AES
FUNDACIÓN



Guía de Seguridad en Eventos de Masas

Índice

Presentación 4

Presentación institucional 5

1. Introducción y Justificación 7

2. Objetivos y Alcance de la Guía 8

   2.1 Objetivos 8

   2.2 Alcance 9

   2.3 Limitaciones del Alcance 11

3. Panorama Actual y Cifras Sectoriales 13

   3.1 Relevancia de los eventos y espectáculos en España 13

   3.2 Riesgos asociados a las concentraciones de masas 14

   3.3 Contexto normativo fragmentado 24

   3.4 Oportunidades para el desarrollo de un modelo español 25

4. Marco Normativo y Regulador 31

   4.1 Marco estatal 31

   4.2 Marco autonómico 32

   4.3 Normativa municipal y ordenanzas locales 33

   4.4 Referencias y marcos europeos 33

   4.5 Estándares y buenas prácticas internacionales 34

   4.6 Retos del marco normativo 35

5. Análisis de Riesgos en Eventos de Masas 37

   5.1 Metodologías de análisis de riesgos aplicables 37

   5.2 Tipología de amenazas en eventos de masas 41

   5.3 Factores agravantes en la gestión del riesgo 47

   5.4 Evaluación práctica de riesgos 47

   5.5 Recomendaciones para la gestión de riesgos 49

6. Planificación y Operativa de la Seguridad 50

   6.1 Plan de Autoprotección y Emergencias 50

   6.2 Organización de Equipos y Cadena de Mando 52

   6.3 Coordinación Interinstitucional 53

   6.4 Protocolos de Actuación Durante el Evento 54

   6.5 Recomendaciones prácticas para la operativa 55

Índice

7. Arquitectura Tecnológica y Sistemas Inteligentes de Seguridad 56

7.1 Capa operativa: digitalización de la respuesta y gestión de equipos 57

7.2 Capa de percepción: sistemas de captación e inteligencia de datos 63

7.3 Capa de inteligencia: unificación de datos en centros de control 75

7.4 Capa de integración: conectividad con la ciudad y el territorio 79

7.5 Recomendaciones para la adopción tecnológica 83

8. Recomendaciones finales, lecciones aprendidas y conclusiones 84

9. Glosario, normativa, bibliografía y contactos de referencia 87

9.1 Glosario de términos clave 87

9.2 Referencias normativas y bibliografía 88

9.3 Organismos y entidades de referencia 91

Guía de Seguridad en Eventos de Masas

Elaborada por el área de seguridad electrónica de AES y el Observatorio SEET impulsado por AES FUNDACIÓN

Nombre	Empresa	Papel en la elaboración de la guía
Alberto Terradas	HÖRMANN	Redactor
Alejandro Ferro	SECURITAS	Redactor
Alejandro García	OBSERVATORIO SEET	Coordinador/Redactor
Antonio Escamilla	AES FUNDACIÓN	Revisor
David Alonso	TELEFÓNICA	Redactor
David del Rey	SECURITAS	Coordinador/Redactor
Eva Plana	MOTOROLA	Redactora
Guilherme Ribeiro	ADVANCIS	Redactor
José Luis Andrés	VERISURE	Redactor
Juan José López	TRABLISA	Redactor
Juan Luis Alborg	SECURITAS	Redactor
Paloma Velasco	AES	Revisora
Ricardo Cañizares	AES FUNDACIÓN	Revisor
Roberto Frías	SECURITAS	Redactor

Presentación

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.



Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en Publicaciones AES Fundación así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **"dinamizando la seguridad ciudadana"**



Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

Presentación

La seguridad en eventos de masas constituye un desafío de especial complejidad para las administraciones públicas, los organizadores y promotores, los responsables de seguridad, los servicios de emergencia y los gestores de los espacios e infraestructuras donde se desarrollan. La elevada concentración de personas, la diversidad de escenarios y la evolución de las amenazas exigen superar los enfoques basados exclusivamente en medidas aisladas de vigilancia y control.

Festivales, conciertos, competiciones deportivas, celebraciones populares, actos institucionales y otros eventos celebrados en recintos o espacios públicos generan entornos temporales de alta exigencia. Su protección requiere actuar durante todo el ciclo de vida del evento, desde la planificación y el montaje hasta la celebración, evacuación, desmontaje y evaluación posterior, garantizando en cada fase la seguridad de las personas y la continuidad de las funciones esenciales.

En este contexto, AES Fundación y el Observatorio SEET – Seguridad en Eventos, Espectáculos y Turismo en Destinos impulsan la presente Guía de Seguridad en Eventos de Masas con el objetivo de proporcionar un marco técnico y operativo de referencia para la planificación, coordinación, gestión y evaluación de los dispositivos de seguridad aplicables a grandes concentraciones humanas.

La guía adopta una visión integral y multidisciplinar basada en:

- La identificación, análisis y tratamiento dinámico de los riesgos.
- La planificación operativa, la autoprotección y la continuidad del servicio.
- La coordinación entre seguridad pública, seguridad privada, servicios sanitarios y organización.
- La preparación previa apoyada en información e inteligencia operacional.
- La disponibilidad de comunicaciones fiables, redundantes e interoperables.
- La incorporación proporcionada de tecnologías inteligentes.
- La colaboración público-privada y la mejora continua a partir de la experiencia.

El documento no sustituye la normativa estatal, autonómica o local aplicable ni las competencias atribuidas a las autoridades y profesionales intervinientes. Su finalidad es complementar las obligaciones legales mediante criterios técnicos, metodologías, recomendaciones y buenas prácticas que faciliten una planificación más homogénea y mejoren la capacidad de anticipación, prevención, respuesta y recuperación ante incidentes.

La tecnología se aborda como una capacidad transversal al servicio del dispositivo operativo. La videovigilancia y la analítica avanzada, los sistemas de control de accesos y aforos, la sensorización, la geolocalización de recursos, las comunicaciones críticas, los drones, los sistemas de detección de aeronaves no tripuladas y las plataformas integradas de mando y control pueden mejorar la conciencia situacional y la toma de decisiones cuando responden a riesgos previamente identificados y se integran correctamente con las personas, los procedimientos y los centros de coordinación.

Desde el Observatorio SEET se promueve esta iniciativa con la vocación de disponer de un documento técnico de referencia, colaborativo y evolutivo, alineado con los principios de prevención, proporcionalidad, interoperabilidad, resiliencia y mejora continua. La guía se completa con un anexo tecnológico concebido como mapa sectorial de capacidades y criterios de aplicación, sin finalidad de homologación, certificación o recomendación comercial de soluciones concretas.



David del Rey
Coordinador del área de seguridad electrónica.



Alejandro García Martín
Embajador del Observatorio SEET.



INTRODUCCIÓN Y JUSTIFICACIÓN 1

Los eventos de masas constituyen una expresión relevante de la actividad social, cultural, deportiva, religiosa, institucional y económica. Conciertos, festivales, competiciones deportivas, ferias, celebraciones populares, procesiones, congresos y actos desarrollados en espacios públicos o recintos de gran capacidad reúnen cada año a millones de personas y generan un impacto significativo en las ciudades y destinos que los acogen.

La concentración temporal de personas, recursos e infraestructuras transforma estos eventos en entornos de elevada complejidad operativa. A los riesgos asociados al aforo, los accesos, la movilidad y la evacuación se suman amenazas de orden público, emergencias sanitarias, incendios, fenómenos meteorológicos adversos, fallos en suministros y comunicaciones, ciberincidentes, intrusiones aéreas y otras acciones deliberadas capaces de afectar a las personas, los bienes o la continuidad del evento.

La seguridad no puede limitarse al periodo de apertura al público. Debe planificarse desde las fases iniciales de diseño, autorización y montaje, mantenerse durante la celebración y la salida de los asistentes, y prolongarse durante el desmontaje y la evaluación posterior. Cada fase presenta riesgos y necesidades diferentes, por lo que requiere medidas específicas, responsables definidos y mecanismos adecuados de supervisión y coordinación.

España dispone de normativa estatal, autonómica, sectorial y municipal aplicable a distintos aspectos de los espectáculos públicos, la autoprotección, la protección civil, la seguridad ciudadana, la seguridad privada, la protección de datos y la ciberseguridad. No obstante, la diversidad de regulaciones, competencias, tipologías de eventos y procedimientos de autorización dificulta la aplicación de criterios técnicos homogéneos, especialmente en eventos temporales celebrados en espacios urbanos abiertos.

Esta realidad justifica la elaboración de un marco de referencia que facilite la interpretación coordinada de las distintas exigencias, promueva buenas prácticas y ayude a transformar el análisis de riesgos en un dispositivo operativo proporcionado, verificable y adaptable a la evolución del evento.

La presente guía se articula en torno a cuatro ejes:

- La gestión integral y dinámica de los riesgos durante todo el ciclo de vida del evento.
- La planificación operativa, la autoprotección y la continuidad de las capacidades esenciales.
- La coordinación efectiva entre organizadores, administraciones, Fuerzas y Cuerpos de Seguridad, seguridad privada, protección civil, servicios sanitarios y demás actores implicados.
- La aplicación proporcionada e interoperable de tecnologías que mejoren la obtención de información, la conciencia situacional, las comunicaciones y la respuesta.

La tecnología no se plantea como un fin en sí misma ni como sustitución del criterio profesional. Su aportación depende de que responda a necesidades previamente identificadas, se integre con los procedimientos y medios humanos y cumpla las exigencias de seguridad, fiabilidad, interoperabilidad, accesibilidad, protección de datos y ciberseguridad.

Con este enfoque, AES Fundación y el Observatorio SEET pretenden contribuir al desarrollo de eventos más seguros y resilientes, proporcionando a los profesionales y entidades implicadas una base común para planificar, coordinar, verificar y mejorar sus dispositivos de seguridad.

2 OBJETIVOS Y ALCANCE DE LA GUÍA

2.1 OBJETIVOS

La presente guía tiene como finalidad proporcionar un marco técnico y operativo de referencia, adaptado al contexto español, para la gestión integral de la seguridad en eventos de masas. Pretende facilitar que los distintos actores implicados compartan criterios de planificación, coordinación, intervención y evaluación, respetando en todo momento la normativa aplicable y las competencias atribuidas a cada organización.

Sus principales objetivos son:

1. Establecer una base común de referencia para las administraciones públicas, organizadores, promotores, responsables de seguridad, Fuerzas y Cuerpos de Seguridad, servicios de emergencia, empresas de seguridad y profesionales técnicos que intervienen en un evento de masas.
2. Favorecer la aplicación coordinada de criterios y metodologías de seguridad, autoprotección, protección civil y continuidad operativa ante la diversidad normativa, territorial y organizativa existente.
3. Promover un enfoque preventivo y basado en riesgos que permita identificar amenazas, vulnerabilidades, capacidades e interdependencias desde las primeras fases de planificación del evento.
4. Incorporar la información y la inteligencia operacional como apoyo a la evaluación de amenazas deliberadas, la anticipación de escenarios y la adaptación de los dispositivos de seguridad.
5. Facilitar que el análisis de riesgos se traduzca en medidas concretas, responsables definidos, procedimientos operativos, recursos dimensionados y mecanismos de verificación y seguimiento.
6. Reforzar la coordinación y la interoperabilidad entre seguridad pública, seguridad privada, protección civil, servicios sanitarios, organización y demás actores participantes, incluyendo la definición de cadenas de mando y planes de comunicaciones.
7. Orientar la selección e integración de tecnologías de seguridad conforme a criterios de necesidad, proporcionalidad, fiabilidad, interoperabilidad, accesibilidad, protección de datos, ciberseguridad y continuidad del servicio.
8. Impulsar la preparación, formación y validación práctica de los dispositivos mediante inspecciones previas, pruebas técnicas, ejercicios de comunicaciones y simulacros adaptados a los riesgos del evento.
9. Fomentar la evaluación posterior, la trazabilidad de las actuaciones y la incorporación de las lecciones aprendidas, contribuyendo al desarrollo de protocolos, recomendaciones, estándares sectoriales y posibles instrumentos normativos que favorezcan una mayor homogeneidad técnica.
10. Reforzar la confianza de asistentes, profesionales, organizadores y administraciones mediante dispositivos de seguridad eficaces, proporcionados, comprensibles y orientados a la protección de las personas.

2.2 ALCANCE

La guía es aplicable, con las adaptaciones necesarias en función del riesgo y de la normativa correspondiente, a eventos capaces de generar concentraciones significativas de personas, tanto en recintos permanentes como en instalaciones temporales, espacios abiertos, vías públicas o entornos urbanos complejos.

Su contenido puede utilizarse como referencia en conciertos, festivales, competiciones y espectáculos deportivos, ferias, congresos, celebraciones populares, actos religiosos, eventos institucionales, manifestaciones, carreras urbanas y otras actividades de pública concurrencia. La consideración de un evento como objeto de esta guía no depende exclusivamente de su aforo, sino también de factores como la configuración del espacio, la densidad prevista, el perfil de los asistentes, la duración, la movilidad asociada, las amenazas existentes, la complejidad organizativa y la capacidad de respuesta disponible.



2 OBJETIVOS Y ALCANCE DE LA GUÍA

Las recomendaciones abarcan el ciclo completo del evento:

- Diseño, planificación y tramitación administrativa.
- Evaluación de riesgos y preparación del dispositivo.
- Montaje de instalaciones e infraestructuras temporales.
- Inspecciones, pruebas y verificaciones previas.
- Accesos, celebración y permanencia del público.
- Respuesta ante incidentes y emergencias.
- Salida, evacuación o dispersión de los asistentes.
- Desmontaje y retirada de medios e instalaciones.
- Evaluación posterior e incorporación de lecciones aprendidas.

La guía se dirige principalmente a:

- Administraciones públicas estatales, autonómicas y locales, en el ejercicio de sus competencias de regulación, autorización, inspección, coordinación y protección de la seguridad pública.
- Organizadores, promotores y titulares de recintos, responsables de planificar el evento, dotarlo de los medios necesarios y garantizar el cumplimiento de las condiciones autorizadas.
- Directores y responsables de seguridad, encargados de convertir el análisis de riesgos en un dispositivo operativo coordinado y verificable.
- Empresas y profesionales de seguridad privada, responsables de las funciones y servicios que les atribuye la normativa vigente.
- Fuerzas y Cuerpos de Seguridad, en sus funciones de prevención, protección de la seguridad ciudadana, mantenimiento del orden público y coordinación de los dispositivos que correspondan.
- Servicios de protección civil, bomberos, asistencia sanitaria y emergencias, cuya integración resulta esencial para la prevención y respuesta ante situaciones críticas.
- Ingenierías, arquitecturas, consultoras, integradores tecnológicos y otros profesionales esponsables del diseño, implantación, validación y mantenimiento de infraestructuras y sistemas.
- Operadores de transporte, movilidad, telecomunicaciones, energía y otros servicios esenciales cuya actividad pueda condicionar la seguridad o continuidad del evento.
- Personal auxiliar, voluntariado y equipos de información y atención al público, dentro de las funciones que tengan asignadas.
- Asistentes y ciudadanía, como destinatarios de las medidas de protección y participantes necesarios en el cumplimiento de las instrucciones de seguridad y emergencia.

Las recomendaciones deberán aplicarse conforme a los principios de necesidad y proporcionalidad, adaptando los recursos, procedimientos y tecnologías a las características y riesgos concretos de cada evento. La guía no establece un dispositivo único ni determina medios mínimos universales, sino que proporciona criterios para justificar y diseñar la solución más adecuada en cada caso.

2.3 LIMITACIONES DEL ALCANCE

La presente guía tiene carácter técnico, orientativo y divulgativo. Sus contenidos no sustituyen la normativa aplicable, las disposiciones de las autoridades competentes ni los documentos, proyectos, planes o autorizaciones exigibles para la celebración de cada evento.

En particular, la guía no sustituye:

- El Plan de Autoprotección, Plan de Emergencia, Plan de Seguridad, Protocolo de Seguridad, Prevención y Control o cualquier otro documento obligatorio según la naturaleza, ubicación y características del evento.
- Los proyectos técnicos de instalaciones, estructuras temporales, protección contra incendios, electricidad, telecomunicaciones, accesibilidad, evacuación u otras infraestructuras sujetas a regulación específica.
- Los estudios, permisos, autorizaciones e informes sectoriales que deban emitir las administraciones, Fuerzas y Cuerpos de Seguridad, servicios de emergencia, autoridades aeronáuticas u otros organismos competentes.
- La evaluación de riesgos laborales y las obligaciones correspondientes en materia de seguridad y salud de los trabajadores.
- La planificación sanitaria específica, el dimensionamiento de los recursos asistenciales y los protocolos clínicos aplicables.
- Los planes de movilidad, tráfico, transporte, limpieza, medioambiente u otros servicios municipales, aunque la guía contempla su necesaria coordinación con el dispositivo de seguridad.
- El criterio profesional de los técnicos competentes, directores de seguridad, responsables de autoprotección, mandos de los servicios públicos y demás profesionales habilitados.

Las referencias a protección contra incendios, atención sanitaria, prevención de riesgos laborales, movilidad, operaciones con drones, protección de datos o ciberseguridad se incorporan únicamente en la medida necesaria para comprender su relación con la seguridad integral y la coordinación operativa del evento. Su desarrollo detallado deberá realizarse conforme a su normativa, planificación y documentación específicas.

Las tecnologías, prestaciones y casos de uso incluidos en la guía y en sus anexos tienen carácter orientativo. Su inclusión no implica que resulten necesarias o adecuadas para todos los eventos, ni constituye certificación, homologación, validación técnica o recomendación comercial por parte de AES Fundación o del Observatorio SEET.

La selección de medidas deberá justificarse mediante el correspondiente análisis de riesgos y atender a las características concretas del evento. La aplicación de esta guía no garantiza por sí sola la ausencia de incidentes ni exime a ninguna entidad o profesional de las responsabilidades que legalmente le correspondan.



3.1 RELEVANCIA DE LOS EVENTOS Y ESPECTÁCULOS EN ESPAÑA

España desarrolla cada año una intensa actividad cultural, musical, deportiva, ferial, religiosa y festiva que moviliza a millones de personas y genera un impacto relevante sobre la economía, el turismo, la movilidad y el funcionamiento de las ciudades.

La dimensión del sector puede apreciarse a través de algunos indicadores recientes:

- La música en vivo alcanzó en España durante 2025 una facturación por venta de entradas de 807,2 millones de euros, según el Anuario de la Música en Vivo 2026 de la Asociación de Promotores Musicales.
- El turismo de reuniones, congresos y eventos generó en 2023 un volumen de negocio estimado superior a 13.300 millones de euros, según los datos difundidos por la Federación Española de Municipios y Provincias y el Spain Convention Bureau.
- Las competiciones profesionales de fútbol de LALIGA EA SPORTS y LALIGA HYPERMOTION registraron más de 17,3 millones de asistentes durante la temporada 2024-2025.
- Celebraciones como la Semana Santa, las Fallas, los Sanfermines, los carnavales, las ferias y numerosas fiestas patronales concentran grandes volúmenes de población en espacios urbanos abiertos, frecuentemente durante varios días y con una elevada interacción entre asistentes, residentes, visitantes y servicios municipales.

Estas cifras pertenecen a actividades y periodos diferentes y no deben agregarse entre sí. Su finalidad es mostrar la magnitud y diversidad de un sector que comprende desde acontecimientos celebrados en instalaciones permanentes hasta eventos temporales, itinerantes o distribuidos por distintos espacios de una ciudad.

La relevancia de estos eventos no se limita a su aforo. Su desarrollo puede afectar simultáneamente a la movilidad, el transporte público, la asistencia sanitaria, las telecomunicaciones, el suministro energético, la actividad comercial, la convivencia ciudadana y el uso del espacio público. Además, las fases de montaje y desmontaje incorporan personal, vehículos, estructuras y materiales que también requieren medidas específicas de protección.

El crecimiento y la diversificación de los eventos incrementan la complejidad de su planificación. La seguridad debe responder no solo al número de asistentes, sino también a la densidad de ocupación, las características del emplazamiento, la duración, el perfil y comportamiento del público, la existencia de infraestructuras temporales, las condiciones meteorológicas, las amenazas deliberadas y la capacidad de coordinación y respuesta disponible.

Por ello, la importancia económica y social del sector debe ir acompañada de modelos de seguridad capaces de proteger a las personas, mantener los servicios esenciales y reducir el impacto de los incidentes sobre el evento y su entorno.

3.2 RIESGOS ASOCIADOS A LAS CONCENTRACIONES DE MASAS

Los eventos de masas pueden estar expuestos a amenazas de distinta naturaleza cuyos efectos se ven condicionados por el aforo, la densidad de ocupación, las características del espacio, las vulnerabilidades existentes y la capacidad de respuesta disponible. Entre las principales categorías deben considerarse:

- **Riesgos físicos** y asociados a la dinámica de multitudes, como caídas, atrapamientos, presiones, avalanchas, incendios o fallos estructurales.
- **Riesgos sociales y de orden público**, como altercados, vandalismo, conductas violentas o conflictos entre grupos.
- **Amenazas deliberadas**, incluidos terrorismo, sabotaje, intrusión, uso de vehículos hostiles o ataques mediante drones.
- **Riesgos tecnológicos y cibernéticos** que afecten al control de accesos, las comunicaciones, los sistemas de seguridad o los servicios esenciales.
- **Riesgos sanitario**s, derivados de emergencias médicas, temperaturas extremas, intoxicaciones o incidentes con múltiples afectados.
- **Fenómenos meteorológicos y ambientales** capaces de comprometer a los asistentes, las instalaciones temporales o la continuidad del evento.

Estas amenazas deben analizarse de forma conjunta, considerando sus posibles interdependencias y efectos en cascada.

3.2.1 AMENAZAS FÍSICAS

Descripción:

Las amenazas físicas comprenden aquellos sucesos capaces de producir lesiones, atrapamientos, aplastamientos, quemaduras u otros daños directos sobre las personas. Incluyen los incidentes derivados de la dinámica de las multitudes, los incendios, los fallos estructurales, la caída de elementos, los accidentes en instalaciones temporales y las deficiencias en los sistemas o recorridos de evacuación.

En los eventos de masas, un incidente inicialmente localizado puede propagarse con rapidez debido a la elevada densidad de ocupación, la existencia de cuellos de botella, la limitada percepción del riesgo por parte del público o la aparición de movimientos colectivos no previstos. Por ello, el análisis no debe limitarse a comprobar el aforo autorizado, sino que debe considerar la distribución y evolución de la ocupación, los flujos de entrada, salida y circulación interior, así como la capacidad efectiva de evacuación.

