AES
FUNDACIÓN



Anexos

Guía de Seguridad en Eventos de Masas



ANEXO I

CHECKLIST OPERATIVO DE SEGURIDAD Y AUTOPROTECCIÓN DEL EVENTO

Datos de identificación	**4**
Antes del evento	**5**
Durante el evento	**9**
Finalización y fase posterior	**11**
Validación final	**12**

CHECKLIST OPERATIVO DE SEGURIDAD Y AUTOPROTECCIÓN DEL EVENTO

El presente checklist constituye una herramienta de apoyo para verificar la preparación y el seguimiento de las principales medidas organizativas, operativas y tecnológicas del evento. Deberá adaptarse a su tipología, dimensión, emplazamiento y nivel de riesgo, asignando responsables y dejando constancia de las comprobaciones realizadas y de las deficiencias detectadas.

Su utilización no sustituye al Plan de Autoprotección, a las autorizaciones administrativas pertinentes, a las inspecciones reglamentarias ni a los procedimientos de los servicios públicos intervinientes. Las desviaciones identificadas deberán corregirse antes de la apertura o, cuando no resulte posible, quedar evaluadas y acompañadas de medidas compensatorias expresamente aprobadas.

Datos de identificación

Campo	Información
Denominación del evento	
Organizador o promotor	
Lugar y recinto	
Fecha y horario	
Aforo autorizado	
Ocupación prevista	
Responsable del evento	
Dirección o coordinación de seguridad	
Responsable de autoprotección	
Responsable sanitario	
Responsable técnico	
Centro de control o puesto de coordinación	
Fecha de cumplimentación	
Responsable de la revisión	

CHECKLIST OPERATIVO DE SEGURIDAD Y AUTOPROTECCIÓN DEL EVENTO

Antes del evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o medida
1	Autorizaciones	Se dispone de las licencias, autorizaciones, seguros y comunicaciones administrativas exigibles.	Organización	Administración competente		
2	Planificación	El Plan de Autoprotección está actualizado, implantado y coordinado con los organismos competentes.	Responsable de autoprotección	Organización y servicios públicos		
3	Riesgos	El análisis contempla amenazas físicas, sociales, deliberadas, sanitarias, meteorológicas, tecnológicas y de continuidad.	Dirección de seguridad	Organización y responsables técnicos		
4	Inteligencia	Se ha recopilado y contrastado información sobre amenazas, convocatorias, entorno, antecedentes y colectivos de interés.	Dirección de seguridad	Fuerzas y Cuerpos de Seguridad		
5	Meteorología	Se han definido fuentes de información, umbrales y medidas ante calor, frío, lluvia, viento, tormentas u otros fenómenos.	Organización	Protección civil y responsable técnico		
6	Organización	El organigrama, la cadena de mando, las responsabilidades y los procedimientos de escalado están definidos y comunicados.	Dirección del evento	Todos los responsables		
7	Coordinación	Se ha celebrado una reunión operativa con los servicios públicos, seguridad privada, sanitarios y proveedores críticos.	Organización	Organismos intervinientes		

Antes del evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o medida
8	Personal	La dotación de seguridad, auxiliares, sanitarios y técnicos está dimensionada, acreditada, formada y distribuida por puestos.	Cada responsable funcional	Organización		
9	Aforo	Se han definido el aforo total, las capacidades sectorizadas y los procedimientos de conteo, cierre y reapertura de accesos.	Organización	Seguridad y control de accesos		
10	Accesos	Los carriles, filtros, acreditaciones y puestos de inspección están dimensionados para los flujos previstos.	Seguridad	Organización y personal auxiliar		
11	Flujos	Se han analizado entradas, salidas, circulaciones interiores, espacios de transición y conexiones con el transporte.	Organización	Seguridad, movilidad y emergencias		
12	Evacuación	Las salidas, recorridos, puertas y barras antipánico están identificados, señalizados, libres y operativos.	Responsable de autoprotección	Seguridad y responsable técnico		
13	Accesibilidad	Los accesos, recorridos, espacios seguros y medios de información contemplan las necesidades de personas con discapacidad.	Organización	Responsables técnicos y auxiliares		
14	Infraestructuras	Se han inspeccionado estructuras temporales, vallados, escenarios, gradas, cubiertas, anclajes y elementos suspendidos.	Responsable técnico	Instaladores y organización		

Antes del evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o medida
15	Incendios	Los sistemas de detección, alarma y extinción están accesibles, señalizados, mantenidos y comprobados.	Responsable técnico	Responsable de autoprotección		
16	Sanidad	Los recursos sanitarios, puestos asistenciales, ambulancias, accesos y rutas de evacuación sanitaria están preparados.	Responsable sanitario	Organización y emergencias		
17	Salud pública	Se han revisado agua, alimentos, higiene, saneamiento, residuos y medidas frente a riesgos epidemiológicos o intoxicaciones.	Organización	Servicios sanitarios y proveedores		
18	Comunicaciones	El Plan de Comunicaciones establece canales, grupos, prioridades, indicativos, responsables y procedimientos alternativos.	Dirección de seguridad	Todos los organismos		
19	Cobertura	Se han probado las radiocomunicaciones y redes de datos en zonas críticas, incluyendo sótanos y recorridos de evacuación.	Responsable de comunicaciones	Operadores y equipos intervinientes		
20	Red móvil	Se ha valorado con los operadores el refuerzo de cobertura o capacidad y la disponibilidad de comunicaciones para emergencias.	Organización	Operadores y servicios públicos		
21	Información pública	Están preparados y autorizados los mensajes de megafonía, pantallas, aplicaciones y canales institucionales.	Organización	Seguridad, emergencias y comunicación		

