



El Desafío de Seguridad en el Mundial de Fútbol 2026. (I) Lecciones Estratégicas para la Alta Dirección de Infraestructuras Críticas

La Copa Mundial de la FIFA 2026 marca un hito sin precedentes en la historia de la seguridad de eventos masivos e infraestructuras críticas. No se trata solo de la expansión a 48 selecciones, sino de un despliegue que abarca tres naciones, con México albergando sedes de alta complejidad operativa.

El Mundial de Fútbol de 2026 no es solo el evento deportivo más grande del planeta; para un Director de Seguridad o Responsable de Fuerzas Públicas o de Infraestructuras Críticas, representa el banco de pruebas definitivo en tiempo real de la resiliencia a gran escala, la gestión de macro-masas y la protección de servicios esenciales (transportes, energía, telecomunicaciones, sanidad) bajo máxima presión.



Para los Directores de Seguridad y CSOs del sector estratégico, este megaevento es el laboratorio de operaciones híbridas más complejo de la década. Analizar su arquitectura de protección nos ofrece una hoja de ruta fundamental para la resiliencia corporativa contemporánea.

Veamos esquemáticamente la realidad de nuestra percepción y repasar un decálogo básico sobre el Desafío de Seguridad en el Mundial 2026.



Geopolítica: Marco Estratégico del Operativo Mundial 2026

La seguridad de un evento transnacional comienza con el análisis del entorno macroestratégico.

La triada organizadora (México, Estados Unidos y Canadá) opera bajo vectores de riesgo asimétricos desde tensiones migratorias y fronteras, hasta ciberamenazas de actores estatales y el crimen organizado transnacional.

El diseño de este operativo demuestra que la seguridad ya no puede planificarse a nivel local; requiere un entendimiento profundo de la geopolítica mundial para prever cómo los conflictos internacionales pueden traducirse en amenazas de sabotaje o protestas extremistas en territorio nacional.



Inteligencia Estratégica, Prevención y Seguimiento Operativo

La fase reactiva ha muerto en la alta seguridad. El éxito en el Mundial 2026 descansa sobre un ciclo de inteligencia robusto.

La recopilación de datos en fuentes abiertas (OSINT), la inteligencia de señales (SIGINT) y la monitorización de la Dark Web permiten anticipar desde ciberataques a las redes de transporte hasta la llegada de grupos de aficionados radicales.

Los Directores y Jefes de Seguridad deben extraer una lección clave: la prevención es directamente proporcional a la calidad de la inteligencia compartida.



Gestión Integral de Riesgos y Amenazas durante 39 días de Operación

La continuidad operativa durante los 39 días de competición representa un maratón de desgaste sistémico.

La matriz de riesgos contempla vulnerabilidades y amenazas multidimensionales: ataques de denegación de servicio (DDoS) contra sistemas de billeteo, drones no autorizados sobrevolando zonas de exclusión, terrorismo, delincuencia organizada e incidencias de orden público.

El reto crítico aquí no es solo la gravedad de las amenazas, sino el factor fatiga. Mantener la tensión operativa, el estado de alerta de los recursos humanos, las plantillas y la redundancia de sistemas críticos durante más de un mes exige una planificación logística del recurso de seguridad que las corporaciones tradicionales suelen subestimar.



Recursos Humanos y Tecnologías de Control y Videovigilancia Inteligente

El equilibrio entre el factor humano y la automatización encuentra en este evento su máxima expresión. Las sedes en México se apoyan en ecosistemas tecnológicos de última generación:

- Cámaras con analítica inteligente de vídeo predictiva y reconocimiento facial para identificar perfiles de riesgo en los perímetros limítrofes (landside).
- Sistemas de control de acceso biométricos sin contacto (Contactless) e identidad digital, agilizando el flujo de masas sin perder trazabilidad.
- Sistemas Anti-Dron (C-UAS) para blindar el espacio aéreo de los estadios y áreas críticas.

Sin embargo, la tecnología queda ciega sin operadores altamente cualificados. El binomio tecnológico y de recursos humanos requiere personal entrenado en la interpretación de alertas tempranas para evitar la saturación por falsos positivos.



Modelos de Mando Unificado de Seguridad Público-Privada

Una de las mayores aportaciones metodológicas de este evento es la implementación de Centros de Mando Unificados (C4i / C5i) específicos, donde la frontera entre la seguridad pública y la privada se difumina de forma controlada.



Bajo un solo mando estratégico, las instituciones de la ley pública y las corporaciones privadas comparten frecuencias de comunicación, mapas de riesgos en tiempo real y planes y protocolos de actuación unificados.

Este modelo de gobernanza es el espejo donde deben mirarse las industrias estratégicas.