Casos reales:

Madrid Arena, España, 2012

Durante una fiesta celebrada en este recinto se produjo una situación crítica de presión y atrapamiento de personas que causó la muerte de cinco jóvenes. Las resoluciones judiciales identificaron distintas deficiencias relacionadas con la ocupación, la organización de los accesos, la utilización de los espacios interiores, los medios disponibles y la gestión de la emergencia. El caso evidenció que el aforo no puede tratarse únicamente como una cifra total, sino que debe controlarse la ocupación de cada zona, la interacción entre los flujos y la disponibilidad permanente de los recorridos de evacuación.

Discoteca Kiss, Brasil, 2013

El incendio de la discoteca Kiss, ocurrido en Santa Maria, causó 242 fallecidos y cientos de heridos. El fuego se inició durante una actuación en la que un elemento pirotécnico entró en contacto con material combustible situado en el techo. La rápida propagación del humo y de los gases tóxicos, junto con las dificultades de orientación y evacuación, multiplicó las consecuencias y puso de manifiesto la importancia de controlar los materiales, los efectos especiales y las condiciones reales de salida.

Lecciones aprendidas:

La prevención de las amenazas físicas exige controlar tanto el aforo total como la ocupación diferenciada de cada espacio, separar los flujos de entrada y salida, evitar concentraciones peligrosas y mantener libres, señalizadas, iluminadas y operativas todas las vías de evacuación. Las zonas de mayor densidad deben supervisarse desde el centro de control y disponer de procedimientos para detener los accesos, redistribuir al público y activar una respuesta temprana.

Antes de la apertura deben inspeccionarse las instalaciones temporales, los elementos estructurales, los materiales y revestimientos, los medios de extinción, el alumbrado de emergencia, la señalización y las barras antipánico. También deben autorizarse y controlarse expresamente la pirotecnia y los efectos especiales, considerando en los escenarios de emergencia la posible presencia de humo, gases tóxicos y pérdida de visibilidad.

Ambos casos demuestran que las consecuencias más graves suelen derivarse de la acumulación de fallos organizativos, técnicos y operativos. Una estructura clara de mando, personal suficiente y formado, comunicaciones operativas, videovigilancia supervisada, recursos sanitarios adecuadamente dimensionados, inspecciones previas y monitorización continua son esenciales para impedir que una incidencia evolucione hasta una emergencia colectiva.


17:22
DIRECTOR EMERGENCIAS
112

3.2.2 AMENAZAS SOCIALES Y DE ORDEN PÚBLICO

Descripción:

Las amenazas sociales y de orden público comprenden aquellas conductas o dinámicas colectivas capaces de alterar el desarrollo normal del evento, generar situaciones de violencia o dificultar la actuación de los servicios de seguridad y emergencia. Pueden incluir peleas, vandalismo, enfrentamientos entre grupos, invasiones de zonas restringidas, desórdenes asociados al consumo de alcohol o drogas y alteraciones vinculadas a rivalidades deportivas, conflictos sociales o acciones reivindicativas.

La celebración de una manifestación, concentración o protesta pacífica no constituye por sí misma una amenaza. El análisis debe centrarse en comportamientos, capacidades, antecedentes y circunstancias objetivas, evitando valoraciones basadas exclusivamente en la identidad, ideología o finalidad de los participantes.

La preparación debe incorporar información sobre convocatorias, grupos enfrentados, desplazamientos, puntos de fricción y acontecimientos coincidentes. También debe considerar que un ruido, una carrera, una pelea o un rumor pueden provocar reacciones colectivas desproporcionadas cuando existe alta densidad de público y escasa visibilidad sobre lo que sucede.

Casos reales:

Semana Santa de Sevilla, España, 2017

Durante la Madrugá del 14 de abril de 2017 se produjeron distintos incidentes en zonas del centro histórico de Sevilla que desencadenaron carreras, situaciones de pánico y movimientos desordenados entre el público. La investigación judicial analizó separadamente diferentes hechos y personas investigadas, sin que deba presentarse el episodio como una única acción coordinada.

El caso evidencia la rapidez con la que una alteración localizada puede propagarse por calles próximas mediante el movimiento de la multitud, los rumores y la percepción de una amenaza no confirmada. También muestra la dificultad de gestionar un evento distribuido, con itinerarios estrechos, elevada ocupación y múltiples organizaciones y servicios actuando simultáneamente

Cumbre del G20 en Hamburgo, Alemania, 2017

La cumbre del G20 estuvo acompañada por numerosas manifestaciones y por episodios graves de violencia, daños, incendios y alteraciones de la movilidad. La coexistencia de delegaciones internacionales, residentes, manifestantes pacíficos, grupos violentos y amplios dispositivos policiales generó un escenario urbano de gran complejidad.

El caso demuestra que la planificación debe extenderse más allá del recinto principal e incluir itinerarios, infraestructuras de transporte, espacios de concentración, actividades simultáneas y posibles desplazamientos de los incidentes hacia otras zonas.

Lecciones aprendidas:

La prevención de las amenazas sociales exige integrar la inteligencia previa y el seguimiento dinámico del entorno en la planificación y durante el desarrollo del evento. El análisis debe incorporar el comportamiento colectivo, diferenciar las concentraciones pacíficas de las conductas violentas e identificar cambios de actitud, movimientos inesperados o alteraciones que puedan anticipar una situación de riesgo.

Ante carreras, avalanchas o episodios de tensión, resulta esencial detectar y verificar rápidamente su origen para evitar respuestas desproporcionadas o decisiones basadas en información incompleta. La comunicación oficial, coordinada y accesible debe contrarrestar los rumores y proporcionar instrucciones claras al público, especialmente cuando la información falsa pueda provocar movimientos colectivos, enfrentamientos o situaciones de pánico.

El dispositivo debe mantener libres las rutas de emergencia y evacuación, disponer de recursos móviles y reservas operativas y asegurar la coordinación entre los diferentes niveles de mando y servicios intervinientes. La respuesta debe combinar prevención, comunicación, control proporcionado y capacidad de intervención, adaptándose a la evolución de la situación y evitando que una incidencia localizada se propague hasta comprometer la seguridad del conjunto del evento.

3.2.3 AMENAZAS DELIBERADAS

Descripción:

Las amenazas deliberadas comprenden acciones intencionadas dirigidas a causar daños, interrumpir el evento, generar temor o afectar a personas, bienes y servicios esenciales. Incluyen atentados terroristas, sabotajes, amenazas de bomba, ataques con armas o vehículos, intrusiones aéreas mediante drones y otras formas de violencia planificada.

A diferencia de los riesgos accidentales, estas amenazas pueden ser ejecutadas por adversarios que observan las medidas existentes, seleccionan objetivos vulnerables y adaptan su actuación. Su evaluación no debe apoyarse únicamente en antecedentes estadísticos, sino también en información e inteligencia sobre capacidades, intenciones, oportunidades y posibles objetivos.

Casos reales:

Atentados de Barcelona y Cambrils, España, 2017

Los atentados cometidos en Barcelona y Cambrils causaron 16 fallecidos y numerosos heridos. El ataque de Las Ramblas mostró la vulnerabilidad de los espacios urbanos abiertos y altamente concurridos frente al uso hostil de vehículos. Los hechos también evidenciaron la posibilidad de que distintos incidentes, localizaciones y actores formen parte de una misma amenaza.

Entre sus principales aprendizajes se encuentran la necesidad de identificar zonas expuestas a ataques con vehículos, establecer medidas de protección proporcionadas, relacionar incidentes aparentemente independientes y mantener una coordinación rápida entre servicios policiales, sanitarios y de emergencia

Manchester Arena, Reino Unido, 2017

Un atacante suicida detonó un explosivo en la zona de salida del Manchester Arena al finalizar un concierto, causando la muerte de 22 personas. La investigación oficial destacó deficiencias en la identificación de comportamientos sospechosos, el intercambio de información, la preparación y la coordinación de la respuesta.

El caso demuestra que la protección debe abarcar también las zonas de transición, espera y dispersión situadas fuera del espacio principal del espectáculo.

Lecciones aprendidas:

La prevención de las amenazas deliberadas exige aplicar inteligencia previa y mantener una vigilancia proporcionada durante todas las fases del evento. El análisis debe considerar la intención, capacidad y oportunidad de posibles actores hostiles, identificar cambios en el nivel de amenaza y adaptar las medidas de protección sin generar interferencias innecesarias en el desarrollo de la actividad.

Los accesos, salidas, perímetros y espacios de transición requieren una protección específica, al constituir puntos especialmente vulnerables por la concentración y el movimiento del público. Deben combinarse controles, videovigilancia, presencia operativa y detección temprana de comportamientos, objetos o vehículos sospechosos, manteniendo libres y disponibles las rutas de emergencia y evacuación.

El dispositivo debe establecer canales inmediatos de alerta y coordinación, definir procedimientos de actuación y preparar la respuesta ante incidentes con múltiples víctimas. La gestión debe integrar seguridad física, comunicaciones operativas e información pública coordinada, garantizando una estructura clara de mando y una intervención rápida que limite la propagación del daño, facilite la asistencia y evite que una acción localizada comprometa al conjunto del evento

3.2.4 *AMENAZAS TECNOLÓGICAS Y CIBERNÉTICAS*

Descripción:

Comprenden los ciberataques y los fallos de suministro eléctrico, comunicaciones, iluminación, megafonía, videovigilancia, control de accesos, ticketing o sistemas de información que puedan comprometer la seguridad, la coordinación y la continuidad operativa del evento.

Casos reales:

Mutua Madrid Open, España, 2025

El apagón eléctrico peninsular obligó a suspender la jornada del torneo, al quedar afectados el marcador electrónico, las cámaras, las comunicaciones y otros sistemas necesarios para su desarrollo.

Juegos Olímpicos y Paralímpicos de París, Francia, 2024

El dispositivo de ciberseguridad gestionó 548 eventos relacionados con entidades vinculadas a la organización, poniendo de manifiesto la exposición tecnológica de los grandes acontecimientos internacionales.

Lecciones aprendidas:

Los eventos deben disponer de sistemas redundantes, alimentación de emergencia, comunicaciones alternativas y procedimientos manuales de contingencia. También resulta esencial proteger las infraestructuras digitales, comprobar previamente los sistemas críticos y establecer protocolos que permitan mantener la información, la coordinación y la gestión segura del público ante una pérdida total o parcial de los servicios tecnológicos.



3.2.5 *RIESGOS SANITARIOS Y DE SALUD PÚBLICA*

Descripción:

Comprenden las emergencias médicas individuales o colectivas, las intoxicaciones alimentarias, el consumo de alcohol u otras sustancias, la propagación de enfermedades transmisibles y las deficiencias relacionadas con la higiene, el saneamiento o la disponibilidad de agua potable.

La concentración de personas, la duración del evento, el perfil de los asistentes y la existencia de actividades de restauración o alojamiento temporal pueden incrementar estos riesgos y favorecer su propagación. Su gestión requiere medidas preventivas, vigilancia sanitaria y epidemiológica, recursos asistenciales adecuadamente dimensionados y coordinación con los servicios de emergencias y salud pública.

Casos reales:

Festival Vino Somontano, Barbastro, España, 2025

Un brote de salmonelosis asociado a la muestra gastronómica del festival afectó a más de 400 personas y provocó varios ingresos hospitalarios. La investigación sanitaria vinculó el origen del brote a alimentos servidos en uno de los establecimientos participantes. El episodio puso de manifiesto la necesidad de controlar la trazabilidad, conservación, preparación y distribución de los alimentos, así como de disponer de mecanismos para identificar rápidamente a los afectados y retirar los productos sospechosos.

Peregrinación del Hajj, Arabia Saudí, 2000

La celebración estuvo asociada a un brote internacional de enfermedad meningocócica causada, principalmente, por el serogrupo W135. Se notificaron casos entre peregrinos, personas que regresaron a sus países y contactos próximos, lo que extendió sus efectos más allá del propio evento. El brote evidenció la capacidad de las grandes concentraciones internacionales para facilitar la transmisión y posterior dispersión geográfica de enfermedades infecciosas.

Lecciones aprendidas:

La planificación debe evaluar los riesgos derivados de la manipulación y venta de alimentos, el abastecimiento de agua, las instalaciones sanitarias, el alojamiento colectivo y los hábitos previsibles de consumo. Los operadores de restauración deben estar autorizados, disponer de personal formado y aplicar controles de higiene, conservación, temperatura, trazabilidad y gestión de alérgenos.

Los eventos con asistentes procedentes de diferentes territorios requieren coordinación con las autoridades de salud pública, evaluación epidemiológica previa y sistemas de vigilancia que permitan detectar agrupaciones de síntomas o incrementos anómalos de la demanda asistencial. Cuando proceda, deben establecerse recomendaciones de vacunación, medidas higiénicas y procedimientos de comunicación y seguimiento posteriores al evento.

El dispositivo debe contar con puestos asistenciales, personal sanitario, medios de evacuación y accesos reservados para ambulancias, considerando también los riesgos relacionados con el alcohol, las drogas y la atención a personas vulnerables. La detección temprana, el intercambio de información y una comunicación clara con el público son esenciales para impedir que varios casos individuales evolucionen hasta convertirse en una emergencia sanitaria colectiva.



3.2.6 *FENÓMENOS METEOROLÓGICOS Y AMBIENTALES*

Descripción:

Comprenden los episodios de viento intenso, tormentas, rayos, lluvias torrenciales, inundaciones, temperaturas extremas, nevadas, incendios forestales, mala calidad del aire y otros fenómenos capaces de afectar a las personas, las instalaciones y la continuidad del evento.

Estos fenómenos pueden evolucionar con rapidez y provocar caída de estructuras, interrupción de suministros, pérdida de comunicaciones, bloqueo de accesos o necesidad de evacuación. Su gestión requiere analizar la exposición y vulnerabilidad del emplazamiento, realizar un seguimiento continuo de las previsiones y establecer umbrales objetivos para modificar, suspender o cancelar la actividad.

Casos reales:

Medusa Festival, Cullera, España, 2022

Durante la madrugada se produjo un reventón térmico acompañado de fuertes rachas de viento que derribaron partes del escenario y de otras estructuras temporales. Una persona falleció y alrededor de cuarenta resultaron heridas. En el recinto se encontraban aproximadamente 50.000 asistentes. El evento fue evacuado y posteriormente cancelado. El caso evidenció la necesidad de relacionar las previsiones y alertas meteorológicas con la resistencia de las instalaciones y con decisiones operativas adoptadas con suficiente antelación.

Jamboree Scout Mundial, Corea del Sur, 2023

Más de 40.000 participantes se alojaron en un campamento afectado inicialmente por lluvias e inundaciones y, posteriormente, por una ola de calor que provocó cientos de asistencias. La aproximación del tifón Khanun obligó a evacuar preventivamente a aproximadamente 37.000 personas y trasladarlas a alojamientos alternativos. La sucesión de fenómenos mostró la importancia de evaluar conjuntamente el emplazamiento, las condiciones ambientales y la capacidad logística de reubicación.

Lecciones aprendidas:

La planificación debe partir del análisis histórico y estacional del emplazamiento, considerando su exposición al viento, inundaciones, temperaturas extremas, rayos, incendios forestales y contaminación. Las estructuras temporales, escenarios, cubiertas, cerramientos, torres, pantallas y elementos suspendidos deben calcularse, montarse e inspeccionarse para las condiciones previsibles, definiendo límites de utilización y procedimientos para su aseguramiento o desmontaje.

Durante el evento debe mantenerse una vigilancia meteorológica y ambiental continua mediante fuentes oficiales y, cuando resulte necesario, sensores desplegados en el recinto. El plan debe fijar niveles de prealerta, alerta y emergencia, así como umbrales objetivos para detener actividades, desalojar zonas expuestas, habilitar refugios, modificar horarios o suspender el evento. La autoridad responsable de adoptar estas decisiones debe estar claramente identificada.

También deben preverse rutas seguras, espacios de refugio, suministros de emergencia, comunicaciones alternativas y medios para informar al público de forma rápida y comprensible. La coordinación con protección civil, servicios meteorológicos, bomberos, emergencias sanitarias y autoridades territoriales resulta esencial para anticipar la evolución del fenómeno y evitar que una alerta conocida se transforme en una emergencia colectiva.

3.3 CONTEXTO NORMATIVO FRAGMENTADO

La seguridad en eventos de masas en España se desarrolla bajo un marco regulador complejo y multinivel, en el que concurren competencias estatales, autonómicas y municipales, además de disposiciones sectoriales aplicables según la actividad y el emplazamiento. Esta realidad genera diferencias en los procedimientos de autorización, las exigencias documentales, los criterios de aforo y las medidas de seguridad y autoprotección.

Aunque existe un marco estatal general en materia de protección civil y seguridad privada, su aplicación se completa con normativa autonómica, ordenanzas municipales y regulaciones sectoriales, lo que dificulta la adopción de criterios operativos homogéneos y la interoperabilidad entre los actores públicos y privados.

En términos generales, el contexto regulador puede resumirse en los siguientes ámbitos:

- **Espectáculos públicos y actividades recreativas:** regulados principalmente mediante normativa autonómica y ordenanzas municipales, con diferencias territoriales en materia de aforos, licencias, horarios, autoprotección y medidas de seguridad.
- **Eventos en espacios públicos:** autorizados mediante normativa sectorial, regulación del dominio público y condicionados técnicos establecidos por las administraciones competentes, sin una regulación estatal específica y unificada.
- **Espectáculos deportivos:** disponen de regulación estatal específica mediante la Ley 19/2007 y el Real Decreto 203/2010, que establecen obligaciones sobre prevención de la violencia y la intolerancia, condiciones de acceso y permanencia, coordinación policial y organización de la seguridad.
- **Marco europeo:** las disposiciones sobre resiliencia, ciberseguridad, infraestructuras críticas y protección de datos influyen en las organizaciones incluidas en sus ámbitos de aplicación, especialmente mediante las directivas NIS2 y CER.
- **Necesidad de criterios comunes:** la inexistencia de una norma técnica única para todas las tipologías de eventos refuerza la utilidad de guías, procedimientos coordinados y buenas prácticas compartidas entre administraciones, promotores, servicios de emergencia y seguridad privada.

3.4 OPORTUNIDADES PARA EL DESARROLLO DE UN MODELO ESPAÑOL

La evolución de las amenazas, la creciente complejidad operativa de los eventos y la transformación digital del sector ofrecen la oportunidad de impulsar en España un modelo avanzado de seguridad basado en la anticipación, la interoperabilidad, la profesionalización y la colaboración público-privada.

Este modelo debe superar una visión de la seguridad limitada al cumplimiento administrativo e incorporarla desde las primeras fases de diseño y planificación del evento. La combinación de análisis de riesgos, inteligencia previa, procedimientos operativos, personal cualificado y tecnologías adecuadamente integradas permite mejorar la prevención, la coordinación y la capacidad de respuesta.

Desde la perspectiva del Observatorio SEET, resulta necesario promover criterios técnicos comunes, metodologías adaptables a distintas tipologías de eventos y mecanismos estables de cooperación entre promotores, administraciones, fuerzas y cuerpos de seguridad, servicios de emergencias y seguridad privada. La innovación debe aplicarse de forma proporcionada, interoperable y respetuosa con la normativa, situando la protección de las personas como objetivo central.

3.4.1 SEGURIDAD INTELIGENTE: INCORPORACIÓN DE LA SEGURIDAD COMO PILAR ESTRATÉGICO JUNTO A LA SOSTENIBILIDAD, ACCESIBILIDAD E INNOVACIÓN.

Promotor del evento

- **Planificación estratégica:** Incorporar la seguridad desde el diseño permite anticipar riesgos, dimensionar adecuadamente los recursos y coordinarla con la accesibilidad, la sostenibilidad y la experiencia del público.
- **Valor añadido:** Un evento seguro y bien organizado mejora la confianza de asistentes, trabajadores, patrocinadores y administraciones, además de reducir interrupciones y costes derivados de incidentes.
- **Gestión integrada:** La combinación de procedimientos, personal cualificado y tecnologías proporcionadas facilita el seguimiento de aforos, flujos, incidencias y condiciones operativas.

Administración pública

- **Gobernanza coordinada:** Favorece la cooperación entre seguridad, emergencias, movilidad, sanidad, servicios urbanos y responsables de la autorización del evento.
- **Resiliencia territorial:** Permite anticipar el impacto sobre el espacio público, el transporte, las infraestructuras y los servicios esenciales, mejorando la preparación de la ciudad.
- **Evaluación y mejora:** La disponibilidad de información operativa facilita comprobar el cumplimiento de las condiciones autorizadas y evaluar posteriormente el dispositivo.

3 PANORAMA ACTUAL Y CIFRAS SECTORIALES

Seguridad privada

- **Profesionalización:** La incorporación de nuevas capacidades exige formación especializada, procedimientos claros y una adecuada asignación de funciones y responsabilidades.
- **Apoyo tecnológico:** La videovigilancia, la analítica de multitudes, los sensores, los drones o los sistemas de localización pueden reforzar la observación y la respuesta.
- **Interoperabilidad operativa:** La integración con el centro de control y los servicios públicos mejora el intercambio de información y la ejecución coordinada de las decisiones.

Seguridad pública

- **Prevención basada en información:** La inteligencia previa y el seguimiento dinámico permiten adaptar el dispositivo a la evolución de las amenazas y del entorno.
- **Respuesta coordinada:** Las alertas tempranas, los mapas operativos y las comunicaciones críticas facilitan la gestión conjunta de incidentes y emergencias.
- **Trazabilidad:** El registro de incidencias, comunicaciones y decisiones favorece la evaluación, la rendición de cuentas y la mejora continua.

Usuarios/asistentes

- **Experiencia segura y accesible:** Una adecuada gestión de accesos, recorridos, información y asistencia reduce esperas, incertidumbre y situaciones de riesgo.
- **Comunicación y participación:** Los canales accesibles permiten recibir instrucciones y alertas, solicitar ayuda o comunicar incidencias, preservando la privacidad.
- **Confianza:** La integración visible y proporcionada de la seguridad mejora la percepción del evento sin generar barreras innecesarias ni afectar a su carácter abierto e inclusivo.