Antes del evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o medida
22	Tecnología	Cámaras, sensores, control de accesos, plataformas, drones y restantes sistemas han sido configurados y probados conjuntamente.	Responsable técnico	Seguridad y proveedores		
23	Ciberseguridad	Se han revisado inventario, credenciales, actualizaciones, segmentación, accesos remotos, registros y copias de respaldo.	Responsable tecnológico	Proveedores y dirección de seguridad		
24	Energía	Se han probado SAI, grupos electrógenos, alumbrado de emergencia, combustible, autonomía y conmutación de cargas.	Responsable técnico	Instaladores y organización		
25	Continuidad	Existen procedimientos manuales o alternativos ante fallos de energía, comunicaciones, control de accesos o plataforma central.	Dirección del evento	Responsables funcionales		
26	Centro de control	El centro está operativo, con puestos, planos, directorios, registros, comunicaciones y condiciones adecuadas de trabajo.	Dirección de seguridad	Responsables técnicos		
27	Simulacros	Se han realizado ejercicios o pruebas de los escenarios prioritarios y corregido las deficiencias detectadas.	Responsable de autoprotección	Todos los intervinientes		
28	Apertura	Se ha efectuado la inspección final y existe autorización expresa para abrir, con las incidencias pendientes evaluadas.	Dirección del evento	Responsables de seguridad y técnicos		

Estados: C = Conforme · NC = No conforme · P = Pendiente · NA = No aplicable.

Durante el evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o actuación
29	Mando	Los responsables están localizados y se mantienen activos los canales de coordinación y escalado.	Dirección del evento	Todos los responsables		
30	Personal	Los puestos están cubiertos y los relevos, descansos y reservas operativas se gestionan conforme a lo previsto.	Cada responsable funcional	Centro de control		
31	Ocupación	Se controla la ocupación total y por sectores, verificando las alertas y actuando antes de alcanzar niveles críticos.	Seguridad	Control de accesos y centro de control		
32	Flujos	Se supervisan accesos, salidas, colas, densidades y movimientos anómalos dentro y fuera del recinto.	Seguridad	Auxiliares, movilidad y centro de control		
33	Evacuación	Las salidas y recorridos permanecen libres, visibles, iluminados y operativos durante toda la actividad.	Seguridad	Responsable técnico		
34	Riesgos	Se actualiza la evaluación según la evolución del público, la meteorología, el entorno y las incidencias registradas.	Dirección de seguridad	Responsables funcionales		

Durante el evento

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o actuación
35	Sanidad	Se supervisan las asistencias, tiempos de respuesta, capacidad disponible y posibles patrones sanitarios anómalos.	Responsable sanitario	Centro de control		
36	Comunicaciones	Se comprueba periódicamente la disponibilidad de canales principales y alternativos y se registran las degradaciones.	Responsable de comunicaciones	Organismos intervinientes		
37	Información pública	Los mensajes son verificados, autorizados, accesibles y coherentes entre megafonía, pantallas, aplicaciones y redes oficiales.	Responsable de comunicación	Dirección y emergencias		
38	Sistemas críticos	Se monitorizan las alarmas, comunicaciones, energía, videovigilancia, accesos, sensores y plataformas tecnológicas.	Responsable técnico	Centro de control y proveedores		
39	Incidencias	Las alertas se verifican, clasifican, asignan y cierran conforme a los procedimientos, dejando trazabilidad suficiente.	Centro de control	Responsables intervinientes		
40	Medidas correctoras	Las desviaciones detectadas generan decisiones proporcionadas, responsables asignados y seguimiento hasta su resolución.	Dirección del evento	Responsables funcionales		

Estados: C = Conforme · NC = No conforme · P = Pendiente · NA = No aplicable.

Finalización y fase posterior

N.º	Ámbito	Comprobación	Responsable principal	Coordinación o participantes	Estado	Evidencia, incidencia o acción de mejora
41	Salida	Se mantiene el dispositivo hasta completar la dispersión del público y normalizar el entorno y el transporte.	Dirección del evento	Seguridad, movilidad y servicios públicos		
42	Desmontaje	El desmontaje y la retirada de equipos se realizan sin afectar a recorridos, servicios esenciales ni seguridad del entorno.	Responsable técnico	Proveedores y organización		
43	Incidencias	Se consolidan los registros operativos, sanitarios, técnicos y de seguridad conforme a los plazos aplicables.	Organización	Responsables funcionales		
44	Protección de datos	Se revisan la conservación, bloqueo, anonimización o eliminación de datos e imágenes conforme a su finalidad.	Responsable del tratamiento	Seguridad y responsable tecnológico		
45	Evaluación	Se celebra una reunión posterior con los actores principales para analizar resultados, desviaciones y coordinación.	Dirección del evento	Organismos y proveedores		
46	Acciones de mejora	Cada medida correctora dispone de responsable, prioridad, plazo y mecanismo de seguimiento.	Organización	Responsables afectados		
47	Lecciones aprendidas	Las conclusiones se incorporan a futuros análisis de riesgos, planes, procedimientos, formación y contrataciones.	Organización	Todos los participantes		

Estados: C = Conforme · NC = No conforme · P = Pendiente · NA = No aplicable.

