asociación
FININT	Financial Intelligence	Inteligencia financiera; análisis de flujos de dinero para detectar actividades ilícitas
HUMINT	Human Intelligence	Inteligencia obtenida mediante fuentes humanas
I&W	Indicators and Warnings	Sistema de indicadores y alertas tempranas para anticipar amenazas
IMINT	Imagery Intelligence	Inteligencia obtenida mediante análisis de imágenes
LNO/PRIV	Liaison Officer / Private Sector	Oficial de enlace con sector privado
OSINT	Open-Source Intelligence	Inteligencia obtenida de fuentes abiertas (públicas)
P/I	Probability/Impact	Matriz de probabilidad e impacto para priorización de riesgos
RACI	Responsible, Accountable, Consulted, Informed	Matriz de asignación de responsabilidades
RPO	Recovery Point Objective	Objetivo de punto de recuperación; cantidad máxima de datos que se puede perder

Acrónimo	Significado	Descripción
RTO	Recovery Time Objective	Objetivo de tiempo de recuperación; tiempo máximo aceptable para restaurar servicios
SIGINT	Signals Intelligence	Inteligencia obtenida mediante intercepción de señales
SOC	Security Operations Center	Centro de operaciones de seguridad (ciberseguridad)
SRE	Secretaría de Relaciones Exteriores	Cancillería de México
TTPs	Tactics, Techniques and Procedures	Tácticas, técnicas y procedimientos operativos
TTX	Tabletop Exercise	Ejercicio de simulación de gabinete
UIF	Unidad de Inteligencia Financiera	Organismo mexicano de inteligencia financiera para prevención de lavado de dinero
VIP	Very Important Person	Persona de alta importancia que requiere protección especial

G.2 Términos técnicos de seguridad

Término	Definición
Actor solitario	Individuo que planea y ejecuta un ataque sin apoyo directo de una organización, aunque puede estar inspirado por ideología de grupos existentes
Blanco de oportunidad	Objetivo seleccionado por su accesibilidad y vulnerabilidad más que por su valor estratégico específico
Célula	Pequeño grupo organizado que opera con relativa autonomía dentro de una estructura mayor
Centro de Fusión	Instalación que integra información de múltiples agencias para análisis y coordinación de respuesta
Cobro de piso	Modalidad de extorsión en la que organizaciones criminales exigen pagos periódicos a negocios a cambio de “protección”
Crowd crush	Incidente de aplastamiento por multitud en el que la densidad de personas causa lesiones o muerte por compresión

Término	Definición
Crowd management	Conjunto de técnicas y procedimientos para gestionar de forma segura grandes concentraciones de personas
Depredación	Delitos de oportunidad en los que el agresor selecciona víctimas percibidas como vulnerables
Desinformación	Información falsa difundida deliberadamente con intención de engañar
Economía del evento	Conjunto de actividades económicas temporales generadas alrededor de un evento masivo
Escalamiento	Incremento progresivo en la intensidad o gravedad de una situación conflictiva
Evento de cola	Escenario de muy baja probabilidad, pero muy alto impacto, ubicado en los extremos de una distribución de riesgos
Fan Zone	Área designada para concentración de aficionados con pantallas para ver partidos y actividades relacionadas
Halconeo	Práctica de vigilancia criminal mediante observadores que reportan movimientos de autoridades o víctimas potenciales
Hooliganismo	Comportamiento violento asociado a grupos de aficionados al fútbol
Línea base	Nivel normal o promedio de actividad contra el cual se miden las variaciones
Modus operandi	Patrón característico de comportamiento de un actor criminal
Nodo crítico	Punto en una red de infraestructura cuya falla afectaría significativamente al sistema completo
Pánico masivo	Comportamiento colectivo de huida desordenada que puede causar lesiones independientemente de la amenaza real
Phishing	Técnica de fraude que busca obtener información sensible haciéndose pasar por entidad legítima
Ransomware	Software malicioso que cifra datos y exige pago para su recuperación
Secuestro exprés	Privación ilegal de la libertad de corta duración con fines de extorsión inmediata
Semáforo	Sistema de codificación por colores (verde/ámbar/rojo) para indicar niveles de alerta

Término	Definición
Spillover	Propagación de efectos de un incidente hacia sistemas o áreas no directamente afectadas
Superficie de ataque	Conjunto total de puntos vulnerables que pueden ser explotados por un atacante
Targeting	Selección deliberada de víctimas específicas basada en características identificables
Typosquatting	Registro de dominios web con errores tipográficos de sitios legítimos para fraude
Umbral	Nivel predefinido que, al ser alcanzado, activa una respuesta específica
Vocería única	Principio de comunicación de crisis que designa una sola fuente autorizada para declaraciones públicas
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza para causar daño

G.3 Organizaciones mencionadas

Sigla/Nombre	Descripción
CJNG	Cártel Jalisco Nueva Generación; organización criminal mexicana con presencia nacional
Europol	Agencia de la Unión Europea para la Cooperación Policial
FBI	Federal Bureau of Investigation; agencia federal de investigación de Estados Unidos
Interpol	Organización Internacional de Policía Criminal

Este análisis representa una evaluación prospectiva basada en OSINT y metodologías de análisis de inteligencia estratégica. Las proyecciones y escenarios presentados son hipotéticos y diseñados para facilitar el entendimiento de la problemática actual, no pretenden señalar de eventos específicos que ocurrirán con certeza.