3.4.2 *INNOVACIÓN TECNOLÓGICA: IA APLICADA A LA GESTIÓN DE MULTITUDES, ANALÍTICA PREDICTIVA, SISTEMAS DE EVACUACIÓN INTELIGENTE Y COMUNICACIONES CRÍTICAS EN TIEMPO REAL.*

Promotor del evento

- Optimización operativa: La analítica de datos permite anticipar variaciones de aforo y flujos, adaptar los recursos disponibles y detectar situaciones que requieran intervención.
- Continuidad del evento: Los sistemas de alerta, comunicaciones redundantes y procedimientos de contingencia reducen el impacto de fallos técnicos o incidencias operativas.
- Valor añadido: Una innovación orientada a necesidades reales mejora la seguridad, la experiencia del público y la confianza de patrocinadores, administraciones y asistentes.

Administración pública

- Gestión basada en datos: La integración de información sobre movilidad, ocupación, incidencias y servicios públicos mejora el conocimiento de la situación y apoya la toma de decisiones.
- Integración territorial: La conexión con plataformas y centros municipales permite gestionar conjuntamente el evento y sus efectos sobre el transporte, el espacio público y los servicios urbanos.
- Evaluación y trazabilidad: El registro de datos, alertas y actuaciones facilita el seguimiento del dispositivo y la evaluación posterior de sus resultados.

Seguridad privada

- Herramientas avanzadas: La videovigilancia con analítica, los mapas de densidad, los sensores, los drones y los sistemas integrados de gestión refuerzan la capacidad de observación.
- Eficacia operativa: La localización de recursos y las comunicaciones críticas permiten coordinar los equipos y responder con mayor rapidez ante una incidencia.
- Formación especializada: La utilización responsable de estas tecnologías requiere personal capacitado para interpretar alertas, verificar resultados y aplicar los procedimientos previstos.

Seguridad pública

- Detección temprana: La analítica avanzada puede identificar concentraciones, movimientos o comportamientos anómalos que deban ser comprobados por los operadores.
- Coordinación interinstitucional: Los sistemas compartidos de comunicación y visualización favorecen una respuesta conjunta y una imagen operativa común.
- Apoyo a la intervención: Los sensores, drones, plataformas geoespaciales y simuladores aportan información para planificar y ejecutar actuaciones, manteniendo la decisión bajo responsabilidad humana.

Usuarios/asistentes

- Información accesible: Las aplicaciones, paneles, sistemas de megafonía y canales móviles pueden ofrecer alertas, instrucciones y rutas alternativas en tiempo real.
- Solicitud de asistencia: Los canales habilitados permiten comunicar incidencias, necesidades médicas o situaciones de riesgo y facilitar su localización.
- Confianza y privacidad: La tecnología debe aplicarse de forma transparente, proporcionada, segura y respetuosa con la protección de datos y los derechos de las personas.

3.4.3 *COLABORACIÓN PÚBLICO-PRIVADA: CRECIENTE IMPLICACIÓN DE EMPRESAS DE SEGURIDAD, ORGANIZADORES DE EVENTOS Y ADMINISTRACIONES EN LA CONSTRUCCIÓN DE PROTOCOLOS COMUNES.*

Promotor del evento

- Acceso a capacidades especializadas: La colaboración con administraciones, servicios de emergencias y empresas de seguridad permite disponer de conocimiento técnico, personal cualificado, tecnología y apoyo logístico.
- Planificación coordinada: Los criterios y procedimientos previamente acordados facilitan la preparación de la documentación, las inspecciones y la coordinación del dispositivo.
- Cumplimiento y responsabilidad: La definición de funciones, requisitos y mecanismos de control reduce incertidumbres y favorece el cumplimiento de las obligaciones del organizador.
- Confianza institucional: La participación activa en estructuras de cooperación refuerza la imagen del promotor como entidad responsable y comprometida con la seguridad.

Administración pública

- Aprovechamiento de capacidades: La colaboración permite integrar los recursos privados disponibles en la planificación general, respetando las competencias y responsabilidades de cada actor.
- Criterios comunes: La experiencia compartida facilita la elaboración de guías, protocolos y requisitos técnicos aplicables a diferentes tipologías de eventos.
- Innovación responsable: Las empresas pueden aportar soluciones y conocimientos especializados cuya utilidad, interoperabilidad y adecuación normativa deben evaluarse previamente.
- Mejora continua: El intercambio de información y la evaluación conjunta de los dispositivos favorecen el aprendizaje institucional y la adopción de medidas correctoras.

Seguridad privada

- Integración operativa: La participación desde las fases iniciales permite conocer los riesgos, procedimientos, canales de comunicación y funciones asignadas dentro del dispositivo.
- Formación compartida: Los ejercicios y actividades conjuntas mejoran la preparación, homogeneizan criterios de actuación y refuerzan el conocimiento mutuo.
- Interoperabilidad: Los protocolos y comunicaciones previamente definidos facilitan la coordinación con las fuerzas y cuerpos de seguridad y los servicios de emergencias.
- Especialización profesional: La colaboración impulsa nuevas competencias relacionadas con inteligencia, tecnología, gestión de multitudes y respuesta ante emergencias.

Seguridad pública

- Conocimiento anticipado: El intercambio proporcionado de información permite mejorar la evaluación de amenazas y adaptar el despliegue a la evolución del riesgo.
- Coordinación táctica: La definición de mandos, enlaces, canales y procedimientos reduce errores y facilita una respuesta conjunta ante los incidentes.
- Complementariedad de funciones: La seguridad privada puede desarrollar las tareas legalmente atribuidas, permitiendo concentrar los recursos públicos en las funciones que les corresponden.
- Visión operativa común: Compartir información relevante y verificada mejora la conciencia situacional y la capacidad de adoptar decisiones coordinadas.

Usuarios/asistentes

- Protección integral: La coordinación entre los actores mejora la cobertura preventiva y la capacidad de atención ante incidencias y emergencias.
- Información coherente: Los protocolos comunes permiten transmitir avisos e instrucciones claros, accesibles y consistentes por los distintos canales disponibles.
- Respuesta eficaz: La comunicación directa entre equipos reduce los tiempos de detección, movilización y asistencia.
- Mayor confianza: La existencia de una estructura coordinada y preparada mejora la percepción de seguridad y la experiencia general del público.

4 MARCO NORMATIVO Y REGULADOR



La seguridad de los eventos de masas se encuentra sometida a un marco regulador complejo y multinivel, en el que confluyen competencias estatales, autonómicas y municipales, junto con normativa sectorial sobre protección civil, seguridad privada, espectáculos públicos, eventos deportivos, sanidad, ciberseguridad, protección de datos e infraestructuras críticas.

La diversidad normativa y competencial plantea retos operativos para promotores, organizadores, ingenierías, directores de seguridad, empresas prestadoras de servicios y administraciones públicas. Estos retos adquieren especial relevancia en eventos celebrados en espacios públicos y entornos urbanos abiertos, donde intervienen diferentes organismos y deben coordinarse la seguridad, las emergencias, la movilidad y los servicios municipales.

La presente guía no sustituye las normas aplicables ni los requisitos establecidos por las autoridades competentes. Su finalidad es proporcionar un marco técnico de referencia que facilite la interpretación coordinada de las obligaciones, la adopción de criterios operativos comunes, la interoperabilidad entre los actores y la incorporación de buenas prácticas de prevención, resiliencia y seguridad integral.

4.1 MARCO ESTATAL



En España no existe una ley estatal única que regule integralmente la seguridad de todos los eventos de masas. No obstante, distintas normas establecen obligaciones aplicables según la naturaleza del evento, el espacio utilizado, los servicios contratados y los riesgos existentes:

- Ley 17/2015, del Sistema Nacional de Protección Civil, que establece el marco general de prevención, planificación, respuesta, recuperación y coordinación ante emergencias.
- Real Decreto 524/2023, por el que se aprueba la Norma Básica de Protección Civil y se establecen criterios comunes para la identificación de riesgos y la integración de los distintos instrumentos de planificación.
- Real Decreto 393/2007, Norma Básica de Autoprotección, formalmente derogado, pero aplicable transitoriamente hasta la aprobación del nuevo instrumento de planificación que lo sustituya. Establece, entre otros supuestos, obligaciones para determinados recintos, instalaciones desmontables y actividades al aire libre en función de su capacidad o aforo.
- Ley 5/2014, de Seguridad Privada, que regula la participación de empresas, departamentos y personal de seguridad privada, así como su colaboración con las fuerzas y cuerpos de seguridad.
- Ley 19/2007 y Real Decreto 203/2010, aplicables a competiciones y espectáculos deportivos. Configuran un modelo basado en el control de accesos y permanencia, los medios técnicos y la videovigilancia, la Unidad de Control Organizativo, el coordinador de seguridad y los protocolos de prevención y control. Este marco ha servido de base al modelo aplicado en el fútbol profesional.
- Ley 8/2011, de protección de las infraestructuras críticas, cuando el evento afecte a operadores o infraestructuras incluidos en su ámbito de aplicación.

Estas disposiciones se complementan con normativa sobre seguridad ciudadana, protección de datos, prevención de incendios, edificación, instalaciones temporales, sanidad, tráfico y transporte.

4.2 MARCO AUTONÓMICO



Las comunidades autónomas disponen de competencias en materia de espectáculos públicos, aLey 17/2015, del Sistema Nacional de Protección Civil, que establece el marco general de prevención, planificación, respuesta, recuperación y coordinación ante emergencias.

- Real Decreto 524/2023, por el que se aprueba la Norma Básica de Protección Civil y se establecen criterios comunes para la identificación de riesgos y la integración de los distintos instrumentos de planificación.
- Real Decreto 393/2007, Norma Básica de Autoprotección, formalmente derogado, pero aplicable transitoriamente hasta la aprobación del nuevo instrumento de planificación que lo sustituya. Establece, entre otros supuestos, obligaciones para determinados recintos, instalaciones desmontables y actividades al aire libre en función de su capacidad o aforo.
- Ley 5/2014, de Seguridad Privada, que regula la participación de empresas, departamentos y personal de seguridad privada, así como su colaboración con las fuerzas y cuerpos de seguridad.
- Ley 19/2007 y Real Decreto 203/2010, aplicables a competiciones y espectáculos deportivos. Configuran un modelo basado en el control de accesos y permanencia, los medios técnicos y la videovigilancia, la Unidad de Control Organizativo, el coordinador de seguridad y los protocolos de prevención y control. Este marco ha servido de base al modelo aplicado en el fútbol profesional.
- Ley 8/2011, de protección de las infraestructuras críticas, cuando el evento afecte a operadores o infraestructuras incluidos en su ámbito de aplicación.

Estas disposiciones se complementan con normativa sobre seguridad ciudadana, protección de datos, prevención de incendios, edificación, instalaciones temporales, sanidad, tráfico y transporte.ctividades recreativas, emergencias y protección civil. Sus leyes y reglamentos determinan los requisitos aplicables a los establecimientos, recintos y eventos celebrados en cada territorio, generando diferencias en aspectos como:

- Clasificación de espectáculos y actividades.
- Condiciones de admisión, acceso y permanencia.
- Límites y control de aforos.
- Seguros y responsabilidades.
- Planes de autoprotección y dispositivos sanitarios.
- Horarios, inspección y régimen sancionador.
- Condiciones de seguridad de recintos e instalaciones temporales.

Entre las normas autonómicas de referencia se encuentran la Ley 11/2009 de Cataluña, la Ley 13/1999 de Andalucía y la Ley 14/2010 de la Comunitat Valenciana, junto con sus respectivos desarrollos reglamentarios.

Los organizadores deben identificar la normativa vigente en el territorio y los requisitos concretos establecidos por la autoridad competente. Esta diversidad refuerza la utilidad de disponer de criterios técnicos y buenas prácticas comunes que puedan adaptarse a cada marco autonómico.

4.3 NORMATIVA MUNICIPAL Y ORDENANZAS LOCALES



Los ayuntamientos ejercen competencias esenciales en la autorización y supervisión de eventos celebrados en establecimientos municipales, espacios públicos y vías urbanas. Entre sus principales instrumentos se encuentran:

- Autorizaciones para la celebración del evento y la ocupación del dominio público.
- Ordenanzas sobre convivencia, ruido, movilidad, accesibilidad, limpieza y uso de espacios públicos.
- Licencias o controles relativos a instalaciones, estructuras temporales y actividades.
- Condicionados técnicos sobre seguridad, emergencias, asistencia sanitaria y protección contra incendios.
- Protocolos de coordinación con policía local, bomberos, protección civil, movilidad y servicios sanitarios.

Los requisitos deben establecerse atendiendo a la normativa estatal y autonómica, las características del emplazamiento y el análisis específico de riesgos. Su definición anticipada y coordinada reduce incertidumbres, evita exigencias contradictorias y facilita la integración del evento en los servicios y planes municipales.

4.4 REFERENCIAS Y MARCOS EUROPEOS



La planificación y utilización de tecnologías en eventos de masas debe considerar también la normativa de la Unión Europea, especialmente:

- Reglamento General de Protección de Datos y normativa nacional complementaria, aplicables al tratamiento de datos mediante videovigilancia, aplicaciones, sistemas de acreditación, localización o control de accesos.

- Reglamento Europeo de Inteligencia Artificial, que establece obligaciones según el riesgo y limita determinados usos, especialmente los relacionados con identificación biométrica y vigilancia en espacios de acceso público.
- Directiva NIS2, sobre un nivel común elevado de ciberseguridad, cuando los operadores, proveedores tecnológicos o infraestructuras implicados estén incluidos en su ámbito de aplicación.
- Directiva CER, sobre resiliencia de las entidades críticas, cuando el evento dependa de servicios esenciales o afecte a entidades formalmente identificadas como críticas.
- Reglamentación europea sobre aeronaves no tripuladas, aplicable a la utilización de drones en funciones de vigilancia, supervisión o apoyo a emergencias.

Estas disposiciones no se aplican automáticamente a todos los eventos. Su incidencia debe evaluarse según la entidad responsable, la tecnología utilizada, el tratamiento de datos realizado y las infraestructuras o servicios afectados.

4.5 ESTÁNDARES Y BUENAS PRÁCTICAS INTERNACIONALES



Además de la normativa obligatoria, existen estándares y documentos técnicos que pueden utilizarse como referencia para diseñar, implantar y evaluar los dispositivos de seguridad:

- ISO 31000:2018, sobre principios y procesos generales de gestión del riesgo.
- ISO 22301:2019, sobre sistemas de gestión de continuidad de negocio y mantenimiento de las funciones críticas ante interrupciones.
- ISO 22320:2018, sobre gestión de incidentes, estructuras de mando, responsabilidades, coordinación y gestión de recursos.
- ISO 22315:2014, relativa a la planificación de evacuaciones masivas, e ISO 22379:2022, sobre organización de grandes eventos urbanos o regionales.
- ISO 22343-1 e ISO 22343-2:2023, sobre ensayo, clasificación y aplicación de barreras de seguridad frente a vehículos, como referencia actualizada frente a las anteriores PAS 68 y PAS 69.
- NFPA 101, Life Safety Code, como referencia internacional sobre protección de ocupantes, evacuación y seguridad contra incendios.
- Reglamentos y guías de UEFA y FIFA, especialmente relevantes para la seguridad, organización y operación de estadios y acontecimientos deportivos.
- Orientaciones de la Organización Mundial de la Salud, aplicables a la evaluación y gestión de riesgos sanitarios en concentraciones multitudinarias.

Estos documentos son de aplicaciía del evento y utilizarse como complemento, nunca como sustitución de la legislación vigente.ón voluntaria salvo que una norma, autorización, contrato o pliego los haga exigibles. Su selección debe justificarse según la tipolog

4.6 RETOS DEL MARCO NORMATIVO

El marco regulador aplicable a la seguridad de los eventos de masas presenta importantes desafíos derivados de la distribución territorial de competencias, la diversidad de tipologías de eventos, la evolución de las amenazas y la incorporación progresiva de nuevas tecnologías.

La coexistencia de normativa estatal, autonómica y municipal genera diferencias en los procedimientos de autorización, supervisión y exigencia técnica. Estas diferencias resultan especialmente relevantes en eventos celebrados en espacios públicos y entornos urbanos abiertos, donde deben coordinarse seguridad, emergencias, movilidad, sanidad, servicios urbanos y protección del entorno.

Entre los principales retos identificados destacan:

- Fragmentación normativa territorial: La diversidad de leyes autonómicas, reglamentos y ordenanzas municipales produce diferencias en materia de aforos, autoprotección, dispositivos sanitarios, seguridad privada, inspección y autorización.
- Ausencia de un marco técnico integral: Aunque existen normas estatales generales y regulaciones sectoriales, no se dispone de criterios técnicos unificados aplicables a la seguridad integral de todas las tipologías de eventos de masas.
- Coordinación competencial y operativa: La intervención de distintas administraciones, fuerzas y cuerpos de seguridad, servicios de emergencias y operadores privados exige delimitar responsabilidades, establecer estructuras de mando y compartir información relevante.
- Adaptación a riesgos emergentes: La transformación de las amenazas obliga a incorporar la ciberseguridad, la protección frente a acciones deliberadas, los fenómenos meteorológicos extremos, la salud pública y la continuidad de los servicios esenciales.
- Regulación de nuevas tecnologías: La utilización de inteligencia artificial, biometría, drones, aplicaciones móviles, sistemas de localización y analítica de vídeo requiere compatibilizar su utilidad operativa con la protección de datos, la ciberseguridad y los derechos fundamentales.
- Actualización e implantación efectiva: Los planes y protocolos deben revisarse periódicamente, someterse a ejercicios y coordinarse con los recursos realmente disponibles, evitando que el cumplimiento quede limitado a la elaboración documental.
- Desarrollo de buenas prácticas comunes: AES Fundación y el Observatorio SEET pueden contribuir a promover guías técnicas, recomendaciones y modelos de referencia que faciliten la homogeneización de criterios, respetando las competencias y particularidades de cada territorio.

La superación de estos retos requiere cooperación estable entre las administraciones públicas, los promotores, las ingenierías, los servicios de emergencias y la seguridad privada, junto con mecanismos de evaluación que permitan incorporar las lecciones aprendidas después de cada evento.

5 ANÁLISIS DE RIESGOS EN EVENTOS DE MASAS



La identificación y evaluación de riesgos constituye el núcleo técnico de cualquier estrategia de seguridad aplicada a eventos de masas. La complejidad creciente de las concentraciones humanas, unida a la evolución de amenazas híbridas y entornos altamente digitalizados, obliga a adoptar metodologías multidisciplinares capaces de integrar variables físicas, sociales, tecnológicas y operativas.

El análisis de riesgos en eventos multitudinarios no debe entenderse únicamente como una obligación documental vinculada al cumplimiento normativo, sino como una herramienta de toma de decisiones estratégicas que condiciona el diseño del dispositivo de seguridad, la asignación de recursos y la capacidad de respuesta ante incidentes críticos.

Desde la perspectiva del Observatorio SEET, el análisis de riesgos debe evolucionar hacia un modelo dinámico y orientado a la inteligencia, que combine información procedente de fuentes abiertas, actores públicos y privados, observación operativa y antecedentes del evento. Esta información debe complementarse con simulación de escenarios y sistemas de monitorización que permitan revisar la evaluación y adaptar las medidas durante su desarrollo.

A continuación, se indican algunas de las estratégicas de identificación y mitigación de riesgos en eventos de masas:

- Mapeo de público y evacuación: simulaciones de flujo para dimensionar personal necesario.
- Control de accesos: sistemas de revisión y rutas de evacuación claramente señalizadas.
- Evaluación de infraestructuras temporales: cumplimiento normativo, resistencia estructural y seguridad eléctrica.
- Factores externos: condiciones meteorológicas, riesgos sociales o políticos.
- Preparación y capacitación: equipos entrenados en primeros auxilios, gestión de multitudes y respuesta ante crisis.

Enfoques Innovadores y Tecnológicos

- Análisis predictivo con IA: pronostica incidentes potenciales a partir de datos históricos y redes sociales.
- Simulaciones en tiempo real: modelado de movimientos de multitudes para anticipar congestiones.
- IoT y sensores ambientales: monitoreo de condiciones físicas y alertas inmediatas.
- Software de gestión de riesgos: integra mapas de riesgos, trazabilidad de controles y reportes dinámicos.

Normativa y Buenas Prácticas

- Adaptar las metodologías: basadas en estándares como la ISO 31000 para gestión integral de riesgos.
- Involucrar a autoridades locales y servicios de emergencia: policía, bomberos y protección civil.
- Revisar y actualizar planes periódicamente, integrando lecciones aprendidas de eventos anteriores.

5.1 METODOLOGÍAS DE ANÁLISIS DE RIESGOS APLICABLES

La evaluación puede combinar metodologías como ISO 31000, Mosler, Cuantitativo Mixto, Gretener, MAGERIT, SEPTRI o CARVER, seleccionadas según la naturaleza de los riesgos analizados. Estas herramientas deben complementarse con inteligencia previa, conocimiento experto, simulación de escenarios, monitorización y una planificación operativa adecuada.

Ningún método garantiza por sí solo la seguridad del evento. Su aplicación permite comparar escenarios, identificar vulnerabilidades, priorizar medidas y fundamentar la asignación de recursos, manteniendo la evaluación actualizada conforme evoluciona la amenaza, la exposición y el contexto operativo.

ISO 31000 DE GESTIÓN DEL RIESGO:

La ISO 31000 ofrece un enfoque integral para gestionar el riesgo en cualquier tipo de empresa, proporcionando principios, una estructura de apoyo y un proceso claro que permite anticiparse a la incertidumbre, reducir amenazas y aprovechar oportunidades. Este marco facilita la toma de decisiones informadas, promueve la mejora continua, la resiliencia empresarial y la integración del riesgo en todos los niveles estratégicos y operativos.

La norma ISO 31000 está dirigida a cualquier organización, pública o privada, independientemente de su tamaño, sector o nivel de madurez en la gestión de riesgos. Su enfoque flexible y adaptable la convierte en una herramienta útil tanto para grandes corporaciones como para pequeñas y medianas empresas, entidades gubernamentales, organizaciones sin ánimo de lucro e incluso proyectos individuales que requieran una gestión estructurada del riesgo.

METODOLOGÍA MOSLER:

La **metodología Mosler**, también conocida como **Penta**, es un método **secuencial y estructurado** para la identificación, análisis y evaluación de riesgos basado en la ISO 3100. Se caracteriza por su enfoque cuantitativo basado en criterios ponderados de manera numérica, lo que permite **calcular tanto la probabilidad como el impacto** de los riesgos en distintos tipos de activos (personas, infraestructura, información, recursos financieros, etc.).