Validación final

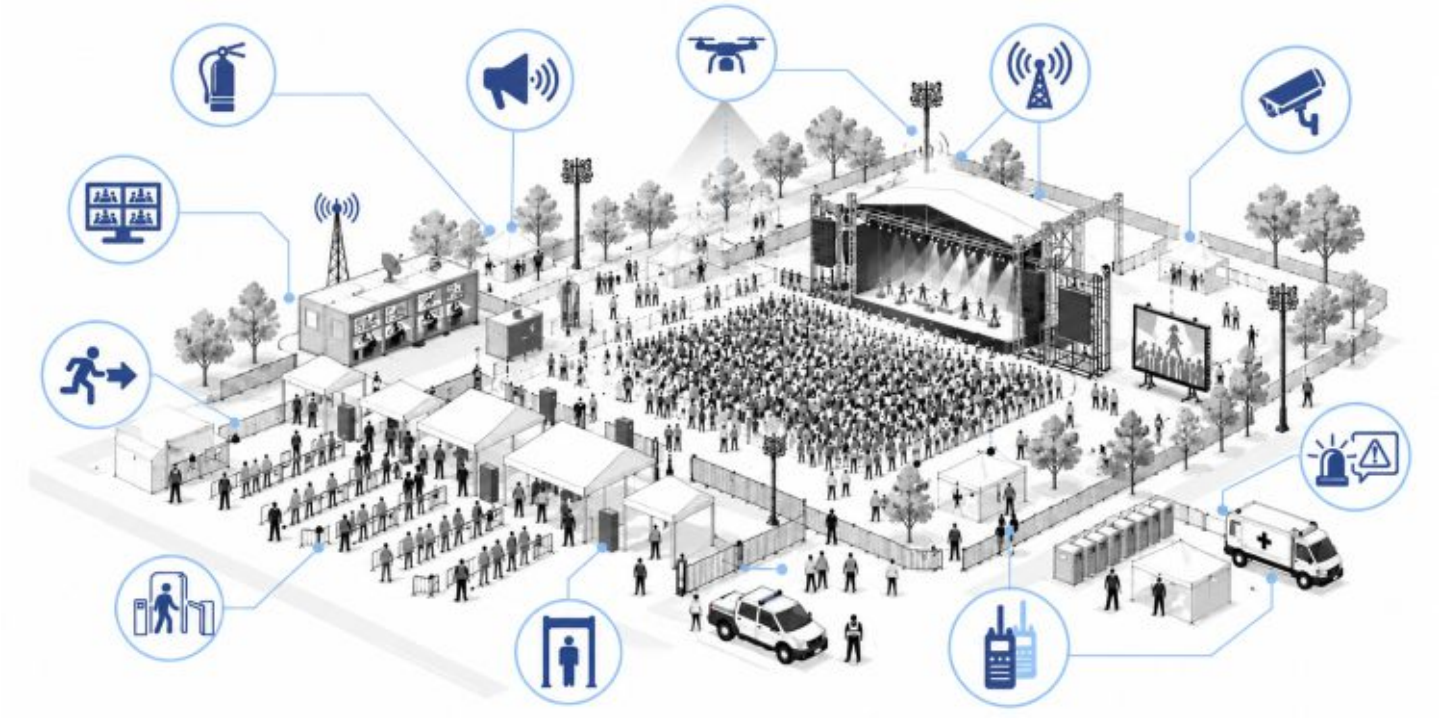
Resultado de la revisión	Identificación y firma	Fecha
Responsable del evento		
Dirección o coordinación de seguridad		
Responsable de autoprotección		
Responsable técnico		
Otros responsables intervinientes		



ANEXO II

CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS

Gestión digital de misiones y procedimientos operativos 16
Localización interior y exterior de personal y recursos 19
Verificación digital checklist y trazabilidad operativa 22
Videovigilancia inteligente y cámaras corporales 25
Torres autónomas de videovigilancia temporal 28
Sensorización IoT temporal y monitorización estructural 31
Control de accesos, acreditación y gestión de la ocupación 34
Protección frente a vehículos hostiles y control de accesos viarios 37
Detección no invasiva de amenazas y objetos prohibidos 40
Vigilancia aérea mediante uas convencionales y drones cautivos 43
Sistemas de detección y seguimiento de drones C-UAS 46
Monitorización meteorológica y alerta ambiental 49
Vigilancia sanitaria y detección temprana de patrones 52
Redes de conectividad y radiocomunicaciones de misión crítica 55
Megafonía, señalización, notificación masiva y app de emergencia 58
Energía de respaldo, iluminación y continuidad de servicio 61
Plataformas de gestión de seguridad integrada, PSIM 64
Gemelos digitales y simulación de escenarios 67
Redes interoperables y pasarelas de comunicación entre organismos 70
Plataformas de ciudad inteligente y gestión del entorno urbano 73