Planes de Seguridad Específicos por Sede y Partido

No existen soluciones universales. Un partido catalogado como «de alto riesgo» debido a rivalidades históricas o visitas de mandatarios VIP requiere un blindaje dinámico totalmente distinto a otro de fase de grupos estándar.

Del mismo modo, el Estadio Azteca en Ciudad de México, el Estadio BBVA en Monterrey o el Estadio Akron en Guadalajara presentan infraestructuras, vías de evacuación y entornos urbanos heterogéneos.

La lección para el gestor de infraestructuras es clara: el Plan de Seguridad del Operador (PSO) debe capilarizarse en Planes de Protección Específicos (PPE) que atiendan la micro-vulnerabilidad de cada activo.



Protocolos, Gestión de Crisis, Comunicación y Tiempos de Respuesta

Cuando un incidente supera las barreras de prevención, el tiempo se mide en vidas y reputación institucional.

Los manuales de gestión de crisis del Mundial 2026 están diseñados bajo la premisa de la resiliencia: contención inmediata y comunicación estratégica.

Un rumor mal gestionado en redes sociales puede provocar una estampida humana de consecuencias catastróficas.

Los comités de crisis operarán con portavoces designados y mensajes pre-aprobados para mitigar el pánico de forma simultánea a la intervención operativa sobre el terreno.



Gestión y Coordinación con Infraestructuras Sanitarias

La seguridad de la vida es la prioridad absoluta. Los planes operativos integran de forma simbiótica los dispositivos de seguridad con las redes hospitalarias y los servicios de emergencia médica (Triage masivo).

Esto incluye desde la previsión de corredores de emergencia sanitaria libres de tráfico en las ciudades sede, hasta protocolos específicos de descontaminación ante incidentes NBQR (Nuclear, Biológico, Químico o Radiológico).

La sanidad debe ser tratada, correctamente, como la infraestructura crítica de soporte vital del evento.



Formación y Capacitación Especializada: Simulacros y Operaciones

La excelencia no se improvisa. Meses antes del silbatazo inicial, los Directores de Seguridad, jefes de sector y personal de primera línea se someterán a programas de capacitación especializada de alto nivel.

La clave del éxito radica en los simulacros de mesa (Tabletop Exercises) y los ejercicios de fuerza viva a escala real.

Poner a prueba los sistemas mediante la simulación de escenarios concurrentes (por ejemplo, un apagón eléctrico simultáneo a un hackeo de las comunicaciones) es la única vía para garantizar que los protocolos se ejecuten de forma automática bajo condiciones de estrés extremo.



Regulación, Guías y Estándares Internacionales

El paraguas que dota de rigor científico e institucional a todo este despliegue son los estándares internacionales.

Desde las normativas específicas de la FIFA en materia de seguridad en los estadios, pasando por los estándares ISO 22301 (Continuidad de Negocio), ISO 31000 (Gestión de Riesgos) hasta las directrices de protección de infraestructuras críticas más exigentes del mundo.

El cumplimiento y la auditoría de estas guías garantizarán la homologación de los niveles de seguridad con independencia de la sede geográfica.

CONCLUSIÓN: la Herencia Metodológica del 2026

Para los profesionales que tenemos la responsabilidad de formar a los futuros líderes de la seguridad estratégica, el Mundial de Fútbol de 2026 constituye una clase magistral de Gobernanza Corporativa y Resiliencia Nacional.

La principal lección para la alta dirección es que la seguridad no es un compartimento estanco ni una póliza de seguros estática: es una disciplina viva, tecnológica, dependiente de la inteligencia y, sobre todo, profundamente integrada con el sector público y el tejido social.

Aquellas organizaciones que adopten estos niveles de rigor estratégico en sus propias operaciones corporativas serán las únicas preparadas para sobrevivir y liderar en el complejo entorno global actual.



Así, el Gobierno mexicano presentó el Plan Kukulcán -nombre que hace referencia a la deidad mesoamericana Kukulcán, que significa serpiente emplumada- que incluye el despliegue de 100.000 efectivos de Policía, Ejército y Seguridad Privada, aeronaves, Videovigilancia inteligente y sistemas antidrones para resguardar “de cualquier amenaza” estadios, hoteles, aeropuertos y zonas para aficionados y visitantes.



Las prioridades del Plan Kukulcán se centran en blindar por completo las tres ciudades sede (Ciudad de México, Guadalajara y Monterrey), mitigar amenazas transnacionales como el terrorismo y garantizar el orden público antes, durante y después del Mundial de Fútbol. Diseñado de la mano de la FIFA por el Gobierno de México, este megaoperativo estará respaldado por tecnología de inteligencia artificial y defensa aérea.

Manuel Sánchez Gómez-Merelo
Vocal de la Junta Directiva de AES