Características principales de la Metodología:

1. Secuencialidad de fases (definición, análisis, evaluación y clasificación del riesgo), asegurando la coherencia entre cada etapa.
2. Criterios Penta (F, S, P, E, A, V):
   - Función (F): impacto en la actividad.
   - Sustitución (S): facilidad de reemplazo del bien afectado.
   - Profundidad (P): perturbación psicológica y reputacional.
   - Extensión (E): alcance geográfico/lógico del daño.
   - Agresión (A): probabilidad de manifestación.
   - Vulnerabilidad (V): susceptibilidad al daño si ocurre el riesgo.
3. Evaluación cuantitativa: se calcula el Carácter del Riesgo C, la Probabilidad Pb y el Riesgo Estimado ER = C \times Pb.
4. Clasificación objetiva: riesgos categorizados desde Muy Bajo hasta Elevado, lo que facilita la priorización de medidas preventivas o correctivas.
5. Flexibilidad: aplicable a riesgos naturales, tecnológicos y antisociales.

METODOLOGÍA CARVER APLICADA A AMENAZAS DELIBERADAS

CARVER es una metodología de análisis y priorización de objetivos y vulnerabilidades especialmente útil frente a amenazas deliberadas, en las que la probabilidad histórica puede resultar insuficiente. Evalúa la criticidad del elemento, su accesibilidad, la posibilidad de recuperación, su vulnerabilidad, los efectos previsibles y su facilidad de reconocimiento.

En eventos de masas permite analizar accesos, zonas de concentración, centros de control, suministros, comunicaciones y otros activos susceptibles de una acción intencionada. Su aplicación debe complementarse con la valoración de la capacidad, intención o motivación y oportunidad del posible adversario, utilizando información contrastada y revisando el análisis conforme evolucione la amenaza.

CARVER no sustituye a la evaluación general de riesgos, sino que aporta una perspectiva específica para priorizar medidas de protección frente a terrorismo, sabotaje, activismo violento u otras acciones deliberadas.

COMPARATIVA METODOLOGÍAS SIMILARES

Las metodologías presentan alcances diferentes y deben seleccionarse atendiendo a la naturaleza de los riesgos, los activos afectados y la finalidad del análisis. Algunas ofrecen una evaluación general, mientras que otras se orientan específicamente a incendios, seguridad alimentaria, sistemas de información o amenazas deliberadas.



Metodología	Enfoque	Factores principales	Aplicación en eventos	Ventajas y limitaciones
ISO 31000	Marco general cualitativo o cuantitativo	Contexto, identificación, análisis, evaluación, tratamiento y seguimiento	Gestión integral de todas las categorías de riesgo	Flexible y transversal; no proporciona por sí misma una fórmula concreta de cálculo
Mosler	Semicuantitativo y secuencial	Función, sustitución, profundidad, extensión, agresión y vulnerabilidad	Riesgos patrimoniales, operativos, tecnológicos y antisociales	Facilita la comparación y priorización; depende del criterio experto al puntuar
Cuantitativo Mixto	Cuantitativo con ponderaciones	Probabilidad, impacto, exposición y valoración económica	Comparación de riesgos operativos y económicos	Permite priorizar inversiones; puede simplificar factores humanos o reputacionales
William T. Fine	Semicuantitativo	Consecuencia, exposición y probabilidad	Riesgos de seguridad y accidentes asociados a actividades e instalaciones	Facilita priorizar y justificar medidas correctoras; requiere escalas correctamente calibradas
HACCP o APPCC	Preventivo y basado en puntos críticos de control	Peligros alimentarios, límites críticos, vigilancia y acciones correctoras	Restauración, catering, almacenamiento y distribución de alimentos	Muy útil para seguridad alimentaria; no constituye un método general para todos los riesgos del evento
Gretener	Semicuantitativo y específico de incendios	Peligro potencial, medidas de protección y riesgo de incendio aceptado	Evaluación complementaria de edificios y determinados recintos	Permite valorar medidas contra incendios; su aplicación es limitada fuera de este ámbito
MAGERIT	Cualitativo y cuantitativo basado en activos	Activos, amenazas, vulnerabilidades, impactos y salvaguardas	Sistemas de información, comunicaciones, instalaciones y servicios tecnológicos	Estructurada y detallada; requiere inventario de activos y conocimientos especializados
SEPTRI	Evaluación y propuesta de tratamiento	Riesgos, factores de protección y medidas de seguridad	Seguridad patrimonial y organizativa	Orientada al tratamiento del riesgo; su aplicación exige criterios homogéneos y experiencia
CARVER	Priorización de objetivos y vulnerabilidades	Criticidad, accesibilidad, recuperabilidad, vulnerabilidad, efectos y reconocimiento	Terrorismo, sabotaje, activismo violento y otras amenazas deliberadas	Aporta la perspectiva del adversario; debe apoyarse en inteligencia actualizada
DOFA adaptada	Cualitativo y estratégico	Debilidades, amenazas, fortalezas y oportunidades	Diagnóstico inicial del evento y de su organización	Sencilla y participativa; no permite cuantificar ni priorizar el riesgo por sí sola

Conclusiones:

No existe una metodología única adecuada para todos los riesgos de un evento de masas. ISO 31000 puede utilizarse como marco general, mientras que Mosler, Cuantitativo Mixto o William T. Fine facilitan la valoración y priorización. HACCP, Gretener, MAGERIT y CARVER aportan análisis especializados para riesgos alimentarios, incendios, sistemas de información y amenazas deliberadas, respectivamente.

La selección debe responder al objeto del análisis, la información disponible y el nivel de detalle requerido. En eventos complejos resulta recomendable combinar un método general con herramientas específicas, evitando duplicidades y documentando los criterios utilizados. Los resultados deben contrastarse mediante inteligencia, experiencia operativa, inspecciones, simulaciones y seguimiento durante el evento.

5.2 TIPOLOGÍA DE AMENAZAS EN EVENTOS MASIVOS

Los eventos de masas pueden verse afectados por amenazas, peligros y fallos de diferente origen que interactúan entre sí y generan efectos encadenados. Su clasificación facilita la identificación sistemática de escenarios, evita que determinados riesgos queden sin analizar y permite asignar responsabilidades y medidas de tratamiento.

La seguridad debe adaptarse a la naturaleza, emplazamiento, duración y perfil del evento. Un mismo incidente puede pertenecer inicialmente a una categoría y producir consecuencias en otras; por ello, la clasificación no debe utilizarse como una estructura cerrada, sino como una herramienta para construir escenarios combinados.

Categoría	Descripción	Principales ejemplos
Amenazas físicas	Sucesos que pueden causar daños directos sobre las personas o las instalaciones	Presión de multitudes, atrapamientos, incendios, caídas, fallos estructurales, accidentes eléctricos y deficiencias de evacuación
Amenazas sociales y de orden público	Comportamientos colectivos o conflictos capaces de alterar el desarrollo del evento	Disturbios, peleas, rivalidad entre grupos, vandalismo, carreras, rumores, protestas conflictivas y alteraciones del orden
Amenazas deliberadas	Acciones intencionadas dirigidas a causar daño, interrupción, intimidación o impacto mediático	Terrorismo, sabotaje, vehículos hostiles, armas, explosivos, intrusión organizada y amenazas híbridas
Amenazas tecnológicas y cibernéticas	Ataques o fallos que comprometen los sistemas y servicios necesarios para la operación	Fallos eléctricos, pérdida de comunicaciones, caída del ticketing, interrupción de la megafonía, ciberataques y filtraciones de datos
Riesgos sanitarios y de salud pública	Situaciones que afectan a la salud individual o colectiva y pueden superar la capacidad asistencial	Emergencias médicas, intoxicaciones alimentarias, consumo de alcohol o drogas, brotes infecciosos y deficiencias higiénico-sanitarias
Fenómenos meteorológicos y ambientales	Condiciones naturales o ambientales capaces de afectar al público, las instalaciones y la continuidad	Viento intenso, tormentas, rayos, lluvias, inundaciones, temperaturas extremas, incendios forestales y contaminación

La evaluación debe considerar tanto cada categoría de forma individual como sus posibles interacciones. Los escenarios combinados suelen incrementar la gravedad y dificultar la respuesta.

Incidente inicial	Posibles efectos encadenados
Tormenta o viento intenso	Daños estructurales, corte eléctrico, pérdida de comunicaciones, lesiones y evacuación
Fallo del control de accesos	Colas, sobreocupación, presión de multitudes, altercados y retraso de los servicios de emergencia
Rumor o información falsa	Carreras, movimientos colectivos, caídas, bloqueo de salidas y situaciones de pánico
Ciberataque o fallo tecnológico	Pérdida de ticketing, videovigilancia, megafonía, información operativa o coordinación
Intoxicación o brote infeccioso	Aumento de la demanda asistencial, evacuaciones sanitarias, comunicación pública y posible suspensión
Acción deliberada	Múltiples víctimas, alteraciones colectivas, interrupción de servicios y despliegue de recursos extraordinarios

La identificación debe abarcar el recinto y su entorno, incluyendo accesos, zonas de espera, transporte, espacios de transición, infraestructuras temporales y servicios esenciales. Para cada escenario se determinarán las causas, activos expuestos, vulnerabilidades, consecuencias, señales de alerta, medidas preventivas, responsables y capacidad de respuesta disponible.

5.2.1 RIESGOS MÁS FRECUENTES

La frecuencia y gravedad de los riesgos dependen de la tipología del evento, el emplazamiento, el aforo, la duración, el perfil del público y las condiciones del entorno. Los siguientes escenarios deben considerarse como referencia inicial, sin perjuicio de incorporar la incorporación de otros derivados del análisis específico particular del evento:

Escenario	Factores asociados	Posibles consecuencias
Concentraciones y presión de multitudes	Alta densidad, cuellos de botella, flujos enfrentados, apertura de puertas o movimientos inesperados	Caídas, atrapamientos, asfixia, aplastamiento y bloqueo de vías de evacuación
Incendios y fallos estructurales	Instalaciones temporales, materiales combustibles, deficiencias eléctricas, sobrecargas o mantenimiento insuficiente	Quemaduras, intoxicación por humo, derrumbes, lesiones y evacuación
Emergencias sanitarias	Patologías previas, intoxicaciones, alcohol, drogas, brotes infecciosos o capacidad asistencial insuficiente	Múltiples afectados, saturación de recursos, traslados y suspensión de actividades
Alteraciones sociales y del orden público	Rivalidad, conflictos, protestas, rumores, conductas violentas o consumo de sustancias	Peleas, vandalismo, carreras, movimientos colectivos y daños personales
Acciones deliberadas	Terrorismo, sabotaje, intrusión, vehículos hostiles, armas o explosivos	Múltiples víctimas, pánico, interrupción del evento y activación de recursos extraordinarios
Fallos organizativos y logísticos	Sobrecupo, controles lentos, señalización deficiente, personal insuficiente o falta de coordinación	Colas, aglomeraciones, retrasos, accesos bloqueados y evacuaciones desordenadas
Fallos tecnológicos y cibernéticos	Interrupción eléctrica, pérdida de comunicaciones, caída del ticketing o ataque a los sistemas	Pérdida de control, información o vigilancia y dificultades para coordinar la respuesta
Fenómenos meteorológicos y ambientales	Viento, tormentas, rayos, lluvias, temperaturas extremas, incendios forestales o contaminación	Daños estructurales, afecciones sanitarias, aislamiento, evacuación o cancelación

Estos escenarios deben analizarse tanto individualmente como en sus posibles combinaciones. La prioridad no vendrá determinada únicamente por su frecuencia histórica, sino también por la exposición, la vulnerabilidad, la magnitud de las consecuencias y, en las amenazas deliberadas, por la capacidad, intención y oportunidad del posible adversario.

5.2.2 ESTRATEGIAS DE MITIGACIÓN

Las medidas de mitigación deben seleccionarse a partir del análisis específico del evento y aplicarse de forma proporcionada al nivel de riesgo. Cada medida debe tener un responsable, un plazo de implantación y un procedimiento para comprobar su eficacia antes y durante la celebración.

Ámbito de actuación	Principales medidas de mitigación
Análisis e inteligencia	Identificar amenazas, vulnerabilidades y escenarios; recopilar y contrastar información relevante; mantener actualizado el registro de riesgos y sus responsables
Accesos y gestión de multitudes	Dimensionar controles y zonas de espera; separar flujos; controlar la ocupación total y por sectores; prever la detención de accesos y mantener libres las rutas de emergencia
Infraestructuras e instalaciones	Revisar estructuras temporales, instalaciones eléctricas, protección contra incendios, señalización, alumbrado de emergencia, salidas y barras antipánico
Organización y recursos	Definir funciones, estructura de mando, procedimientos de actuación y reservas operativas; adaptar el despliegue a la evolución del evento
Formación y ejercicios	Capacitar al personal en sus funciones, gestión de multitudes, primeros auxilios y emergencias; realizar comprobaciones, ejercicios de mesa o simulacros
Tecnología de apoyo	Utilizar, cuando esté justificado, videovigilancia, analítica, sensores, drones, sistemas de localización y plataformas de gestión, verificando sus alertas y disponibilidad
Continuidad y comunicaciones	Prever alimentación de respaldo, comunicaciones alternativas y procedimientos manuales; disponer de canales coordinados para informar a equipos y asistentes
Coordinación externa	Establecer enlaces y procedimientos con fuerzas y cuerpos de seguridad, bomberos, protección civil, servicios sanitarios, movilidad y demás organismos intervinientes
Salud y condiciones ambientales	Dimensionar la asistencia sanitaria; controlar alimentos, agua e higiene; vigilar las condiciones meteorológicas y establecer umbrales para adaptar o suspender actividades
Información y participación	Facilitar normas, avisos e instrucciones accesibles; habilitar canales para solicitar ayuda o comunicar incidencias y evitar la propagación de rumores

La implantación debe comprobarse antes de la apertura mediante inspecciones, pruebas funcionales y reuniones de coordinación. Durante el evento, la monitorización permitirá revisar los riesgos y activar medidas adicionales cuando cambien la ocupación, el entorno o el nivel de amenaza.

La seguridad es una responsabilidad compartida, aunque corresponde al organizador garantizar el cumplimiento de sus obligaciones. Los asistentes deben recibir información clara y seguir las instrucciones del personal y de los servicios intervinientes, evitando conductas que puedan poner en riesgo al resto del público.

5.2.3 PAPEL DE LA SEGURIDAD PRIVADA EN EVENTOS DE MASAS

La seguridad privada constituye un componente esencial del dispositivo de protección de numerosos eventos de masas. Su participación debe planificarse conforme a la Ley 5/2014, de Seguridad Privada, delimitarse dentro del plan operativo y coordinarse con las fuerzas y cuerpos de seguridad y los servicios de emergencias, respetando las competencias de cada actor.

El director de seguridad, cuando su intervención sea preceptiva o haya sido prevista por la organización, dirigirá y coordinará los servicios y recursos de seguridad privada. El personal habilitado desarrollará exclusivamente las funciones atribuidas por la normativa, sin asumir competencias reservadas a las autoridades o a otros servicios profesionales.

Función	Actuaciones principales
Control y protección de accesos	Controlar entradas y zonas restringidas, comprobar acreditaciones cuando corresponda y realizar los controles de seguridad legalmente previstos sobre personas, objetos y vehículos
Vigilancia interior y perimetral	Proteger personas, bienes e instalaciones mediante presencia operativa y supervisión de accesos, perímetros, zonas críticas y espacios de especial protección
Prevención y detección	Identificar conductas, objetos o situaciones anómalas; verificar las alertas generadas por los sistemas y comunicar inmediatamente las incidencias
Apoyo a la gestión de multitudes	Supervisar zonas de concentración y circulación, informar al público, advertir de incrementos de densidad y ejecutar las medidas operativas previstas
Coordinación con autoridades	Mantener los enlaces y canales establecidos, transmitir información relevante y colaborar con las fuerzas y cuerpos de seguridad conforme a sus instrucciones
Actuación ante emergencias	Alertar, proteger la zona, facilitar la evacuación y prestar la primera ayuda dentro de su formación y medios, sin sustituir a los servicios sanitarios o de emergencia
Protección de activos críticos	Custodiar centros de control, sistemas de comunicaciones, instalaciones, equipos y recursos logísticos frente a intrusiones, robos, daños o sabotajes
Registro y trazabilidad	Documentar incidencias, comunicaciones y actuaciones para facilitar el seguimiento operativo, la investigación y la evaluación posterior

La seguridad privada debe disponer de información suficiente sobre los riesgos, la distribución del recinto, las rutas de evacuación, los procedimientos de comunicación y la estructura de mando. Su eficacia depende del dimensionamiento adecuado del servicio, la formación específica, el conocimiento previo del emplazamiento y la integración real con el conjunto del dispositivo.

El personal auxiliar, de admisión, organización o voluntariado puede desarrollar tareas informativas y logísticas, pero no debe realizar funciones legalmente reservadas al personal de seguridad privada.



5.3 FACTORES AGRAVANTES EN LA GESTIÓN DEL RIESGO

Determinadas circunstancias pueden aumentar la probabilidad de un incidente, agravar sus consecuencias o reducir la capacidad de respuesta. Entre las principales se encuentran:

- Sobreocupación: superación del aforo o distribución desequilibrada del público entre zonas.
- Espacios inadecuados: utilización de recintos, accesos o áreas de espera no dimensionados para la concentración prevista.
- Flujos deficientes: cruces entre entradas y salidas, cuellos de botella o bloqueo de rutas de emergencia.
- Señalización y comunicación insuficientes: mensajes contradictorios, pérdida de megafonía o ausencia de instrucciones accesibles.
- Falta de coordinación: responsabilidades imprecisas, canales incompatibles o deficiencias en la estructura de mando.
- Formación insuficiente: personal, auxiliares o voluntarios sin conocimiento de sus funciones y procedimientos.
- Mantenimiento deficiente: sistemas de seguridad o evacuación existentes, pero averiados, bloqueados o no disponibles, como alumbrado, extintores, comunicaciones, puertas o barras antipánico.

Como medida de mitigación, deben realizarse inspecciones y pruebas funcionales antes de la apertura, registrar las deficiencias detectadas y verificar su corrección o establecer medidas compensatorias antes del inicio del evento.

5.4 EVALUACIÓN PRÁCTICA DE RIESGOS

Para cada evento debe elaborarse un registro de riesgos que identifique los escenarios, sus causas, los elementos expuestos, las vulnerabilidades, las consecuencias y las medidas de tratamiento. La valoración podrá realizarse mediante una matriz de probabilidad e impacto o mediante otra de las metodologías descritas anteriormente.

En las amenazas deliberadas, la probabilidad histórica debe complementarse con información sobre la capacidad, intención o motivación y oportunidad del posible adversario.

Nivel	Criterio de actuación
Crítico	Requiere tratamiento inmediato. El evento o la actividad afectada no debe iniciarse o continuar mientras el riesgo permanezca fuera de los límites aceptables
Alto	Exige medidas preventivas específicas, responsables definidos y protocolos de respuesta antes de autorizar o desarrollar la actividad
Medio	Requiere medidas de mitigación, seguimiento y planes de contingencia proporcionados
Bajo	Puede gestionarse mediante controles ordinarios, vigilancia y revisión periódica

Ejemplos orientativos:

Escenario	Valoración inicial	Tratamiento
Concentración excesiva en un acceso principal	Probabilidad alta e impacto muy alto	Redistribución de flujos, detención temporal del acceso y refuerzo operativo
Fallo del sistema de ticketing	Probabilidad media e impacto alto	Sistema redundante, validación alternativa y procedimiento manual
Viento intenso sobre estructuras temporales	Probabilidad variable e impacto muy alto	Monitorización, umbrales de seguridad y suspensión o evacuación preventiva

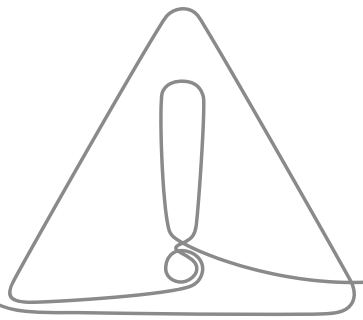
Tras aplicar las medidas debe calcularse o estimarse el riesgo residual. Su aceptación corresponderá al responsable competente y deberá quedar documentada, especialmente cuando pueda afectar a la autorización, continuidad o suspensión del evento.



5.5 RECOMENDACIONES PARA LA GESTIÓN DE RIESGOS

La gestión eficaz de los riesgos exige convertir los resultados del análisis en medidas concretas, verificables y adaptadas a las características de cada evento. Las siguientes recomendaciones proporcionan criterios generales para orientar su planificación, tratamiento y seguimiento, sin sustituir las obligaciones normativas ni las condiciones establecidas por las autoridades competentes:

- Realizar un análisis específico del evento que contemple el recinto, su entorno, los asistentes, las instalaciones, los servicios esenciales y las amenazas previsibles.
- Integrar el análisis en el plan de autoprotección o documento operativo correspondiente, conforme a la normativa y a los requisitos de la autoridad competente.
- Incorporar inteligencia previa y mecanismos de seguimiento que permitan revisar la valoración cuando cambien las amenazas, la ocupación o las condiciones del entorno.
- Evaluar los aforos, flujos y recorridos de evacuación mediante cálculos técnicos y, cuando esté justificado, herramientas de simulación.
- Asignar responsables, plazos e indicadores para cada medida de tratamiento y comprobar su implantación antes de la apertura.
- Inspeccionar y probar los sistemas de seguridad, comunicaciones, suministro de respaldo, señalización, alumbrado y evacuación.
- Definir protocolos de alerta, comunicación, escalado, confinamiento, evacuación, suspensión y recuperación de la actividad.
- Realizar ejercicios o simulacros proporcionados al riesgo, con participación de la organización, seguridad pública y privada y servicios de emergencias.
- Registrar las incidencias y decisiones, evaluar el dispositivo después del evento e incorporar las lecciones aprendidas en futuras ediciones.



6 PLANIFICACIÓN Y OPERATIVA DE LA SEGURIDAD



La planificación operativa representa el proceso mediante el cual el análisis de riesgos se transforma en capacidades reales de prevención, respuesta y recuperación. En eventos de masas, la eficacia de la seguridad no depende únicamente de los recursos disponibles, sino de la correcta integración de procedimientos, cadena de mando, comunicaciones y coordinación entre actores públicos y privados.

La experiencia acumulada en incidentes nacionales e internacionales demuestra que muchos fallos críticos no derivan de la ausencia de medios, sino de deficiencias en la organización operativa, en la interoperabilidad entre servicios o en la falta de validación práctica de los protocolos establecidos.