CATÁLOGO DE SOLUCIONES TECNOLÓGICAS APLICADAS A EVENTOS DE MASAS

Este anexo presenta una selección de soluciones tecnológicas aplicables a la prevención, supervisión y gestión de la seguridad en eventos de masas. Su finalidad es facilitar a organizadores, responsables de seguridad, administraciones, servicios de emergencia y personal técnico una visión práctica de las capacidades disponibles, sus posibles aplicaciones y los requisitos que deben valorarse antes de su implantación.

Las soluciones recogidas tienen carácter informativo y no constituyen una prescripción técnica, certificación, homologación ni recomendación comercial por parte de AES Fundación. Su inclusión tampoco implica que resulten necesarias o adecuadas para todos los eventos. La selección deberá partir del análisis de riesgos, las necesidades operativas, el entorno, la normativa aplicable y los recursos disponibles.

La tecnología debe complementar la planificación, los procedimientos y la actuación de los equipos humanos. Las alertas y resultados automatizados estarán sujetos a los mecanismos de verificación establecidos, especialmente cuando puedan originar actuaciones sobre los asistentes, los accesos, la evacuación o las comunicaciones públicas.

Las prestaciones indicadas deberán comprobarse para cada proyecto mediante documentación técnica, pruebas de funcionamiento y criterios de aceptación previamente definidos. Su eficacia puede variar según la configuración, las condiciones ambientales, la cobertura de comunicaciones, la calidad de los datos y la formación de los operadores.

Las denominaciones comerciales se limitarán a la identificación del proveedor o de la solución presentada. Las características se describirán de forma objetiva y comparable, evitando afirmaciones absolutas sobre precisión, disponibilidad, respuesta inmediata, cumplimiento legal o eliminación de riesgos.

GESTIÓN DIGITAL DE MISIONES Y PROCEDIMIENTOS OPERATIVOS

1 Definición y fundamentos técnicos

Concepto	Las plataformas de gestión digital de misiones son herramientas destinadas a organizar, asignar y supervisar las actuaciones de los equipos desplegados en un evento. Transforman los procedimientos operativos en tareas estructuradas, permitiendo conocer su responsable, prioridad, estado, ubicación y plazo de ejecución. No sustituyen las comunicaciones por voz ni la cadena de mando, sino que las complementan mediante un canal estructurado y trazable.
Principios de funcionamiento	La plataforma recibe avisos generados por operadores, sensores u otros sistemas y los convierte en misiones asociadas a procedimientos previamente configurados. Cada misión puede incluir instrucciones, nivel de prioridad, ubicación, recursos asignados, documentación y condiciones de cierre. Los equipos reciben las tareas en terminales móviles o puestos de operación y actualizan su estado mediante acciones como aceptación, llegada, intervención, solicitud de apoyo y cierre. La información se centraliza en el centro de control, desde donde se supervisa la carga de trabajo y la evolución de las incidencias.

2 Funcionalidades y capacidades

Prestaciones clave	• Creación manual o automática de avisos e incidencias. • Clasificación por tipología, gravedad, prioridad y ubicación. • Asignación de misiones a personas, equipos o perfiles funcionales. • Envío de instrucciones y procedimientos asociados. • Confirmación de recepción y aceptación de tareas. • Seguimiento de los estados de cada actuación. • Solicitud de apoyo, reasignación y escalado de incidencias. • Incorporación de fotografías, formularios, notas y otros datos. • Visualización de recursos e incidencias sobre planos o mapas. • Registro cronológico de comunicaciones y actuaciones. • Elaboración de informes operativos y análisis posterior. • Integración con PSIM, sensores, videovigilancia y sistemas de comunicaciones.
Diferenciación	Frente a la asignación exclusiva mediante radio o teléfono, la gestión digital estructura la información y reduce la necesidad de repetir datos, consultar instrucciones o reconstruir posteriormente las actuaciones. Permite que el centro de control conozca qué tareas permanecen pendientes, quién las está atendiendo y cuáles requieren apoyo. Su eficacia depende de una configuración adecuada, de la formación de los usuarios y de la existencia de procedimientos alternativos cuando la plataforma o las comunicaciones no estén disponibles.