Por ello, esta guía propone una visión de la planificación basada en criterios de ingeniería operativa, digitalización de procesos y gestión dinámica de recursos sobre el terreno.

6.1 PLAN DE AUTOPROTECCIÓN Y EMERGENCIAS

El Plan de Autoprotección es el documento marco que establece el sistema de acciones y medidas orientadas a prevenir y controlar los riesgos sobre las personas y los bienes, así como dar respuesta adecuada a las situaciones de emergencia. En los eventos sometidos a esta obligación, el Plan de Autoprotección deberá ajustarse a la normativa estatal aplicable durante el régimen transitorio establecido por el Real Decreto 524/2023, así como a las disposiciones autonómicas, locales o sectoriales correspondientes.

Sin embargo, la experiencia operativa demuestra que la eficacia de un PAU no reside solo en su contenido documental, sino en su capacidad de ser ejecutado con precisión durante una crisis. Por ello, esta Guía recomienda transitar desde el documento estático hacia un modelo de **Autoprotección Digital Operativa**.

6.1.1 CONTENIDO Y ESTRUCTURA NORMATIVA

Cuando resulte obligatorio, el Plan de Autoprotección se estructurará conforme a la normativa aplicable. Entre sus contenidos esenciales se encuentran:

- Identificación de titulares y emplazamiento de la actividad.
- Inventario, análisis y evaluación de riesgos.
- Inventario de medios y recursos de autoprotección.
- Programa de mantenimiento de instalaciones.
- **Plan de Actuación ante Emergencias:** Definición de la secuencia de respuesta, equipos de intervención y esquemas de jerarquía y comunicación.

6.1.2 LA DIGITALIZACIÓN DEL PAU

La digitalización es el proceso de transformar la información técnica y los protocolos del PAU en una herramienta de gestión dinámica en tiempo real. La digitalización del Plan de Autoprotección puede incorporar, cuando resulte proporcionado a las características y riesgos del evento, los siguientes elementos:

- **Protocolos interactivos:** Los procedimientos de actuación dejan de ser textos en papel para convertirse en flujos de trabajo digitales. Ante una alerta, el sistema notifica automáticamente a los responsables y despliega las instrucciones específicas (misiones) en sus dispositivos móviles.
- **Cartografía digital y geolocalización de activos:** Todos los recursos descritos en el plan (salidas de emergencia, extintores, desfibriladores, puestos sanitarios) deben estar geolocalizados sobre una capa digital. Esto permite que, en caso de incidente, el centro de mando identifique visualmente el recurso más cercano y guíe a los equipos de intervención con precisión.
- **Gestión dinámica de equipos de intervención:** El PAU digital puede facilitar la asignación de tareas considerando la ubicación y disponibilidad del personal autorizado, mejorando la coordinación y respetando la normativa de protección de datos y los límites establecidos para su localización.
- **Trazabilidad y registro de actuaciones (Logs):** La digitalización permite registrar los principales hitos de la emergencia, como la detección, las comunicaciones, la movilización de recursos y las actuaciones realizadas. Los registros deberán proteger su integridad, disponibilidad y control de acceso, facilitando el análisis posterior, la rendición de cuentas y, cuando proceda, la investigación de los hechos.

6.1.3 *VALIDACIÓN Y MANTENIMIENTO DE LA CAPACIDAD OPERATIVA*

Un PAU digitalizado facilita las actividades de implantación, mantenimiento y actualización, permitiendo documentar la formación, los ejercicios, los simulacros y las comprobaciones preventivas de los medios de protección.

La elaboración y validación técnica deberán encomendarse a profesionales con las competencias exigidas por la normativa aplicable. La digitalización no modifica la responsabilidad sobre el contenido del plan y deberá comprobarse que la información, los procedimientos y la cartografía coinciden con las condiciones reales del evento.

6.2 ORGANIZACIÓN DE EQUIPOS Y CADENA DE MANDO

La organización del dispositivo debe establecer una estructura de dirección y coordinación clara, adaptada a la naturaleza y dimensión del evento. Cada participante debe conocer sus funciones, dependencia jerárquica, capacidad de decisión y canales de comunicación, evitando duplicidades, vacíos de responsabilidad o instrucciones contradictorias.

- Organizador o promotor: Responsable de cumplir las obligaciones asociadas a la organización y de proporcionar los medios humanos, técnicos y materiales exigibles.
- Dirección del Plan de Autoprotección y de Emergencias: Figuras definidas en el propio plan para garantizar su implantación, activarlo y dirigir las actuaciones iniciales ante una emergencia.
- Coordinador de Seguridad: Figura prevista específicamente en determinados acontecimientos deportivos y ejercida por un miembro de las fuerzas y cuerpos de seguridad.
- Fuerzas y Cuerpos de Seguridad: Responsables de las funciones que legalmente les corresponden en materia de seguridad ciudadana, orden público e investigación.
- Director de Seguridad y seguridad privada: Responsables de organizar y prestar los servicios privados de vigilancia, protección y control dentro de sus competencias y en coordinación con las autoridades.
- Servicios de emergencias: Integrados por bomberos, protección civil, servicios sanitarios y otros recursos públicos o privados previstos en la planificación.
- Personal auxiliar y voluntariado: Encargado de tareas informativas, orientación y apoyo logístico, sin asumir funciones reservadas al personal de seguridad o emergencias.

La estructura deberá representarse mediante un organigrama operativo conocido por los equipos, acompañado de un directorio de contactos y una matriz de comunicaciones, decisiones y escalado que determine quién informa, quién decide y quién ejecuta en cada escenario.

6.3 COORDINACIÓN INTERINSTITUCIONAL

La coordinación entre organismos es uno de los factores diferenciales de éxito en la gestión de eventos seguros.

La coordinación deberá apoyarse en un Plan de Comunicaciones que identifique interlocutores, redes y canales, grupos de comunicación, prioridades, códigos de llamada, procedimientos de escalado y medios alternativos. El plan deberá contemplar la interoperabilidad entre organizaciones, la posible saturación o pérdida de las redes habituales y la distribución de información operativa y mensajes dirigidos al público.

- Antes del evento: reuniones de coordinación con representantes de policía, seguridad privada, emergencias, protección civil y organización.
- Durante el evento: establecimiento del centro de control, puesto de mando o estructura de coordinación que corresponda, con representación de los servicios necesarios y comunicaciones operativas.
- Después del evento: sesiones de evaluación post-incidente/post-evento para recoger lecciones aprendidas.

Ejemplo práctico: en grandes eventos deportivos, el CCO suele integrar en tiempo real videovigilancia, emergencias sanitarias, policía y seguridad privada, facilitando una respuesta coordinada ante los incidentes.



6.4 PROTOCOLOS DE ACTUACIÓN DURANTE EL EVENTO

Se recomienda disponer de protocolos escritos, conocidos por todos los equipos y ensayados previamente.

Accesos y control de aforo:

- Control mediante sistemas seguros de ticketing, acreditaciones o códigos verificables. El uso de biometría requerirá una necesidad justificada, proporcionalidad y una base jurídica adecuada.
- Vigilancia de objetos prohibidos.
- Monitorización del flujo de entrada y salida para evitar aglomeraciones.
- Señalización adecuada de las vías de evacuación.

Gestión de multitudes:

- Sistemas de señalización dinámica (pantallas, megafonía, apps).
- Personal de apoyo en puntos críticos de concentración.
- Protocolos de redistribución de público en caso de sobreocupación.

Actuación en emergencias:

- Procedimientos para evacuación ordenada y rápida.
- Asignación de responsables por zona de evacuación.
- Uso de mensajes pregrabados multilingües para megafonía.
- Señalización adecuada de las vías de evacuación.

Incidentes sanitarios:

- Protocolos para emergencias médicas individuales, incluyendo reanimación cardiopulmonar (RCP) y utilización de desfibriladores por personal formado.
- Coordinación con hospitales de referencia.
- Puntos fijos de atención sanitaria con capacidad de triage.

Incidentes de orden público o violencia:

- Detección temprana, comunicación y aplicación de las medidas de contención o intervención que correspondan según las competencias de cada servicio.
- Protocolos de comunicación con policía y refuerzo inmediato.
- Sistemas de videovigilancia y registro gestionados conforme a la normativa, con procedimientos de conservación, integridad, acceso y puesta a disposición de las autoridades.

6.5 RECOMENDACIONES PRÁCTICAS PARA LA OPERATIVA

La operativa de seguridad debe traducir la planificación en actuaciones conocidas, verificables y adaptables a la evolución del evento. Antes de la apertura deben comprobarse los recursos, procedimientos y canales de coordinación, asegurando que cada equipo conoce sus funciones y dispone de los medios necesarios para ejecutarlas.

- Realizar una reunión operativa previa con los responsables de organización, seguridad pública y privada, emergencias, servicios sanitarios, movilidad y personal auxiliar.
- Comprobar el recinto y su entorno mediante una inspección previa de accesos, zonas de espera, recorridos, salidas, espacios de intervención y vías de evacuación.
- Verificar los sistemas críticos, incluyendo comunicaciones, videovigilancia, control de accesos, megafonía, alumbrado de emergencia, suministro de respaldo y medios de protección contra incendios.
- Confirmar la disponibilidad de los equipos, su distribución territorial, responsables, horarios, relevos, reservas operativas y capacidad de movilización.
- Difundir el organigrama y el Plan de Comunicaciones, identificando interlocutores, canales, prioridades, procedimientos de escalado y medios alternativos.
- Garantizar la formación del personal en sus funciones, autoprotección, evacuación, comunicaciones y primeros auxilios, según las tareas asignadas.
- Aplicar procedimientos de apertura y cierre, incluyendo la autorización de inicio, control progresivo de accesos, finalización escalonada y supervisión de las zonas exteriores.
- Monitorizar dinámicamente el evento, atendiendo a la ocupación, los flujos, las incidencias, las condiciones ambientales y cualquier cambio en el nivel de amenaza.
- Registrar las incidencias y decisiones, dejando constancia de las alertas, comunicaciones, actuaciones y recursos movilizados.
- Realizar una evaluación posterior, identificando desviaciones, medidas correctoras y lecciones aprendidas para futuras ediciones.

La operativa debe mantenerse flexible y permitir la adaptación del dispositivo sin perder la unidad de dirección. La combinación de comprobaciones previas, seguimiento continuo, comunicaciones eficaces y evaluación posterior permite convertir el plan en una capacidad real de prevención y respuesta.

7 ARQUITECTURA TECNOLÓGICA Y SISTEMAS INTELIGENTES DE SEGURIDAD



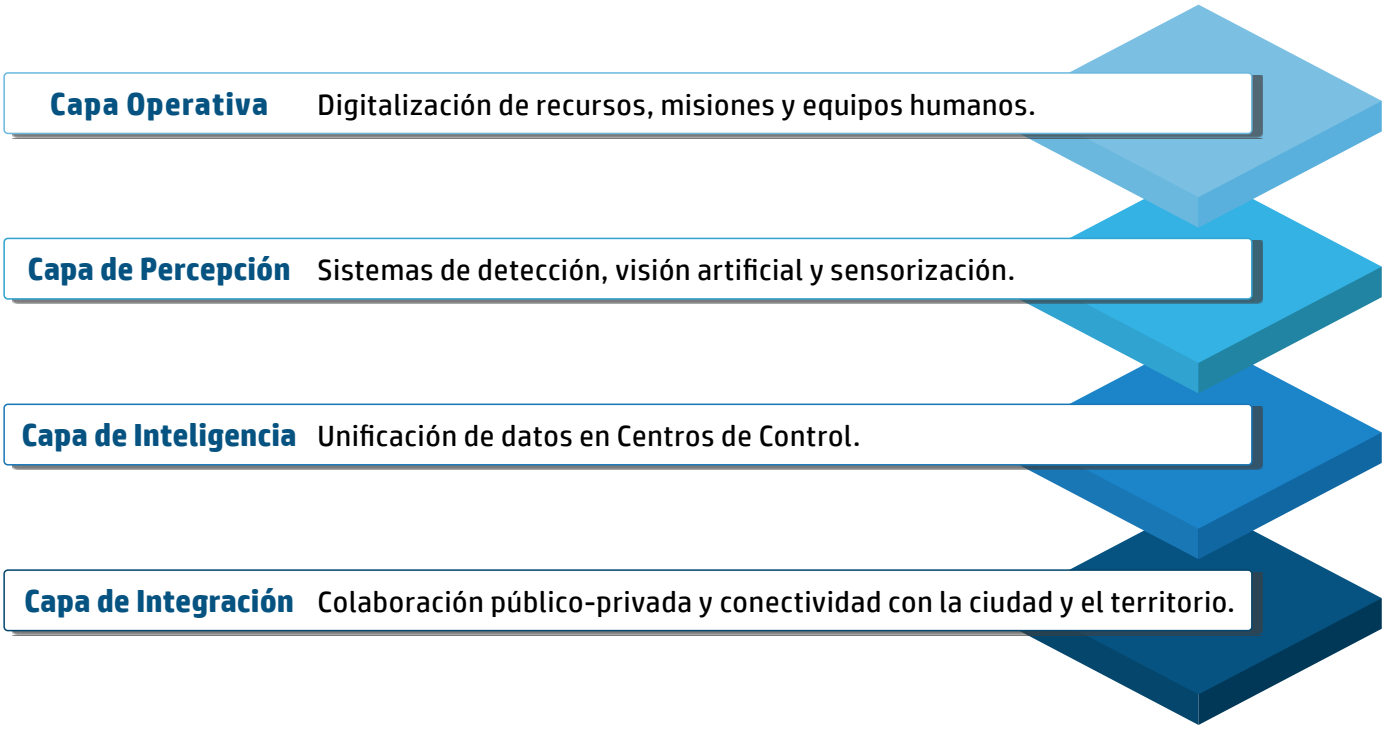
La transformación digital está redefiniendo el concepto de seguridad aplicada a eventos de masas. La evolución desde modelos reactivos basados exclusivamente en presencia física hacia ecosistemas inteligentes de prevención y respuesta representa uno de los principales cambios estructurales del sector en la última década.

La incorporación de tecnologías como inteligencia artificial, analítica avanzada de vídeo, IoT, comunicaciones críticas, geolocalización operativa o plataformas de mando y control permite mejorar significativamente la capacidad de anticipación, la trazabilidad de actuaciones y la coordinación interinstitucional.

No obstante, la tecnología solo aporta valor real cuando se integra dentro de una arquitectura operativa coherente, alineada con el análisis de riesgos, el Plan de Autoprotección y los procedimientos de gestión de crisis.

El objetivo de este capítulo es analizar las soluciones tecnológicas actuales bajo un prisma de escalabilidad e integración. Para ello, se propone un modelo de capas que evoluciona desde la verticalidad operativa (la gestión interna del evento) hacia la integración externa (la conexión con el territorio y los servicios de emergencia de la ciudad).

Bajo esta perspectiva, la consideración de un evento como "seguro" no depende de la mera acumulación de dispositivos, sino de la capacidad del sistema para garantizar que la información fluya sin interrupciones desde el operativo a pie de campo hasta el centro de mando. Este nivel de madurez tecnológica se alcanza mediante el despliegue de cuatro capas de integración:



7.1 CAPA OPERATIVA: DIGITALIZACIÓN DE LA RESPUESTA Y GESTIÓN DE EQUIPOS

Esta capa constituye el "sistema nervioso" interno del evento. Su función primordial es la digitalización de la actividad humana y la gestión de recursos técnicos sobre el terreno, permitiendo que la planificación teórica descrita en el Plan de Autoprotección (PAU) se transforme en una operativa dinámica y controlada.

En función de sus características y del análisis de riesgos, la capa operativa del evento podrá incorporar sistemas digitales que complementen los procedimientos y comunicaciones convencionales, mejoren la coordinación de los equipos y faciliten una gestión dinámica de los recursos sobre el terreno:

7.1.1 GESTIÓN DE MISIONES DIGITALES Y FLUJOS DE TRABAJO

La gestión de la seguridad en eventos de masas puede combinar las comunicaciones de voz con herramientas digitales que reduzcan ambigüedades, estructuren las actuaciones y faciliten su seguimiento. La Gestión de Misiones Digitales traslada determinados procedimientos del Plan de Autoprotección y de los protocolos operativos a flujos de trabajo activos y contextualizados. Una misión digital consiste en una instrucción o secuencia de tareas enviada a los dispositivos autorizados del personal operativo en función de sus competencias, responsabilidad, disponibilidad y, cuando resulte necesario, ubicación.

Para que un evento alcance la consideración técnica de "seguro", el sistema de gestión de misiones debe garantizar:

- **Precisión y eliminación de la ambigüedad:** Los protocolos de emergencia se fragmentan en pasos claros que el operativo debe confirmar, evitando interpretaciones subjetivas en momentos de alto estrés. El uso de checklists guiados asegura que la respuesta proyectada en el diseño del PAU sea la que se ejecute realmente en campo.
- **Segmentación inteligente de la información:** El sistema discrimina la información enviada según el perfil profesional y el área de responsabilidad. Así, un sanitario recibe misiones de triaje y un vigilante misiones de control de flujos, reduciendo drásticamente el "ruido informativo" y mejorando el tiempo de reacción.
- **Trazabilidad y registro de actuaciones:** Los principales hitos de la misión pueden registrarse mediante marcas de tiempo, identificación del usuario y estado de ejecución. Cuando se protegen adecuadamente su integridad, autenticidad, conservación y control de acceso, estos datos facilitan la reconstrucción de las actuaciones, la evaluación del dispositivo y la elaboración de informes y lecciones aprendidas.

Este enfoque convierte a cada miembro del equipo en un nodo activo de información y permite al centro de control supervisar el estado de las tareas, identificar retrasos o incidencias y comprobar la ejecución de los pasos críticos del protocolo. Su eficacia dependerá de la disponibilidad del sistema, la formación del personal y la existencia de procedimientos alternativos ante fallos tecnológicos.

7.1.2 GEOLOCALIZACIÓN DE OPERATIVOS Y ACTIVOS EN TIEMPO REAL:

Si la gestión de misiones representa el sistema nervioso de la seguridad, la geolocalización aporta conciencia espacial al ecosistema operativo. En eventos extensos, itinerantes o con una distribución compleja, conocer la posición y disponibilidad de determinados recursos humanos y materiales puede mejorar su asignación y reducir los tiempos de movilización. La información deberá representarse sobre una cartografía actualizada, con el nivel de precisión necesario para cada función y considerando las limitaciones de las tecnologías de posicionamiento utilizadas.

La integración de esta tecnología en la capa operativa garantiza tres beneficios críticos:

- **Optimización de la respuesta y principio de proximidad:** Ante una alerta sanitaria o de seguridad, el Centro de Control no lanza una llamada general; visualiza el recurso más cercano al incidente y le asigna la misión de forma directa. Esto reduce drásticamente los tiempos de intervención inicial, factor determinante para el éxito en paradas cardiorrespiratorias o conatos de incendio.
- **Conciencia situacional y seguridad del staff:** Elimina la "ceguera operativa" en espacios extensos o complejos. El mando conoce la ubicación real de sus efectivos, pudiendo monitorizar su seguridad y asegurar que las patrullas cubren efectivamente las zonas de riesgo proyectadas en el PAU, evitando áreas desatendidas.
- **Gestión de activos críticos:** La geolocalización no se limita a personas. Digitalizar la ubicación de desfibriladores (DESA), extintores o llaves de corte de suministros permite que cualquier operativo localice el medio de protección más próximo en su dispositivo móvil, incluso en condiciones de baja visibilidad o alto estrés.

El registro de determinados datos de posición puede facilitar la evaluación posterior de la distribución y movilización de los recursos. La localización del personal deberá limitarse a las funciones, espacios y periodos necesarios para la operativa, informando a las personas afectadas y estableciendo controles de acceso, plazos de conservación y medidas de seguridad. Los registros podrán contribuir a la trazabilidad del dispositivo, siempre que se garantice su integridad y se utilicen exclusivamente para las finalidades previamente definidas.

7.1.3 *CHECKLISTS DE VERIFICACIÓN PREVENTIVA Y OPERATIVA:*

La seguridad del evento no depende únicamente de la respuesta ante los incidentes, sino también de la comprobación previa y periódica de las medidas preventivas. Las listas de verificación digitales pueden estructurar estas revisiones, asignar responsables, registrar deficiencias y facilitar su seguimiento. Su utilización complementa las inspecciones y comprobaciones técnicas, contribuyendo a verificar que los medios y procedimientos previstos se encuentran implantados antes de la apertura y durante el desarrollo de la actividad.

La implementación de verificaciones digitales bajo estándares de ingeniería garantiza tres niveles de protección:

- **Verificación de instalaciones y medios de protección**: El personal competente deberá comprobar el estado de los elementos asignados, como las salidas de emergencia, vías de evacuación, medios de extinción, grupos electrógenos, alumbrado de emergencia, sistemas de comunicación, vallados y barras antipánico. Las fotografías, lecturas NFC/QR u otras evidencias pueden asociar la comprobación a un elemento, lugar y momento determinados, sin sustituir el criterio técnico ni acreditar por sí solas que la inspección se haya realizado correctamente.
- **Verificación previa a la apertura**: Antes de permitir la entrada de público deberá completarse un procedimiento de comprobación por zonas o sectores. Las deficiencias detectadas se comunicarán al responsable correspondiente, que deberá ordenar su corrección, establecer medidas compensatorias o impedir la apertura de la zona afectada cuando no existan condiciones suficientes de seguridad. La decisión y las comprobaciones realizadas deberán quedar registradas.

- **Seguimiento de la continuidad operativa:** Durante el evento, se programan verificaciones recurrentes para monitorizar puntos calientes, niveles de ruido o estado de las zonas de restauración. Esto permite detectar desviaciones preventivas antes de que se conviertan en emergencias.

El sistema permite generar informes de las comprobaciones realizadas, las deficiencias detectadas, las medidas correctoras y las personas responsables de cada actuación. Estos registros facilitan el seguimiento, la evaluación posterior y, cuando proceda, la acreditación de las revisiones efectuadas, siempre que se protejan su integridad, autenticidad, conservación y control de acceso. Su existencia no sustituye las inspecciones obligatorias ni excluye las responsabilidades que puedan corresponder.

7.1.4 COMUNICACIONES CRÍTICAS DE DATOS

En eventos de gran concurrencia, las redes móviles comerciales pueden experimentar saturación o degradación, por lo que la respuesta no debe depender de un único canal. Las comunicaciones de voz deben complementarse, cuando lo requiera la operativa, con servicios de datos capaces de transmitir imágenes, posiciones, alertas y protocolos con niveles adecuados de prioridad, disponibilidad y seguridad. Este apartado aborda los servicios y flujos de información utilizados por los equipos, mientras que la infraestructura de red que los soporta se desarrolla en el punto 7.2.7.

La implementación de una infraestructura de datos robusta bajo estándares de ingeniería garantiza tres capacidades estratégicas:

- **Priorización y Calidad de Servicio (QoS):** Las redes privadas, híbridas o los servicios con mecanismos de priorización pueden separar o priorizar el tráfico operativo respecto al utilizado por el público. Su diseño deberá establecer los niveles requeridos de disponibilidad, latencia y capacidad, así como comprobar su funcionamiento mediante pruebas de cobertura y carga representativas de los periodos de máxima concurrencia.
- **Enriquecimiento de la conciencia situacional:** La comunicación de datos permite al operativo enviar fotografías de una incidencia, un objeto sospechoso o una herida, proporcionando al mando una visión exacta de la realidad que la voz no puede describir con la misma precisión. Asimismo, la recepción de planos dinámicos o fichas de intervención en los dispositivos móviles minimiza el error humano.
- **Gestión de alertas silenciosas:** En situaciones de orden público donde la discreción es vital, la comunicación de datos permite activar protocolos y notificar incidencias mediante pulsaciones digitales o alertas vibratorias, evitando el uso de la voz que podría escalar la tensión en el entorno inmediato.

Las comunicaciones de datos contribuyen a la trazabilidad operativa al permitir registrar la información recibida, las alertas emitidas y las decisiones adoptadas. El sistema deberá identificar posibles pérdidas, retrasos o interrupciones de las comunicaciones y conservar los datos necesarios conforme a los criterios de integridad, disponibilidad, seguridad y protección de datos establecidos.

7.1.5 TRAZABILIDAD FORENSE DE LAS ACTUACIONES

La gestión de la seguridad en eventos de masas exige documentar las incidencias, comunicaciones, decisiones y actuaciones relevantes desarrolladas durante la operativa. Los sistemas digitales pueden facilitar esta trazabilidad mediante registros de actividad o logs que permitan reconstruir la secuencia temporal y evaluar la respuesta. El alcance del registro deberá ser proporcionado, técnicamente viable y compatible con la protección de datos, la confidencialidad y los periodos de conservación aplicables.

La implementación de este sistema de registro bajo estándares de ingeniería garantiza tres pilares fundamentales:

- **Reconstrucción cronológica de las actuaciones**: Ante un incidente, el sistema puede facilitar la consulta de las alertas recibidas, las tareas asignadas, las comunicaciones registradas y los tiempos asociados a la intervención. Esta información contribuye a reconstruir los hechos y puede resultar útil en evaluaciones, investigaciones o reclamaciones, siempre que su integridad, autenticidad y cadena de custodia puedan acreditarse.

- **Análisis crítico post-evento:** La disponibilidad de datos objetivos permite evaluar el desempeño de los equipos sin sesgos subjetivos. Identificar cuellos de botella en la comunicación o retrasos en sectores específicos facilita la mejora continua de los planes de autoprotección para futuras ediciones, optimizando tanto la seguridad como la eficiencia de los recursos.

- **Integridad y conservación de la información**: Los registros digitales deberán protegerse mediante controles de acceso, cifrado, sincronización temporal, copias de seguridad y mecanismos que permitan detectar alteraciones. Cuando puedan utilizarse en una investigación, deberán aplicarse procedimientos de preservación y cadena de custodia. Estos registros complementan los informes, grabaciones y demás evidencias disponibles, sin sustituirlos ni otorgarles por sí solos un valor probatorio definitivo.

En conclusión, la trazabilidad constituye una herramienta de control, aprendizaje y rendición de cuentas que permite conocer cómo se gestionaron los incidentes y detectar oportunidades de mejora. Su utilidad dependerá de la calidad y proporcionalidad de los datos registrados, de su correcta interpretación y de la existencia de procedimientos que garanticen su protección y conservación.



7.2 CAPA DE PERCEPCIÓN: SISTEMAS DE CAPTACIÓN E INTELIGENCIA DE DATOS

Si la capa operativa representa el sistema nervioso, la capa de percepción reúne los medios que captan información sobre el entorno, la ocupación, las instalaciones y el desarrollo del evento. Su función es apoyar la detección temprana de anomalías, la medición de flujos y el seguimiento de las condiciones que puedan incrementar el riesgo.

Los sistemas de captación deberán integrarse con los procedimientos operativos y el centro de control, de modo que los datos relevantes puedan convertirse en alertas verificables e información útil para la toma de decisiones. Su implantación deberá ser proporcionada al riesgo y considerar la fiabilidad, cobertura, mantenimiento, ciberseguridad y protección de datos.

7.2.1 VIDEOVIGILANCIA INTELIGENTE Y ANALÍTICA DE VÍDEO (IA)

La videovigilancia puede complementarse con sistemas de analítica de vídeo capaces de procesar imágenes y generar alertas sobre situaciones previamente definidas. En función del análisis de riesgos, estas herramientas pueden apoyar el conteo y la estimación de densidades, el control de flujos, la detección de intrusiones, humo, caídas, carreras, movimientos en direcciones no previstas u otros patrones que requieran comprobación. Las alertas deberán ser verificadas por personal autorizado antes de adoptar decisiones que puedan afectar a las personas.

La implementación de analíticas de vídeo basadas en Inteligencia Artificial (IA) bajo estándares de ingeniería garantiza tres capacidades críticas:

- **Detección de incidentes en tiempo real:** Los algoritmos de IA permiten la identificación instantánea de eventos críticos como conatos de incendio (detección de humo y llama), abandono de objetos sospechosos en vías de evacuación, o intrusiones en zonas restringidas. El sistema genera alertas automáticas hacia el Centro de Control, eliminando la dependencia exclusiva de la fatiga del operador humano.

- **Análisis de comportamiento:** Mediante el seguimiento de la dirección, velocidad y densidad del público, el sistema puede alertar de forma temprana ante movimientos erráticos, caídas accidentales de personas en zonas de paso o el inicio de un "efecto estampida". Esta capacidad es vital para activar protocolos de desvío de flujos antes de que se alcance un punto de saturación crítico e irreversible.

- **Búsqueda forense:** La IA permite realizar búsquedas complejas por atributos (color de vestimenta, complexión, objetos portados) en todo el histórico de cámaras en cuestión de segundos. Esto reduce drásticamente los tiempos de localización en casos de menores extraviados o identificación de autores de incidentes, garantizando una respuesta profesional ante las familias y las autoridades.

El diseño y la puesta en servicio deberán verificar que la ubicación, óptica, iluminación, cobertura, capacidad de procesamiento y comunicaciones responden a los objetivos previstos. También deberán evaluarse las tasas de error, los procedimientos de verificación humana, la ciberseguridad y el cumplimiento de la normativa sobre videovigilancia y protección de datos.

En eventos temporales o espacios sin infraestructura fija podrán utilizarse torres autónomas o unidades portátiles de videovigilancia con alimentación propia, comunicaciones móviles y grabación local. Asimismo, cuando esté justificado, podrán incorporarse cámaras corporales para proteger al personal y documentar intervenciones, estableciendo procedimientos específicos de activación, información, acceso, conservación y cadena de custodia. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.2 *SENSORIZACIÓN IOT*

La monitorización de las condiciones del entorno puede resultar especialmente útil en recintos cubiertos, espacios de gran extensión e instalaciones temporales. En función del análisis de riesgos, podrán desplegarse sensores IoT fijos o portátiles para medir variables físicas, ambientales u operativas y transmitirlas al centro de control. Estos sistemas complementan la observación humana y otros medios de supervisión, facilitando la detección de cambios que podrían pasar inadvertidos o no ser visibles mediante cámaras convencionales.

La implementación de una red de sensorización IoT bajo estándares de ingeniería garantiza tres capacidades de protección avanzada:

- **Detección precoz de incendios y calidad del aire:** El despliegue de sensores de partículas, temperatura y gases (CO2 y CO) permite identificar focos ígneos en etapas de latencia o combustión lenta. Asimismo, la monitorización de los niveles de CO2 se convierte en un indicador técnico fundamental para la gestión de la ventilación y la prevención de riesgos sanitarios en espacios cerrados o con alta densidad de ocupación.
- **Sonometría digital y control de impacto:** La integración de sonómetros inteligentes permite monitorizar de forma continua los niveles de presión sonora (dB). Esto no solo asegura el cumplimiento de las ordenanzas contra la contaminación acústica, sino que sirve como sensor de alerta ante cambios bruscos en el comportamiento del público (gritos masivos, explosiones o ruidos de colapso estructural).
- **Seguridad de infraestructuras temporales:** En eventos con grandes montajes (escenarios, gradas o carpas), el uso de sensores de inclinación, vibración y carga permite detectar fatigas materiales o desplazamientos críticos en la infraestructura antes de que se produzca un fallo catastrófico.

El diseño deberá seleccionar la tecnología de comunicación más adecuada - como LoRaWAN, redes móviles, Wi-Fi, BLE u otras alternativas - atendiendo al alcance, consumo energético, capacidad, latencia y cobertura requeridos. Los sensores deberán calibrarse, probarse y supervisarse, definiendo umbrales de alerta y procedimientos de verificación y mantenimiento.

También podrán utilizarse balizas y dispositivos portátiles para la localización en interiores, la notificación de emergencias, la medición temporal de temperatura, humedad, ruido o calidad del aire y la supervisión de instalaciones. La detección de sustancias mediante sensores específicos deberá considerarse una aplicación especializada y someterse a validación previa de fiabilidad, tasas de error y requisitos legales. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.3 SISTEMAS DE IDENTIFICACIÓN

La gestión de accesos y la movilidad del personal pueden apoyarse en tecnologías de identificación y acreditación adaptadas a la naturaleza y complejidad del evento. Cuando el análisis de riesgos lo justifique, podrán utilizarse RFID, NFC, Bluetooth de baja energía (BLE), códigos QR u otros sistemas para controlar accesos, gestionar autorizaciones por zonas y registrar determinados movimientos. La solución se seleccionará considerando la seguridad, fluidez, accesibilidad, privacidad, interoperabilidad, continuidad operativa y presupuesto disponible.

La aplicación de estos ecosistemas de identificación bajo estándares de ingeniería garantiza:

- **Versatilidad y accesibilidad (Códigos QR):** El uso de códigos QR dinámicos representa una solución eficiente y de bajo coste, ideal para el control de accesos mediante dispositivos móviles convencionales. Su facilidad de distribución y validación permite que eventos de menor escala digitalicen su control de entrada y salida, asegurando que el aforo real se mantenga siempre dentro de los límites legales establecidos en el PAU.

- **Gestión dinámica de zonas restringidas (RFID/NFC/BLE):** Para áreas de alta sensibilidad, se recomiendan tecnologías de proximidad que permitan una gestión "manos libres" o validaciones encriptadas más robustas. Esto asegura que solo operarios con misiones activas accedan a infraestructuras críticas, registrando accesos denegados como alertas automáticas en el Centro de Control.

- **Control de la ocupación y prevención del fraude**: Los identificadores digitales, combinados con el registro de entradas y salidas y con mecanismos de control de reutilización, facilitan la estimación de la ocupación y la detección de duplicidades, cesiones o usos no autorizados. Estos datos deberán contrastarse con los controles operativos, ya que la emisión o validación de una acreditación no garantiza por sí sola la presencia ni la ubicación real de una persona.

La validación técnica de estos sistemas debe comprobar la interoperabilidad de los dispositivos, la disponibilidad de terminales de respaldo y la continuidad del control ante fallos de red o alimentación. Su integración con la respuesta operativa se limitará a los datos estrictamente necesarios, aplicando criterios de privacidad, control de acceso y conservación limitada de la información. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.4 SISTEMAS DE VIGILANCIA AÉREA MEDIANTE UAS (DRONES)

La incorporación de aeronaves no tripuladas (UAS), incluidos los drones cautivos conectados mediante cable, puede ampliar la capacidad de supervisión de los eventos de masas y complementar las cámaras fijas y los equipos desplegados sobre el terreno. Su utilización deberá responder al análisis de riesgos y a las condiciones operativas del evento, especialmente en recintos extensos, espacios exteriores, recorridos itinerantes o zonas de difícil acceso, y ajustarse en todo momento a la normativa aeronáutica, de seguridad y de protección de datos aplicable.

La implantación de unidades UAS, bajo criterios de ingeniería, seguridad operacional y coordinación con el dispositivo del evento, puede aportar las siguientes capacidades:

- **Monitorización dinámica de flujos y masas:** El dron permite observar desde el aire la formación de embudos, densidades críticas o movimientos de masas en puntos ciegos del sistema de CCTV fijo. Esta información visual es vital para que el Centro de Control tome decisiones de redistribución de público o apertura de vías de evacuación de forma anticipada.

- **Apoyo en búsqueda y rescate y localización de incidentes:** Equipados con cámaras de alta resolución y sensores térmicos, los drones pueden localizar rápidamente incidentes sanitarios o conatos de incendio en grandes explanadas o entornos naturales, guiando a los equipos de tierra de forma precisa mediante la transmisión de coordenadas en tiempo real.

- **Evaluación de daños y peritaje post-evento:** La capacidad de capturar imágenes aéreas de alta precisión permite documentar el estado de las infraestructuras antes, durante y después del evento, sirviendo como prueba técnica del cumplimiento de las medidas de seguridad y el estado del recinto.

La planificación de estas operaciones deberá comprobar su adecuación a la normativa aeronáutica aplicable y contemplar las autorizaciones, coordinaciones y limitaciones operativas correspondientes. También deberá verificar la competencia del operador y de los pilotos, las distancias de seguridad, los procedimientos de contingencia, la protección de datos y la transmisión segura y estable de las imágenes al centro de control. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.5 MONITORIZACIÓN DEL ESPECTRO RADIOELÉCTRICO Y SISTEMAS ANTIDRONES (C-UAS)

En determinados eventos, el análisis de riesgos puede requerir que la vigilancia del recinto se extienda al espacio aéreo próximo y a la disponibilidad del espectro utilizado por las comunicaciones críticas. En estos casos, podrán implantarse sistemas de detección y monitorización capaces de advertir la presencia de aeronaves no tripuladas no autorizadas, alteraciones del espectro o posibles interferencias, integrando sus alertas en los procedimientos de verificación, comunicación y respuesta establecidos para el evento.

La integración coordinada de estas tecnologías puede aportar capacidades complementarias en tres ámbitos de protección:

- **Detección, seguimiento y clasificación de UAS**: La combinación de sensores de radiofrecuencia, radares y cámaras puede facilitar la detección y el seguimiento de drones en las inmediaciones del evento. La información obtenida deberá contrastarse con los vuelos autorizados y someterse a verificación antes de clasificar una aeronave como amenaza. Las alertas se comunicarán al centro de control y a las autoridades competentes para activar las medidas de protección previstas. Cualquier actuación de inhibición, interferencia o neutralización quedará reservada a los organismos legalmente habilitados.

- **Disponibilidad de las comunicaciones y detección de interferencias**: La monitorización autorizada del espectro puede advertir anomalías, degradaciones o interferencias que afecten a las comunicaciones de emergencia y a los sistemas de seguridad electrónica. La alerta técnica no determina por sí sola su origen intencionado, por lo que deberá verificarse conforme a los procedimientos establecidos y comunicarse a los responsables competentes. El dispositivo contará, además, con canales alternativos y procedimientos de respaldo que permitan mantener la coordinación operativa.

- **Protección de las personas ante vuelos no autorizados**: La presencia de un dron no autorizado sobre una concentración de personas puede generar riesgos por caída, colisión o utilización malintencionada. Su detección temprana permite valorar la trayectoria y el nivel de amenaza, informar a las autoridades y adoptar medidas proporcionadas, como interrumpir determinadas actividades, despejar zonas expuestas, proteger espacios críticos o aplicar los procedimientos de emergencia previstos.

La implantación de estos sistemas deberá verificar su compatibilidad electromagnética, su integración con las comunicaciones del evento y el cumplimiento de la normativa aeronáutica, de telecomunicaciones y de protección de datos aplicable. El diseño diferenciará claramente las funciones de detección y seguimiento de las medidas activas de interferencia o neutralización, cuyo empleo corresponde exclusivamente a los organismos legalmente habilitados. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.



7.2.6 SISTEMAS DE DETECCIÓN DE AMENAZAS Y OBJETOS PROHIBIDOS NO INVASIVOS

El control de acceso en eventos masivos debe equilibrar la detección de amenazas con la fluidez de entrada, evitando colas y concentraciones que puedan generar nuevos riesgos. Cuando el análisis realizado lo justifique, podrán emplearse tecnologías de detección para identificar posibles armas, objetos contundentes, recipientes u otros elementos prohibidos, reduciendo el contacto físico y las detenciones innecesarias. Su implantación deberá considerar la capacidad real de procesamiento, las tasas de falsas alarmas y los procedimientos de comprobación secundaria.

La integración de estos sistemas de escaneo avanzado bajo estándares de ingeniería garantiza:

- **Detección selectiva en movimiento**: Los sistemas basados en ondas milimétricas, inducción magnética u otras tecnologías de detección pueden analizar a los asistentes durante su paso e identificar objetos o patrones que requieren una comprobación adicional. Sus prestaciones dependerán de la configuración, el entorno y la tipología de las amenazas. Un dimensionamiento adecuado de los carriles y de los puestos de inspección secundaria puede mejorar la fluidez y reducir la formación de colas en el perímetro.

- **Detección de objetos ocultos**: Las tecnologías de imagen pasiva o activa pueden advertir la presencia de objetos adheridos al cuerpo o situados bajo la ropa y señalar al operador la zona en la que debe realizarse una comprobación adicional. Su utilización deberá respetar la intimidad y la protección de datos, limitar la visualización y conservación de imágenes y cumplir los requisitos de seguridad aplicables. Las alertas facilitarán una inspección secundaria proporcionada y realizada por personal autorizado.

- **Integración con el centro de control**: Estos dispositivos pueden transmitir alertas al sistema de gestión operativa para que sean verificadas y se active el procedimiento de inspección o intervención correspondiente. La información se facilitará únicamente al personal autorizado y mediante terminales seguros, limitándola a los datos necesarios para gestionar la incidencia. El tratamiento de imágenes, su conservación y cualquier seguimiento posterior deberán ajustarse a los protocolos establecidos y a la normativa de protección de datos.

La validación técnica deberá comprobar la compatibilidad de estos sistemas con otros equipos, su correcta configuración y el dimensionamiento de los carriles conforme a los flujos previstos. Antes de la apertura se realizarán pruebas de capacidad, tasas de alarma y tiempos de inspección secundaria, definiendo procedimientos alternativos ante averías o saturación. Estos resultados se coordinarán con las previsiones del Plan de Autoprotección. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.7 REDES DE CONECTIVIDAD Y RADIOCOMUNICACIONES DE MISIÓN CRÍTICA

La eficacia del dispositivo tecnológico depende de la disponibilidad y resiliencia de sus comunicaciones. En los eventos de masas, la concentración de usuarios puede saturar las redes móviles públicas, aunque exista cobertura suficiente. El Plan de Comunicaciones deberá combinar, según los riesgos y necesidades operativas, radiocomunicaciones profesionales, redes de datos, canales alternativos y procedimientos de contingencia, coordinando con los operadores de telecomunicaciones el posible refuerzo temporal de capacidad y cobertura.

La implantación coordinada de estas redes, bajo criterios de ingeniería de telecomunicaciones y continuidad operativa, puede aportar tres capacidades estratégicas:

- **Disponibilidad y calidad de servicio (QoS):** Las redes profesionales DMR o TETRA, las infraestructuras LTE/5G privadas y los servicios prioritarios sobre redes públicas pueden proporcionar distintos niveles de disponibilidad y calidad de servicio. La solución se seleccionará según los usuarios, la cobertura y las frecuencias legalmente disponibles, evitando puntos únicos de fallo y estableciendo canales alternativos. Su capacidad deberá comprobarse mediante pruebas de cobertura y carga en condiciones representativas del evento.

- **Operación y comunicaciones manos libres**: Las soluciones de radiocomunicación pueden incorporar periféricos de audio, pulsadores de emergencia y accesorios adaptados a las funciones de cada equipo. El modo manos libres facilita la comunicación de los intervinientes mientras utilizan extintores, camillas u otros medios, prestan asistencia o gestionan movimientos de público. Los equipos deberán configurarse y probarse considerando el ruido ambiental, la autonomía, la ergonomía y la compatibilidad entre dispositivos.

- **Transmisión de datos e interoperabilidad**: Además de la voz, estas redes pueden soportar alertas silenciosas, telemetría, imágenes y localización del personal. Su integración con el centro de control deberá facilitar la coordinación entre seguridad privada, Fuerzas y Cuerpos de Seguridad, protección civil, bomberos y servicios sanitarios. Cuando esté disponible, se valorará el acceso a redes de banda ancha para emergencias y la dotación de terminales o pasarelas compatibles, manteniendo una estructura de comunicaciones jerarquizada y segura.

La validación técnica deberá comprobar la planificación de frecuencias, la compatibilidad con otros servicios y la cobertura efectiva en las zonas de operación, incluidos sótanos, estructuras cerradas y recorridos de evacuación. Se realizarán pruebas de cobertura y capacidad antes del evento, identificando áreas de sombra y estableciendo canales, equipos o procedimientos alternativos para operar ante interferencias, saturación o pérdida de servicio. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.8 SISTEMAS DE MEGAFONÍA DE EMERGENCIA Y NOTIFICACIÓN MASIVA

La comunicación con el público es un elemento esencial para orientar la respuesta ante una emergencia y reducir la incertidumbre. El Plan de Comunicaciones deberá combinar medios complementarios y redundantes, como megafonía, señalización, pantallas, personal de información y, cuando resulte adecuado, notificaciones digitales a dispositivos móviles. La selección de canales considerará el ruido ambiental, la diversidad lingüística, la accesibilidad, la posible saturación de las redes y la pérdida parcial de alguno de los sistemas.