3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Puede utilizarse en festivales, acontecimientos deportivos, ferias, celebraciones populares, procesiones, conciertos, carreras urbanas y otros eventos con numerosos equipos, áreas diferenciadas o incidencias simultáneas. Resulta especialmente útil cuando intervienen seguridad privada, personal auxiliar, equipos sanitarios, mantenimiento, producción y otros servicios que necesitan compartir información bajo una estructura común de coordinación.
Ejemplos de uso operativo	Ante una concentración anómala en un acceso, el centro de control registra la incidencia, asigna una misión al responsable del sector y adjunta las instrucciones aplicables. El equipo confirma la recepción, comprueba la situación y comunica si necesita refuerzos o una modificación de los flujos. La plataforma registra las decisiones y el cierre de la actuación. En una asistencia sanitaria, el operador puede registrar el punto aproximado, clasificar la prioridad y asignar el aviso al recurso correspondiente. Los datos personales y clínicos se limitarán a los estrictamente necesarios y se tratarán conforme a los procedimientos sanitarios y de protección de datos.

4 Beneficios para los actores del evento

Para el Promotor	Facilita la coordinación de los servicios contratados, el seguimiento de incidencias y la evaluación del dispositivo. La trazabilidad ayuda a identificar desviaciones, justificar decisiones y aplicar mejoras en eventos posteriores.
Para el Responsable de Seguridad	Proporciona una visión ordenada de las incidencias, recursos y tareas pendientes. Favorece la aplicación homogénea de los procedimientos, el escalado de situaciones críticas y la coordinación con otros responsables.
Para el Asistente	Puede contribuir a una atención más organizada y a reducir retrasos derivados de información incompleta, duplicada o transmitida al equipo equivocado.
Para la Administración	Facilita el intercambio de información operativa previamente acordada, la coordinación público-privada y el análisis posterior del evento, respetando las competencias y responsabilidades de cada organismo.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá disponer de gestión de usuarios y perfiles, clasificación de incidencias, motor de procedimientos, asignación de recursos, control de estados, registro temporal, cartografía y generación de informes. Las aplicaciones móviles deberán ser compatibles con los terminales previstos, presentar una interfaz sencilla y permitir al menos la recepción, aceptación, actualización y cierre de misiones. Las acciones con incidencia directa sobre accesos, evacuación, megafonía u otros sistemas críticos requerirán confirmación humana o mecanismos de seguridad específicos.
Infraestructura necesaria	Requiere servidores locales o servicios en la nube, conectividad segura, terminales para los usuarios y puestos de supervisión en el centro de control. El diseño deberá considerar la cobertura, capacidad, autonomía de los dispositivos y disponibilidad durante toda la operación. Se preverá un modo de funcionamiento degradado, almacenamiento temporal o procedimientos manuales ante pérdidas de red, plataforma o suministro eléctrico.
Estándares de interoperabilidad	La plataforma deberá disponer de API documentadas y mecanismos normalizados para intercambiar alertas, ubicaciones, estados y registros con sistemas PSIM, GIS, videovigilancia, control de accesos, sensores y comunicaciones. Las integraciones deberán definir formatos, frecuencia de actualización, autenticación, cifrado, gestión de errores y responsabilidades sobre cada dato.
Criterios de calidad y fiabilidad	- Disponibilidad y tiempos de recuperación. - Capacidad para gestionar usuarios e incidencias simultáneas. - Tiempo de entrega y confirmación de las misiones. - Claridad y facilidad de uso de las interfaces. - Trazabilidad de cambios y actuaciones. - Funcionamiento ante conectividad limitada. - Respaldo y recuperación de la información. - Gestión de falsas alarmas, duplicidades y tareas no atendidas. - Resultados de pruebas operativas con los equipos usuarios.
Compliance y seguridad	El sistema deberá aplicar control de acceso por perfiles, autenticación robusta, cifrado, registro de actividad, copias de respaldo, actualización de componentes y gestión de vulnerabilidades. Cuando trate datos personales o de localización, deberán aplicarse el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, utilizando únicamente la información necesaria y estableciendo plazos de conservación. El Esquema Nacional de Seguridad se aplicará cuando la organización o el servicio se encuentren dentro de su ámbito. Los registros aportan trazabilidad y permiten acreditar las actuaciones realizadas, pero su existencia no les confiere automáticamente valor probatorio ni supone un blindaje jurídico para la organización.



LOCALIZACIÓN INTERIOR Y EXTERIOR DE PERSONAL Y RECURSOS

1 Definición y fundamentos técnicos

Concepto	Los sistemas de localización interior y exterior permiten estimar la posición del personal de seguridad, equipos de intervención y determinados recursos operativos durante un evento. Facilitan la comprobación de puestos, la movilización de recursos próximos y el conocimiento de su última posición comunicada. La localización puede realizarse mediante terminales móviles, radios, dispositivos portátiles, etiquetas electrónicas o balizas. Su precisión y frecuencia de actualización dependen de la tecnología utilizada, la infraestructura desplegada y las condiciones del entorno.
Principios de funcionamiento	En espacios exteriores se utilizan habitualmente sistemas globales de navegación por satélite, como GPS o Galileo, complementados por redes móviles o de radiocomunicación para transmitir la posición. En interiores, donde la señal satelital puede ser insuficiente, pueden emplearse balizas Bluetooth, redes Wi-Fi, RFID, banda ultraancha u otras tecnologías de proximidad y posicionamiento. La plataforma calcula o estima la posición a partir de las señales recibidas y la representa sobre planos o mapas del evento. Los datos pueden integrarse con sistemas de gestión de misiones, PSIM o centros de control, indicando su hora de actualización y nivel estimado de precisión.