La implantación coordinada de estos medios, bajo criterios de ingeniería, accesibilidad y continuidad operativa, puede aportar tres funciones esenciales:

- **Inteligibilidad y cobertura acústica**: La megafonía de emergencia deberá diseñarse mediante cálculos electroacústicos y verificarse en condiciones representativas de ocupación y ruido ambiental. Los mensajes serán breves, claros, coherentes con el Plan de Autoprotección y, cuando proceda, estarán disponibles en varios idiomas. La emisión por zonas y su combinación con señales visuales y personal de apoyo facilitarán la comprensión de las instrucciones y su accesibilidad para el conjunto de los asistentes.

- **Notificaciones digitales y comunicación con los asistentes**: Cuando resulte proporcionado, podrán utilizarse aplicaciones voluntarias para enviar avisos, instrucciones o rutas recomendadas y para que los asistentes comuniquen de forma sencilla necesidades médicas, acompañantes perdidos, anomalías o peligros. Siempre que sea posible, estas funciones se prestarán sin identificar al usuario ni recopilar datos innecesarios. La recepción dependerá de la cobertura, la capacidad de la red, la configuración del terminal y el consentimiento requerido, por lo que este canal será complementario y nunca sustituirá a la megafonía y los restantes medios de información.

- **Resiliencia y supervisión del sistema**: Los sistemas de megafonía de emergencia deberán supervisar sus líneas, señalizar averías y disponer de alimentación de respaldo con una autonomía adecuada al análisis de riesgos. Las plataformas de notificación digital contarán con mecanismos de monitorización y contingencia propios. Ante un fallo de suministro o conectividad, el dispositivo deberá conservar al menos los canales esenciales y activar medios alternativos, como equipos portátiles, mensajes predefinidos y comunicación directa por parte del personal.

La validación técnica deberá comprobar el cumplimiento de la normativa y de las normas UNE-EN que resulten aplicables según el tipo y la función del sistema. Los mensajes, prioridades, zonas de difusión y responsables de activación se integrarán en el Plan de Autoprotección y se verificarán mediante pruebas periódicas, sin presuponer la recepción de las notificaciones móviles. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.9 SISTEMAS DE ENERGÍA GARANTIZADA Y CONTINUIDAD DE SERVICIO

La disponibilidad del suministro eléctrico condiciona el funcionamiento de la arquitectura tecnológica y de seguridad del evento. La pérdida de la red pública puede afectar a la videovigilancia, las comunicaciones, los controles de acceso, la megafonía y la iluminación. El diseño deberá identificar y priorizar las cargas críticas, asignarles fuentes de respaldo y autonomías acordes con el análisis de riesgos, y establecer una secuencia controlada de continuidad, recuperación o desconexión segura.

La implantación coordinada de estos sistemas de respaldo, bajo criterios de ingeniería eléctrica y continuidad operativa, puede aportar tres niveles de protección:

- **Sistemas de alimentación ininterrumpida (SAI/UPS)**: Los equipos críticos de percepción, comunicaciones y control deberán contar con sistemas que estabilicen el suministro y mantengan temporalmente su funcionamiento ante microcortes o pérdidas de tensión. Su potencia y autonomía se dimensionarán según las cargas priorizadas y el tiempo necesario para activar la generación secundaria o realizar una parada segura. El estado de las baterías y su capacidad efectiva deberán comprobarse mediante mantenimiento y pruebas periódicas..

- **Grupos electrógenos y fuentes alternativas**: Cuando el análisis de riesgos lo requiera, se dispondrán fuentes independientes dimensionadas para alimentar las cargas críticas priorizadas durante la autonomía prevista. Su diseño contemplará el arranque y la transferencia de carga, la disponibilidad de combustible, la ventilación, la evacuación de gases, la protección contra incendios y su ubicación frente a inundaciones, impactos o accesos no autorizados. Las pruebas previas deberán realizarse en condiciones de carga representativas.

- **Monitorización y gestión energética**: La infraestructura deberá permitir supervisar desde el centro de control el estado de las baterías, la disponibilidad de combustible, la carga conectada y las alarmas de los equipos de respaldo. Esta información facilitará la detección temprana de anomalías y la estimación de la autonomía restante. Se establecerán responsables y procedimientos para verificar las alertas, redistribuir o desconectar cargas y realizar comprobaciones locales cuando se pierda la telemetría.

La validación técnica deberá comprobar la separación y selectividad de los circuitos, la correcta priorización de cargas y la ausencia de puntos únicos de fallo que puedan afectar simultáneamente al suministro principal y al respaldo. Antes del evento se ensayarán la conmutación, las protecciones, la autonomía y el funcionamiento en modo degradado, dejando constancia de las incidencias y medidas correctoras. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.2.10 CIBERSEGURIDAD DE SISTEMAS FÍSICOS E INFRAESTRUCTURAS DIGITALES

La creciente dependencia tecnológica de los eventos exige integrar la ciberseguridad en la planificación general, especialmente cuando un incidente digital puede afectar a los accesos, las comunicaciones o la respuesta ante emergencias. Las cámaras, sensores IoT, redes, plataformas y sistemas de acreditación deberán protegerse mediante medidas proporcionales al riesgo, orientadas a preservar su disponibilidad, integridad, confidencialidad, autenticidad y capacidad de recuperación frente a errores, fallos, accesos no autorizados y ataques deliberados.

La aplicación de una estrategia de ciberseguridad adaptada al entorno operativo del evento deberá contemplar tres ámbitos principales de protección:

- **Protección y segmentación de redes**: Los sistemas de seguridad deberán operar en redes separadas lógica o físicamente de las destinadas al público, la producción y otros servicios del evento. La comunicación entre segmentos se limitará a los flujos necesarios mediante reglas de acceso, cortafuegos y monitorización. Las conexiones remotas y de proveedores estarán autenticadas, autorizadas y registradas, reduciendo la posibilidad de que el compromiso de una red se propague al centro de control o a otros sistemas críticos.

- **Securización de dispositivos y nodos**: Los equipos conectados deberán estar inventariados, configurados de forma segura y protegidos mediante credenciales individuales, control de accesos, cifrado cuando proceda y actualización de firmware y vulnerabilidades. Se deshabilitarán cuentas, puertos y servicios innecesarios, y se verificará el soporte del fabricante durante su vida útil. Estas medidas reducen el riesgo de manipulación de sensores o utilización de cámaras y dispositivos IoT como puntos de entrada a la infraestructura.

- **Monitorización y respuesta ante incidentes**: Los sistemas críticos deberán generar y conservar registros suficientes para detectar anomalías, accesos indebidos o posibles intrusiones. Las alertas se supervisarán y verificarán conforme a un procedimiento que defina responsables, escalado, comunicación, aislamiento, recuperación y conservación de evidencias. El centro de control deberá coordinar la respuesta técnica con la operativa y disponer de configuraciones de respaldo y procedimientos manuales para mantener las funciones esenciales mientras se recuperan los sistemas afectados.

La validación técnica deberá comprobar la aplicación de los requisitos legales y estándares de ciberseguridad que correspondan a la naturaleza del organizador, los sistemas y los servicios utilizados. El Esquema Nacional de Seguridad se aplicará cuando el evento o sus proveedores se encuentren dentro de su ámbito, pudiendo tomarse como referencia complementaria normas como ISO/IEC 27001 e IEC 62443. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.



7.3 CAPA DE INTELIGENCIA: UNIFICACIÓN DE DATOS EN CENTROS DE CONTROL

Esta capa agrega, correlaciona y representa la información procedente de los sistemas operativos y de percepción para facilitar una visión común del evento. El centro de control combina espacios, personas, procedimientos y herramientas tecnológicas que apoyan a los responsables en la evaluación de incidencias y la coordinación de la respuesta. La información deberá presentarse de forma jerarquizada, verificable y adecuada a cada perfil, sin sustituir el criterio ni la responsabilidad de quienes toman las decisiones.

7.3.1 PLATAFORMAS DE GESTIÓN DE SEGURIDAD INTEGRADA (PSIM)

Una plataforma de gestión de seguridad integrada puede reunir en una interfaz gráfica y georreferenciada la información relevante de distintos subsistemas, como videovigilancia, control de ocupación, alarmas de incendio, localización de equipos y sensores ambientales. Su alcance deberá adaptarse a la complejidad y los riesgos del evento, integrando únicamente los datos y funciones que aporten valor operativo. La interoperabilidad reducirá la dispersión de información, sin eliminar la necesidad de procedimientos alternativos ante fallos de la plataforma.

La implantación de una plataforma de gestión unificada, correctamente configurada e integrada con los procedimientos del evento, puede aportar las siguientes capacidades:

- **Visión operativa común**: El personal del centro de control puede visualizar sobre un mapa interactivo la ubicación estimada de las incidencias, los recursos disponibles y las cámaras o sensores relacionados. La plataforma deberá indicar el origen, la hora y el estado de actualización de cada dato, facilitando su verificación. Esta visión integrada ayuda a valorar la situación y reduce la dispersión de información entre sistemas y equipos intervinientes.
- **Digitalización y automatización de procedimientos**: La plataforma puede asociar cada alerta con flujos de trabajo previamente definidos, mostrando cámaras relacionadas, avisando a los responsables y proponiendo las actuaciones correspondientes. Las acciones con incidencia directa sobre la seguridad - como liberar accesos, emitir mensajes de emergencia o modificar recorridos - requerirán confirmación humana o interbloqueos específicos, salvo automatismos expresamente diseñados, evaluados y autorizados. Todas las actuaciones deberán quedar registradas y disponer de ejecución manual alternativa.
- **Análisis de datos y cuadros de mando**: La integración permite generar indicadores operativos, como el nivel estimado de ocupación por sectores, la evolución de los flujos o los tiempos de gestión de incidencias. Estos datos pueden apoyar el ajuste del despliegue durante el evento y el análisis posterior. Los indicadores deberán mostrar su fuente, actualización y nivel de fiabilidad, y ser interpretados junto con la información aportada por los equipos sobre el terreno.

La validación técnica deberá comprobar la interoperabilidad mediante interfaces documentadas, la calidad y sincronización de los datos, los perfiles de acceso y la seguridad de las comunicaciones. La arquitectura evitará que el servidor central constituya un punto único de fallo y dispondrá de respaldo, monitorización y procedimientos alternativos. Las integraciones deberán probarse antes del evento y después de cualquier cambio relevante. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.3.2 *CENTROS DE CONTROL Y PUESTOS DE MANDO*

La naturaleza temporal, itinerante o territorialmente dispersa de algunos eventos puede requerir capacidades de control próximas al lugar de intervención. Según su dimensión y estructura de mando, estas podrán prestarse desde un centro fijo, una instalación temporal, un vehículo de control o un centro remoto de apoyo. Cuando se establezca un Puesto de Mando Avanzado, sus funciones, responsables y comunicaciones deberán coordinarse con el centro de control del evento y con los servicios públicos intervinientes.

El despliegue planificado de unidades móviles de control puede aportar tres ventajas operativas principales:

- **Ubicación operativa y despliegue temporal**: El centro de control móvil permite aproximar determinadas funciones de coordinación al lugar del evento sin exigir que todos los responsables compartan físicamente el mismo espacio. Su emplazamiento deberá ser seguro, accesible y compatible con los recorridos de emergencia. El tiempo de puesta en servicio, la autonomía energética, las comunicaciones, la nivelación y los sistemas auxiliares se comprobarán previamente mediante pruebas de despliegue.
- **Conectividad e intercambio de información**: Estas unidades pueden actuar como nodos temporales para recibir, procesar y compartir información procedente de cámaras, drones, sensores y equipos desplegados. La conexión con otros centros deberá definir los datos intercambiados, los formatos, permisos y niveles de prioridad. Se preverán enlaces redundantes y procedimientos de comunicación degradada, considerando que la capacidad, la latencia o la disponibilidad pueden variar durante el evento.
- **Ergonomía y condiciones de trabajo**: El diseño interior del centro de control deberá considerar la ergonomía, el aislamiento acústico, la climatización, la iluminación, la accesibilidad y el número máximo de ocupantes. Los puestos y pantallas se distribuirán conforme a las funciones y líneas de visión necesarias, evitando una sobrecarga de información. En operaciones prolongadas se establecerán turnos, pausas y relevos que permitan mantener la atención y la capacidad de decisión.

La validación técnica de las unidades móviles deberá comprobar la seguridad eléctrica, la compatibilidad electromagnética, la distribución de cargas, la estabilidad, la ventilación y las condiciones de evacuación y protección contra incendios. También se verificarán las comunicaciones, la autonomía y el funcionamiento conjunto de los equipos en condiciones representativas. Los requisitos se adaptarán al tipo de vehículo o instalación temporal y a su entorno de despliegue. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.

7.3.3 GEMELOS DIGITALES Y SIMULACIÓN DE ESCENARIOS

La gestión de grandes concentraciones requiere herramientas que complementen la observación con capacidades de análisis y anticipación. En eventos complejos puede resultar útil disponer de un gemelo digital, entendido como una representación estructurada y actualizable del recinto, sus infraestructuras, recursos y condiciones operativas. Según su alcance y los datos disponibles, esta herramienta puede apoyar la visualización, la simulación de flujos y la evaluación de escenarios antes y durante la celebración del evento.

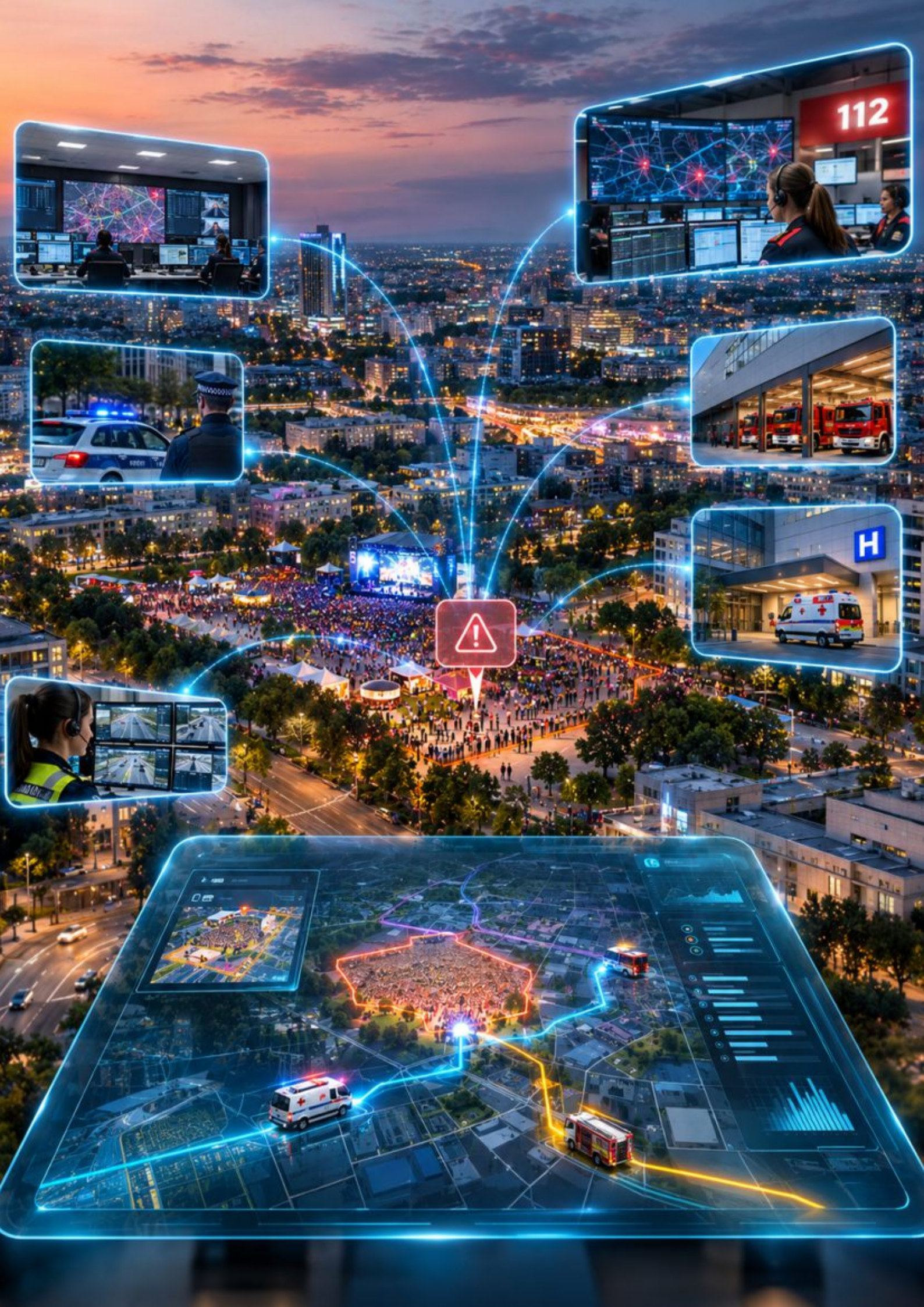
La implantación de un gemelo digital, adecuadamente modelado y mantenido, puede aportar tres capacidades avanzadas de apoyo a la decisión:

- **Simulación de evacuaciones y puntos críticos**: Los modelos de dinámica de multitudes permiten analizar escenarios como incendios, salidas bloqueadas, cambios de aforo o incidentes de orden público. Sus resultados ayudan a comparar alternativas, estimar tiempos de evacuación e identificar posibles cuellos de botella, apoyando la revisión de recorridos y recursos. Estas simulaciones representan comportamientos estimados y deberán contrastarse con inspecciones, ejercicios y criterio técnico antes de adoptar decisiones operativas.

- **Integración de datos dinámicos**: El gemelo digital puede incorporar información procedente del control de ocupación, cámaras, sensores IoT y sistemas operativos. La representación sobre el modelo facilita la visualización de flujos, concentraciones y condiciones ambientales, según la precisión y frecuencia de actualización disponibles. La plataforma deberá mostrar el origen, la vigencia y la fiabilidad de los datos, permitiendo verificar las alertas antes de considerar que existe una situación de densidad crítica.

- **Apoyo a la intervención**: Ante un incidente, el gemelo digital puede facilitar a los responsables una representación de la configuración del espacio, los accesos, los recursos y los activos críticos. Esta información ayuda a valorar rutas de aproximación y alternativas de intervención en recintos extensos, estructuras de varias plantas o espacios con desniveles. Su utilización deberá complementar, y no sustituir, el reconocimiento sobre el terreno y las indicaciones de los equipos desplegados.

La validación técnica deberá comprobar la correspondencia del modelo con el recinto, la procedencia y actualización de los datos y la adecuación de los parámetros utilizados. Las hipótesis, limitaciones y márgenes de incertidumbre de cada simulación deberán documentarse y comunicarse a los responsables, evitando utilizar sus resultados como única base para adoptar decisiones críticas. Ver detalles técnicos en el ANEXO: CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS.


112
H

7.4 CAPA DE INTEGRACIÓN: CONECTIVIDAD CON LA CIUDAD Y EL TERRITORIO

Un evento de masas puede afectar a la movilidad, el transporte, la actividad urbana y los servicios públicos más allá de su perímetro. Cuando su dimensión o impacto lo requieran, el dispositivo tecnológico deberá facilitar el intercambio de información entre el centro de control del evento y los servicios municipales y de emergencia competentes. Esta integración apoyará la coordinación público-privada, respetando las responsabilidades de cada organización, la protección de datos y los criterios acordados de acceso, finalidad, calidad y conservación de la información.

7.4.1 INTEROPERABILIDAD CON PLATAFORMAS DE CIUDAD

La integración entre el evento y las plataformas de ciudad puede facilitar el intercambio controlado de información sobre ocupación, incidencias, movilidad, condiciones ambientales y recursos disponibles. Esta conexión deberá responder a necesidades operativas previamente acordadas y proporcionar a los servicios municipales una visión compartida del impacto del evento. Cada organización conservará sus competencias, sistemas de referencia y responsabilidad sobre los datos que genere o gestione.

La aplicación de estándares y mecanismos de interoperabilidad puede aportar las siguientes capacidades:

- **Gestión de la movilidad y el transporte público**: El intercambio de datos de ocupación, horarios y previsiones de entrada o salida puede ayudar a los operadores y autoridades competentes a adaptar el transporte público, la regulación del tráfico y los itinerarios peatonales. Esta coordinación permite anticipar concentraciones en estaciones, paradas y vías próximas, sin perjuicio de que cada organismo verifique la información y adopte las decisiones correspondientes dentro de sus competencias.
- **Coordinación con los servicios de emergencia externos**: Ante una incidencia relevante, la integración puede facilitar el envío de su ubicación estimada, naturaleza, evolución, accesos disponibles y recursos movilizados. Esta información deberá verificarse, actualizarse y presentarse en formatos previamente acordados. La comunicación entre el centro de control del evento y los centros públicos puede mejorar la preparación de la intervención, complementando los canales oficiales de activación y coordinación establecidos
- **Monitorización del impacto en el entorno urbano**: Los datos procedentes de sensores ambientales, medición acústica y sistemas de movilidad pueden incorporarse a los cuadros de mando municipales para evaluar la incidencia del evento sobre su entorno. La analítica de vídeo u otras fuentes puede apoyar la detección de concentraciones y alteraciones de los flujos de llegada y salida. Su utilización deberá respetar las competencias administrativas, la normativa sectorial y la protección de datos.

La validación técnica deberá comprobar las interfaces, modelos de datos, formatos, frecuencias de actualización y mecanismos de autenticación y cifrado utilizados. Los acuerdos de integración definirán la finalidad, titularidad, calidad, acceso, conservación y responsabilidad sobre la información, así como los procedimientos aplicables ante errores o pérdida de conexión. Siempre que resulte viable, se utilizarán estándares abiertos y API documentadas que reduzcan la dependencia de proveedores concretos.

7.4.2 REDES DE COMUNICACIÓN INTEROPERABLES Y PASARELAS DE ENLACE

La respuesta ante una incidencia relevante requiere comunicaciones coordinadas entre la organización y los organismos intervinientes. La interoperabilidad podrá resolverse mediante grupos de comunicación autorizados, terminales compatibles, pasarelas de enlace, puestos de coordinación o procedimientos de transferencia de información. La interconexión directa con redes de seguridad pública solo se realizará cuando resulte necesaria, técnicamente viable y autorizada por sus responsables, sin comprometer la seguridad ni la disponibilidad de dichas redes.

La implantación coordinada de estas soluciones, bajo criterios de ingeniería de telecomunicaciones y continuidad operativa, puede aportar las siguientes capacidades:

- **Canales de coordinación operativa:** Cuando los responsables de cada organismo lo autoricen, podrán establecerse grupos de comunicación compartidos para intercambiar voz, alertas y datos esenciales entre seguridad privada, protección civil, Fuerzas y Cuerpos de Seguridad y servicios sanitarios. Su configuración deberá respetar la cadena de mando, los perfiles de acceso y la confidencialidad de las comunicaciones, manteniendo procedimientos alternativos de enlace a través de los respectivos centros de control.