2 Funcionalidades y capacidades

Prestaciones clave	• Localización exterior mediante GNSS. • Posicionamiento interior mediante balizas o infraestructura dedicada. • Representación de personas y recursos sobre mapas y planos. • Consulta de la última posición comunicada. • Verificación de la cobertura de puestos operativos. • Identificación de recursos próximos a una incidencia. • Definición de zonas y generación de alertas de entrada o salida. • Seguimiento de recorridos durante intervenciones autorizadas. • Activación de avisos o botones de emergencia. • Asociación de terminales con funciones, equipos o turnos. • Integración con plataformas de misiones y centros de control. • Generación de históricos conforme a los plazos autorizados.
Diferenciación	Frente al control basado exclusivamente en comunicaciones por radio, la localización proporciona una referencia visual sobre la distribución de los recursos y reduce la necesidad de solicitar continuamente su posición. No acredita por sí sola que una persona esté desempeñando correctamente una función ni garantiza su ubicación exacta. Los datos deberán interpretarse considerando el margen de error, la última actualización, el estado del dispositivo y las posibles zonas sin cobertura.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta aplicable en festivales de gran extensión, estadios, pabellones, recintos feriales, procesiones, carreras urbanas y eventos distribuidos en varios espacios o niveles. Puede ser especialmente útil en instalaciones con numerosos accesos, salidas, sectores de público, aparcamientos, zonas técnicas o recorridos de evacuación en los que sea necesario verificar la distribución de los equipos.
Ejemplos de uso operativo	Antes de la apertura, el centro de control puede comprobar que los equipos asignados a accesos, salidas y zonas críticas han comunicado su llegada al puesto previsto. Si se detecta una ausencia, se contacta con el responsable y se reorganizan los recursos sin considerar automáticamente que el dato de posición confirma o descarta la presencia física. Ante una incidencia sanitaria, la plataforma puede mostrar los recursos disponibles próximos al punto comunicado. El operador verifica su estado y les asigna la intervención mediante los canales establecidos. En una evacuación, la última posición recibida puede ayudar a comprobar el repliegue de los equipos, pero deberá contrastarse mediante comunicaciones y recuentos operativos.

4 Beneficios para los actores del evento

Para el Promotor	Facilita el conocimiento de la distribución de los recursos contratados y la evaluación del despliegue previsto. Los datos agregados pueden contribuir a ajustar futuras dotaciones y recorridos.
Para el Responsable de Seguridad	Mejora la visión sobre la disponibilidad y posición estimada de los equipos, facilita la asignación del recurso adecuado y ayuda a detectar puestos sin cobertura o concentraciones de personal no previstas.
Para el Asistente	Puede contribuir a reducir el tiempo necesario para localizar y movilizar equipos de seguridad, sanitarios, auxiliares o técnicos ante una incidencia.
Para la Administración	Puede favorecer la coordinación entre dispositivos, siempre que el intercambio de posiciones esté autorizado, responda a una finalidad concreta y respete las competencias y procedimientos de cada organismo.



5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución podrá combinar terminales móviles, radios con posicionamiento, dispositivos portátiles, balizas interiores y una plataforma cartográfica. Deberá mostrar la identidad o función del recurso, su estado, la hora de actualización y, cuando sea posible, la precisión estimada. Las alertas de zona, inmovilidad o emergencia deberán configurarse conforme a procedimientos operativos y someterse a verificación antes de generar una intervención.
Infraestructura necesaria	En exteriores se requerirá cobertura de navegación por satélite y un medio para transmitir los datos. En interiores podrá ser necesario instalar balizas, antenas, puntos de acceso o nodos de localización, junto con planos correctamente georreferenciados. Los terminales deberán disponer de autonomía suficiente, elementos de recarga o baterías de sustitución. Se analizarán zonas de sombra, interferencias, obstáculos, densidad de dispositivos y funcionamiento ante pérdida de conectividad.
Estándares de interoperabilidad	La solución deberá permitir el intercambio seguro de posiciones, estados y alertas con plataformas GIS, PSIM y sistemas de gestión de misiones mediante API documentadas y formatos normalizados. La integración deberá conservar la marca temporal, la identificación del dispositivo, el sistema de coordenadas y la precisión asociada. Se definirán mecanismos para detectar datos desactualizados, posiciones imposibles o duplicidades.
Criterios de calidad y fiabilidad	• Precisión horizontal y, cuando proceda, vertical. • Frecuencia y retraso de actualización. • Cobertura efectiva interior y exterior. • Autonomía de terminales y balizas. • Capacidad para gestionar dispositivos simultáneos. • Disponibilidad y recuperación del servicio. • Comportamiento en zonas de sombra o alta densidad. • Detección de dispositivos desconectados. • Facilidad de uso y carga operativa. • Resultados de pruebas sobre el terreno.
Compliance y seguridad	La localización del personal implica tratamiento de datos personales y deberá contar con una finalidad legítima, conocida y proporcionada. Se informará a las personas afectadas sobre los datos recopilados, el periodo de utilización, los destinatarios y los plazos de conservación. El seguimiento se limitará al horario, ámbito y funciones relacionados con el evento. Se aplicarán perfiles de acceso, cifrado, registros de consulta y medidas contra la utilización de los datos para finalidades incompatibles. Cuando se compartan posiciones con otras organizaciones, deberán definirse previamente la base jurídica, los responsables, los usuarios autorizados y el nivel de detalle estrictamente necesario.



VERIFICACIÓN DIGITAL, CHECKLIST Y TRAZABILIDAD OPERATIVA

1 Definición y fundamentos técnicos

Concepto	Las herramientas de verificación digital permiten planificar, ejecutar y registrar inspecciones, comprobaciones y actuaciones operativas mediante formularios estructurados. Pueden utilizarse para revisar instalaciones, accesos, vías de evacuación, sistemas de seguridad, equipos y recursos antes, durante y después del evento. Estas herramientas sustituyen o complementan los formularios en papel y permiten asociar cada comprobación con un responsable, momento, ubicación, resultado y evidencia documental. El registro acredita que se realizó una actuación, pero no demuestra por sí mismo que el elemento inspeccionado funcionara correctamente.
Principios de funcionamiento	El sistema presenta al usuario listas de comprobación adaptadas a su función, zona o fase del evento. Cada punto puede requerir una respuesta, observación, fotografía, firma, lectura de código QR o NFC, geolocalización u otro mecanismo de confirmación. Los resultados se transmiten a una plataforma central donde pueden supervisarse las tareas pendientes, las deficiencias y las medidas correctoras. Los registros incorporan marcas temporales, identificación del usuario y un historial de cambios que facilita reconstruir la secuencia de actuaciones. La plataforma puede generar alertas, impedir el cierre de comprobaciones incompletas y escalar los incumplimientos conforme a reglas previamente definidas.

2 Funcionalidades y capacidades

Prestaciones clave	• Creación de listas adaptadas al tipo de evento y perfil del usuario. • Programación de inspecciones y comprobaciones periódicas. • Asignación de tareas por zonas, equipos o responsables. • Registro de resultados conformes, no conformes o no aplicables. • Incorporación de observaciones, fotografías y documentos. • Identificación de equipos mediante códigos QR, NFC u otras etiquetas. • Registro de fechas, horas, usuarios y modificaciones. • Generación de avisos ante incumplimientos o tareas vencidas. • Asignación y seguimiento de medidas correctoras. • Consulta de verificaciones desde el centro de control. • Elaboración de informes y exportación de resultados. • Funcionamiento sin conexión con sincronización posterior, cuando proceda.
Diferenciación	Frente a las listas en papel, la verificación digital facilita la actualización de contenidos, evita formularios incompletos y permite conocer el avance de las inspecciones sin recopilar físicamente los documentos. También mejora la clasificación de incidencias y el seguimiento de las correcciones. Su fiabilidad depende de la calidad de las preguntas, la competencia de quien inspecciona y la comprobación efectiva realizada. Una fotografía, una etiqueta NFC o una marca temporal aportan trazabilidad, pero no sustituyen el juicio técnico ni certifican automáticamente el estado del elemento.



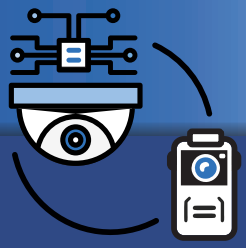
3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Puede utilizarse en conciertos, festivales, acontecimientos deportivos, ferias, procesiones, celebraciones urbanas y montajes temporales. Resulta útil cuando intervienen distintos contratistas o deben verificarse numerosos espacios en periodos reducidos. Sus aplicaciones comprenden las fases de montaje, apertura, celebración, cierre y desmontaje, así como las revisiones periódicas realizadas durante eventos de varios días.
Ejemplos de uso operativo	Antes de la apertura, los responsables recorren sus sectores y comprueban puertas, barras antipánico, señalización, alumbrado, extintores, comunicaciones y ausencia de obstáculos. Las deficiencias se remiten al responsable correspondiente, que documenta su corrección o propone una medida compensatoria para su aprobación. Durante el evento, el personal puede registrar comprobaciones periódicas de salidas, vallados, cuadros eléctricos, grupos electrógenos o puestos sanitarios. Una incidencia crítica genera un aviso al centro de control y permanece abierta hasta que un responsable autorizado verifica su resolución.