- **Intercambio de datos con centros públicos**: La infraestructura podrá facilitar el envío seguro de alertas verificadas, imágenes relevantes, datos de ocupación y otra información necesaria a los centros públicos competentes, incluidos el CECOPAL o CECOPI cuando proceda. La transmisión estará sujeta a autorización, finalidad definida y control de acceso. La información deberá mostrar su origen y actualización, facilitando que las autoridades valoren la situación antes de movilizar recursos adicionales.

- **Resiliencia y disponibilidad de las comunicaciones**: La arquitectura deberá disponer de medios alternativos ante la degradación de una red o pasarela. En eventos de elevada concurrencia se coordinará con los operadores de telecomunicaciones el posible refuerzo temporal de la cobertura y capacidad móvil. También se valorará la disponibilidad de redes de banda ancha para emergencias y de terminales compatibles para los organismos intervinientes, verificando previamente su cobertura, autonomía y funcionamiento conjunto.

La validación técnica deberá comprobar la compatibilidad de terminales, pasarelas, cifrado y formatos de intercambio, así como la cobertura y capacidad en condiciones representativas. El empleo de frecuencias, redes o servicios de seguridad pública requerirá la autorización de sus responsables y el cumplimiento de la normativa aplicable. El Plan de Comunicaciones identificará canales principales y alternativos, responsables, prioridades y procedimientos ante pérdida de servicio.

7.4.3 DIFUSIÓN DE INFORMACIÓN Y GESTIÓN DE FLUJOS EN ENTORNO URBANO

La seguridad de un evento de masas comprende también las vías de aproximación, los espacios de transición y los nodos de transporte del entorno urbano. Cuando la dimensión o incidencia del evento lo requiera, su centro de control deberá coordinarse con los responsables municipales de paneles de mensaje variable, aplicaciones de movilidad y canales institucionales. Esta colaboración permite informar y orientar los movimientos de llegada y salida, reduciendo el riesgo de concentraciones en los espacios públicos próximos.

La utilización coordinada de estos sistemas de información puede aportar tres capacidades de gestión del entorno:

- **Señalética inteligente y guiado dinámico**: El Centro de Control puede enviar datos en tiempo real a los paneles de tráfico y transporte de la ciudad para informar sobre el estado de los accesos, aparcamientos completos o rutas de llegada recomendadas. Si un acceso detecta una saturación crítica de aforo, el sistema puede desviar proactivamente al público hacia entradas alternativas a través de la infraestructura urbana, equilibrando la carga de personas de forma segura.

- **Comunicación preventiva ante emergencias**: Ante una incidencia que requiera evacuación, confinamiento o restricción de accesos, los canales municipales pueden informar a la población del entorno y evitar nuevos desplazamientos hacia la zona afectada. Los mensajes deberán ser autorizados por el responsable competente, indicar claramente las actuaciones recomendadas y mantener coherencia con la información difundida dentro del recinto. También se preverán actualizaciones y comunicaciones de finalización de la alerta.

- **Análisis de movilidad posterior al evento**: Los datos de ocupación, transporte, tráfico y desplazamientos pueden utilizarse para evaluar la llegada y dispersión de los asistentes, identificar puntos de congestión y comparar las previsiones con el comportamiento observado. Las conclusiones ayudarán a revisar futuros planes de movilidad y autoprotección y a dimensionar servicios y espacios de transición. El análisis utilizará preferentemente datos agregados o anonimizados y limitará su conservación a la finalidad establecida.

Los protocolos de información deberán establecer quién elabora, verifica, autoriza, difunde y actualiza cada mensaje, así como los canales y públicos destinatarios. Antes del evento se comprobará la integración con los sistemas municipales y se prepararán mensajes básicos para los escenarios p



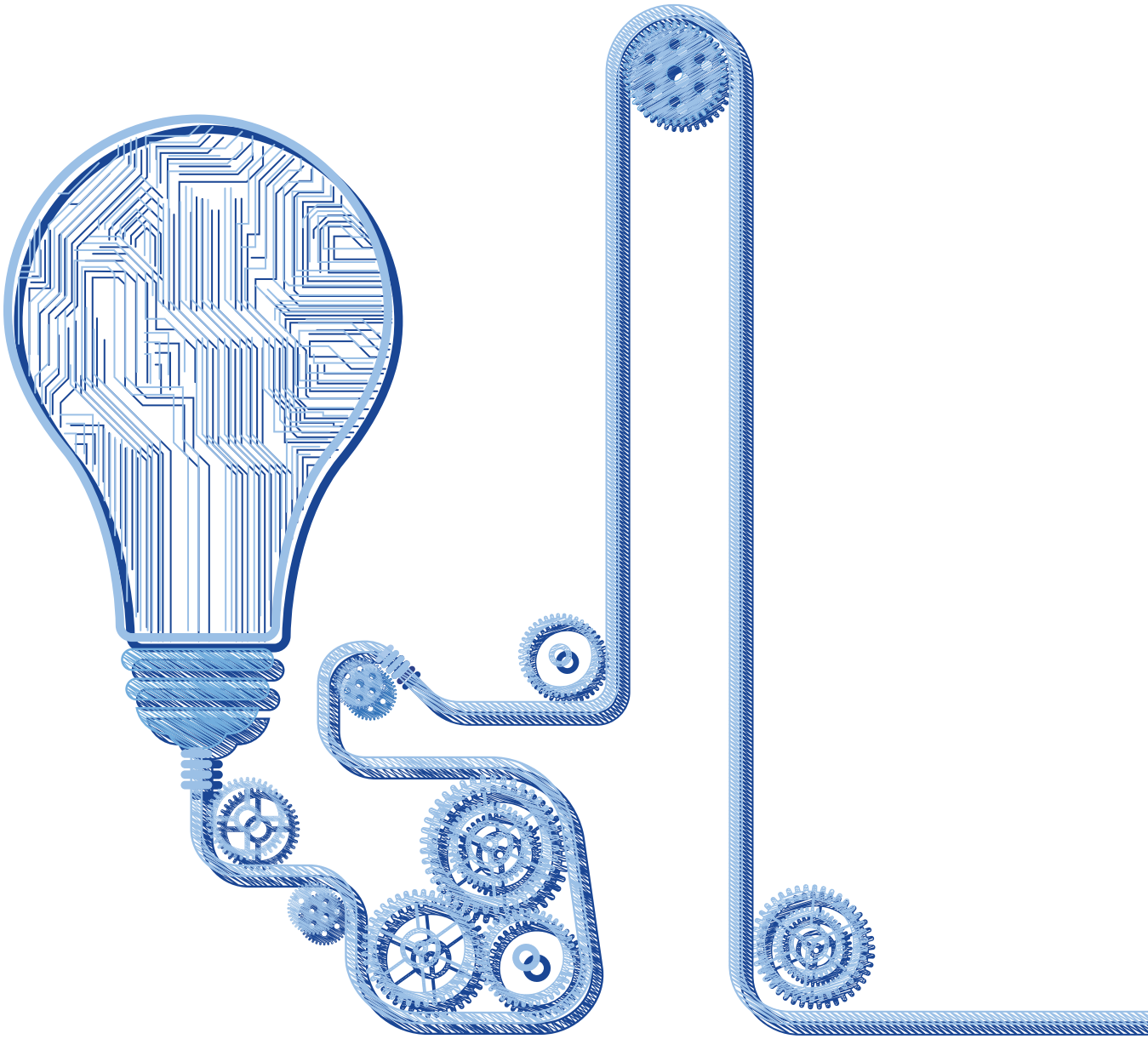
7.5 RECOMENDACIONES PARA LA ADOPCIÓN TECNOLÓGICA

La adopción tecnológica no debe entenderse como la mera adquisición de dispositivos, sino como un proceso planificado que abarque el diseño, la integración, la operación, el mantenimiento y la renovación de los sistemas. Las soluciones deberán responder a necesidades identificadas en el análisis de riesgos y aportar una mejora verificable. Para orientar este proceso se proponen las siguientes recomendaciones:

1. **Estrategia tecnológica adaptada**: Se deberá definir una estrategia de innovación y adopción tecnológica alineada con la tipología, los riesgos, el entorno y la complejidad del evento. El diseño partirá del análisis de riesgos y de las necesidades operativas, identificando para cada solución su finalidad, responsables, costes de ciclo de vida y criterios de evaluación, evitando la incorporación de tecnologías sin una utilidad suficientemente justificada.
2. **Interoperabilidad y estándares abiertos**: Se priorizarán tecnologías interoperables con los sistemas del evento y, cuando resulte necesario y autorizado, con las plataformas municipales, regionales y de seguridad pública. El empleo de estándares abiertos, interfaces documentadas y formatos normalizados facilita la integración y reduce la dependencia de proveedores concretos. La interoperabilidad deberá comprobarse mediante pruebas técnicas y operativas antes del evento.
3. **Privacidad y protección de datos**: El tratamiento de datos personales deberá ser lícito, proporcional y limitado a las finalidades definidas, aplicando la protección de datos desde el diseño y por defecto. Se realizará una evaluación de impacto cuando la naturaleza, el alcance o la tecnología empleada puedan implicar un alto riesgo para las personas. También deberán establecerse plazos de conservación, perfiles de acceso y medidas de seguridad adecuadas.
4. **Capacitación y formación especializada**: La eficacia de los sistemas tecnológicos depende de la competencia de las personas que los utilizan. El personal operativo y los responsables del centro de control recibirán formación adaptada a sus funciones para interpretar datos, verificar alertas y ejecutar los procedimientos establecidos. La capacitación incluirá ejercicios prácticos, gestión de falsas alarmas y actuación mediante procedimientos alternativos cuando las herramientas digitales no estén disponibles.
5. **Proyectos piloto, evaluación y escalabilidad**: Se recomienda validar las nuevas tecnologías mediante pruebas de concepto o proyectos piloto desarrollados en condiciones representativas. La evaluación deberá considerar su eficacia, fiabilidad, capacidad, falsas alarmas, usabilidad, mantenimiento, ciberseguridad e integración con los procedimientos existentes. Los resultados, incluidas las limitaciones detectadas, servirán para decidir su adopción, adaptación o descarte y para planificar un posible despliegue progresivo y escalable.

La validación técnica y operativa de este proceso contribuirá a que la tecnología actúe como un apoyo efectivo a la seguridad y a la toma de decisiones. La documentación de los criterios de selección, las pruebas realizadas, el mantenimiento y las responsabilidades facilitará la mejora continua y permitirá acreditar la diligencia de la organización, sin sustituir el cumplimiento de sus obligaciones legales.

8 RECOMENDACIONES FINALES, LECCIONES APRENDIDAS Y CONCLUSIONES



Los contenidos desarrollados en esta guía y los casos reales analizados en los apartados anteriores muestran que la seguridad de los eventos de masas depende de la combinación coordinada de planificación, organización, medios humanos, tecnología y capacidad de respuesta. Los incidentes más graves no suelen proceder de una única causa, sino de la acumulación de deficiencias técnicas, organizativas y operativas que no fueron detectadas o corregidas a tiempo.

Las siguientes recomendaciones sintetizan los principales criterios expuestos y ofrecen una referencia transversal para orientar la preparación, celebración y evaluación de los eventos. Su aplicación deberá adaptarse a la tipología, dimensión, emplazamiento, perfil de los asistentes y riesgos específicos de cada caso, evitando trasladar automáticamente soluciones adoptadas en otros contextos.

1. **Planificar a partir del riesgo**. Fundamentar la seguridad en un análisis actualizado de amenazas, vulnerabilidades, impactos y capacidades, adaptado a las características de cada evento.

2. **Integrar inteligencia y seguimiento**. Incorporar información previa y monitorizar dinámicamente el entorno para anticipar cambios, verificar alertas y detectar riesgos emergentes.

3. **Definir el mando y las responsabilidades**. Establecer una estructura clara de dirección, coordinación, toma de decisiones, comunicación y escalado desde la planificación inicial.

4. **Coordinar a todos los participantes**. Integrar a organizadores, administraciones, Fuerzas y Cuerpos de Seguridad, seguridad privada, protección civil, servicios sanitarios y operadores esenciales.

5. **Gestionar la ocupación y los movimientos**. Controlar aforos y flujos, prestando especial atención a accesos, salidas, recorridos de evacuación, nodos de transporte y espacios de transición.

6. **Comprobar instalaciones y sistemas críticos**. Inspeccionar antes de la apertura las infraestructuras, vías de evacuación, sistemas de seguridad, comunicaciones, iluminación y fuentes de energía de respaldo.

7. **Preparar comunicaciones resilientes**. Disponer de canales interoperables, redundantes y accesibles para los equipos y el público, con procedimientos alternativos ante saturación o pérdida de servicio.

8. **Utilizar la tecnología con supervisión humana**. Seleccionar soluciones proporcionadas, interoperables y ciberseguras que apoyen la decisión, manteniendo la verificación humana y la capacidad de operar en modo degradado.

9. **Ensayar la respuesta**. Realizar simulaciones y ejercicios que permitan comprobar la coordinación, la capacidad de intervención y evacuación y la eficacia de los procedimientos previstos.

10. **Aprender y mejorar después de cada evento**. Evaluar resultados e incidencias, documentar desviaciones, asignar medidas correctoras y compartir las lecciones obtenidas para mejorar futuros dispositivos.

La seguridad de un evento de masas no puede entenderse como un resultado estático ni como la consecuencia de una única medida. Es un proceso continuo que comienza con la identificación de los riesgos, se materializa mediante una planificación coordinada y se mantiene durante el evento mediante la observación, la comunicación y la capacidad de adaptación. La evaluación posterior y la incorporación sistemática de las lecciones aprendidas completan este ciclo y permiten avanzar hacia eventos más seguros, resilientes, inclusivos y preparados ante escenarios cambiantes.



9.1 GLOSARIO DE TÉRMINOS CLAVE

- **Aforo**: número máximo de personas autorizado para ocupar un recinto o espacio, determinado conforme a sus condiciones de uso, evacuación y normativa aplicable.
- **Ocupación**: número estimado o registrado de personas presentes en un espacio en un momento determinado, que puede controlarse globalmente o por sectores.
- **Gestión de multitudes**: conjunto de medidas de planificación, observación y actuación destinadas a ordenar los flujos, prevenir densidades peligrosas y proteger a las personas.
- **Incidente de presión de multitudes**: situación en la que la densidad, los movimientos colectivos o la configuración del espacio generan empujes, atrapamientos, caídas o compresiones peligrosas.
- **Centro de control**: instalación fija, temporal o móvil desde la que se recibe información, se supervisan los sistemas y se coordina la respuesta operativa del evento.
- **Plan de Autoprotección**: documento que establece los riesgos, medios, responsabilidades y procedimientos destinados a prevenir y responder ante emergencias, exigible en los supuestos establecidos por la normativa aplicable.
- **Interoperabilidad**: capacidad de diferentes sistemas, equipos y organizaciones para intercambiar información y utilizarla de forma coordinada, segura y conforme a sus competencias.
- **PSIM**: plataforma de gestión de seguridad que integra información y alertas de diferentes subsistemas en una interfaz común para apoyar la supervisión y la respuesta.
- **Gemelo digital**: representación estructurada y actualizable de un recinto, sus infraestructuras y condiciones operativas, utilizable para visualizar información y analizar escenarios.
- **UAS**: sistema de aeronave no tripulada, compuesto por la aeronave, sus elementos de control y los componentes necesarios para su operación.
- **IoT**: conjunto de sensores y dispositivos conectados que captan, transmiten o procesan información sobre ocupación, localización, condiciones ambientales u otras variables.
- **Analítica de vídeo**: procesamiento automatizado de imágenes para detectar determinados objetos, comportamientos o situaciones y generar alertas que deberán ser verificadas conforme a los procedimientos establecidos.

9.2 REFERENCIAS NORMATIVAS Y BIBLIOGRAFÍA

NORMATIVA ESTATAL

- Real Decreto 2816/1982, de 27 de agosto, por el que se aprueba el Reglamento General de Policía de Espectáculos Públicos y Actividades Recreativas, en aquello que permanezca vigente.
- Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección.
- Real Decreto 524/2023, de 20 de junio, por el que se aprueba la Norma Básica de Protección Civil.
- Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.
- Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
- Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 171/2004, de 30 de enero, en materia de coordinación de actividades empresariales.
- Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuando resulte aplicable.

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas.

NORMATIVA DE LA UNIÓN EUROPEA

- Reglamento (UE) 2016/679, Reglamento General de Protección de Datos.
- Reglamento (UE) 2019/947, relativo a las normas y procedimientos aplicables a la utilización de aeronaves no tripuladas.
- Reglamento Delegado (UE) 2019/945, sobre sistemas de aeronaves no tripuladas y operadores de terceros países.
- Directiva (UE) 2022/2555, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión — Directiva NIS2 —, y su normativa nacional de transposición.
- Directiva (UE) 2022/2557, relativa a la resiliencia de las entidades críticas — Directiva CER —, y su normativa nacional de transposición.
- Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial.

NORMATIVA AUTONÓMICA Y LOCAL

En cada evento deberá identificarse la normativa de la comunidad autónoma y del municipio correspondiente en materia de espectáculos públicos, actividades recreativas, emergencias, autoprotección, accesibilidad, contaminación acústica, movilidad, ocupación del espacio público, prevención de incendios y servicios sanitarios.

NORMAS Y ESTÁNDARES TÉCNICOS

- ISO 31000:2018, Risk management — Guidelines.
- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.
- ISO 22320:2018, Security and resilience — Emergency management — Guidelines for incident management.
- ISO 22322:2022, Security and resilience — Emergency management — Guidelines for public warning.
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- Serie IEC 62443, seguridad de sistemas de automatización y control industrial.

- ISO 22343-1 e ISO 22343-2, barreras de seguridad frente a vehículos: requisitos, ensayos, selección e instalación.
- Serie UNE-EN 54, sistemas de detección y alarma de incendios, en las partes que resulten aplicables.
- UNE-EN 50849, sistemas electroacústicos para servicios de emergencia.
- NFPA 101, Life Safety Code, como referencia técnica internacional cuando resulte pertinente.

METODOLOGÍAS DE ANÁLISIS Y PLANIFICACIÓN

- Ministerio de Hacienda y Administraciones Públicas. MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 3.
- Metodología CARVER, como herramienta complementaria para valorar criticidad, accesibilidad, recuperabilidad, vulnerabilidad, efecto y reconocibilidad frente a amenazas deliberadas.
- Metodologías de análisis de capacidad, intención o motivación y oportunidad del adversario para la evaluación de amenazas deliberadas.
- Modelos de análisis de flujos, densidad y dinámica de multitudes aplicables a la planificación y evacuación.

GUÍAS Y BUENAS PRÁCTICAS INTERNACIONALES

- Organización Mundial de la Salud. Public Health for Mass Gatherings: Key Considerations.
- Organización Mundial de la Salud. Documentos técnicos sobre preparación sanitaria, enfermedades transmisibles y gestión de riesgos en concentraciones multitudinarias.
- FIFA. Stadium Safety and Security Regulations y Football Stadiums Guidelines. Estas últimas incluyen específicamente la operación de seguridad de los estadios. FIFA Football Stadiums Guidelines.
- UEFA. Safety and Security Regulations, edición vigente.
- Sports Grounds Safety Authority. Guide to Safety at Sports Grounds — Green Guide.
- Events Industry Forum. The Purple Guide to Health, Safety and Welfare at Music and Other Events.
- NFPA. Guías y códigos de seguridad humana, protección contra incendios y gestión de ocupaciones multitudinarias.

FUENTES DE CASOS REALES

Para cada caso real citado en la guía se ha incluido preferentemente una resolución judicial, informe oficial, investigación administrativa, publicación de un organismo público o documento de una organización internacional. Las informaciones periodísticas se han utilizado únicamente como fuente complementaria.

9.3 ORGANISMOS Y ENTIDADES DE REFERENCIA

- **AES Fundación –Observatorio SEET**: conocimiento sectorial, colaboración público-privada y difusión de buenas prácticas sobre seguridad en eventos, espectáculos y destinos.
- **Dirección General de Protección Civil y Emergencias**: planificación, normativa y documentación técnica en materia de protección civil y autoprotección.
- **Delegaciones y Subdelegaciones del Gobierno**: coordinación estatal y autorización o seguimiento de determinados dispositivos de seguridad.
- **Comunidades autónomas y entidades locales**: órganos competentes en espectáculos públicos, emergencias, protección civil, movilidad, sanidad y ocupación del espacio público.
- **Fuerzas y Cuerpos de Seguridad**: coordinación de la seguridad ciudadana, orden público y respuesta ante amenazas deliberadas.
- **Centro Nacional de Protección de Infraestructuras Críticas (CNPIC):** referencia en protección de infraestructuras críticas cuando resulte aplicable.
- **Agencia Estatal de Seguridad Aérea (AESA):** normativa y requisitos aplicables a las operaciones con sistemas de aeronaves no tripuladas.
- **Agencia Española de Protección de Datos (AEPD)**: criterios sobre videovigilancia, biometría, geolocalización y tratamiento de datos personales.
- **Consejo Superior de Deportes y Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte**: referencias para competiciones y espectáculos deportivos.
- **Servicios públicos de emergencias y sanitarios**: coordinación territorial de la prevención, asistencia y respuesta ante incidentes.
- **Organizaciones y asociaciones profesionales**: apoyo técnico, formación especializada, elaboración de estándares y difusión de experiencias sectoriales.

Los datos concretos de contacto, responsables, canales de activación y procedimientos de comunicación deberán definirse y mantenerse actualizados en el Plan de Autoprotección y en el Plan de Comunicaciones de cada evento. Este apartado tiene carácter informativo y no sustituye a los canales oficiales de emergencia ni a los directorios operativos correspondientes.



Elaborada por el área de seguridad electrónica de AES y el Observatorio SEET impulsado por AES FUNDACIÓN

AES ASOCIACIÓN ESPAÑOLA EMPRESAS DE SEGURIDAD

AES FUNDACIÓN

C/Alcalá, 99 2ºA - 28009 Madrid

Telf. 915 765 225

www.aesseguridad.es / aes@aesseguridad.es

www.aesfundacion.es / patronato@aesfundacion.es

@aes_seguridad

ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD

aesseguridad2021

@FundacionAES

AES Fundación

aes_fundacion_