4 Beneficios para los actores del evento

Para el Promotor	Proporciona una visión consolidada del estado de preparación y facilita el seguimiento de contratistas, inspecciones y medidas correctoras. La documentación generada puede acreditar la diligencia organizativa, sin constituir un blindaje frente a responsabilidades.
Para el Responsable de Seguridad	Permite conocer qué áreas han sido revisadas, qué deficiencias siguen pendientes y quién debe resolverlas. Facilita la priorización de actuaciones y la decisión sobre apertura, restricción o aplicación de medidas compensatorias.
Para el Asistente	Contribuye a que instalaciones, recorridos y sistemas críticos sean revisados de forma ordenada, reduciendo la posibilidad de que una deficiencia conocida permanezca sin tratamiento.
Para la Administración	Facilita la consulta o entrega de información estructurada cuando esté prevista, manteniendo diferenciadas las comprobaciones internas de las inspecciones, autorizaciones y controles que correspondan a la autoridad competente.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir gestión de formularios, usuarios, perfiles, calendarios, zonas, activos, resultados y medidas correctoras. Permitirá establecer campos obligatorios, niveles de prioridad, responsables, plazos y condiciones de cierre. Los registros deberán conservar su autoría, marca temporal e historial de modificaciones. Las fotografías y documentos se vincularán con la comprobación correspondiente, evitando archivos aislados o sin contexto.
Infraestructura necesaria	Requiere terminales móviles o tabletas, una plataforma central y conectividad suficiente para sincronizar los datos. Cuando existan zonas sin cobertura, deberá contemplarse la cumplimentación fuera de línea y la transmisión posterior sin pérdida de información. Las etiquetas QR o NFC, si se utilizan, deberán instalarse en emplazamientos accesibles, protegidos y vinculados correctamente con el activo. También deberán preverse terminales de reserva, sistemas de recarga y procedimientos manuales ante indisponibilidad prolongada.
Estándares de interoperabilidad	La plataforma deberá permitir exportar formularios, incidencias, evidencias y estados mediante formatos documentados. Podrá integrarse con sistemas de gestión de activos, mantenimiento, PSIM, GIS y plataformas de gestión operativa. Las interfaces deberán conservar identificadores, versiones, marcas temporales y relaciones entre inspecciones y medidas correctoras. La integración no deberá permitir que una incidencia se cierre automáticamente sin la validación establecida.
Criterios de calidad y fiabilidad	• Facilidad de creación y actualización de formularios. • Claridad de las instrucciones para cada comprobación. • Funcionamiento en línea y fuera de línea. • Trazabilidad de altas, cambios y cierres. • Integridad y recuperación de los registros. • Capacidad para gestionar usuarios simultáneos. • Generación y escalado de alertas. • Tiempo de sincronización. • Exportación de datos e informes. • Usabilidad con equipos de protección y en condiciones ambientales adversas.
Compliance y seguridad	El tratamiento de nombres, ubicaciones, firmas, fotografías y registros deberá respetar la normativa de protección de datos. Solo se recopilará la información necesaria y se establecerán perfiles de acceso, plazos de conservación y mecanismos de bloqueo o eliminación. La plataforma deberá aplicar autenticación segura, cifrado, copias de respaldo, registro de accesos y protección frente a modificaciones no autorizadas. La integridad técnica de un registro no determina automáticamente su valor probatorio, que dependerá de su obtención, conservación, contexto y eventual cadena de custodia.



VIDEOVIGILANCIA INTELIGENTE Y CÁMARAS CORPORALES

1 Definición y fundamentos técnicos

Concepto	La videovigilancia inteligente combina cámaras fijas, móviles o corporales con sistemas de gestión de vídeo y algoritmos de análisis de imágenes. Permite supervisar espacios, detectar situaciones previamente definidas y generar alertas para su verificación por los operadores. Las cámaras corporales registran las intervenciones desde la perspectiva del personal autorizado y pueden integrarse con el centro de control. Ambas tecnologías deben responder a finalidades concretas y utilizarse con supervisión humana.
Principios de funcionamiento	Las cámaras captan secuencias que se procesan localmente, en servidores o en la nube. Los algoritmos identifican objetos, movimientos o patrones y generan alertas cuando se cumplen determinadas condiciones. Las cámaras corporales pueden activarse manualmente, mediante un pulsador de emergencia o a partir de reglas autorizadas. Las imágenes se transmiten o almacenan aplicando controles de acceso, integridad y conservación.

2 Funcionalidades y capacidades

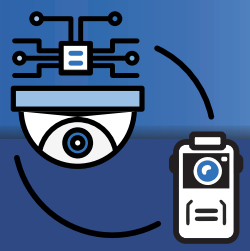
Prestaciones clave	• Conteo y estimación de la ocupación. • Análisis de densidades y mapas de calor. • Detección de movimientos en direcciones no previstas. • Identificación de carreras, caídas, peleas o permanencias prolongadas. • Detección de humo, intrusiones u objetos abandonados. • Búsqueda posterior por atributos visuales no biométricos. • Seguimiento entre cámaras compatibles. • Verificación visual de alarmas procedentes de otros sensores. • Grabación de intervenciones mediante cámaras corporales. • Activación coordinada con alarmas o pulsadores. • Transmisión segura al centro de control. • Generación de registros para el análisis posterior.
Diferenciación	Frente a la observación exclusiva de múltiples pantallas, la analítica ayuda a dirigir la atención hacia situaciones relevantes y reduce la dependencia de una vigilancia visual continua. Las cámaras corporales aportan contexto sobre determinadas intervenciones y pueden favorecer la trazabilidad. Las alertas no constituyen una confirmación automática del incidente. Su precisión depende de la ubicación de las cámaras, la iluminación, la densidad, las oclusiones, la configuración y las condiciones ambientales.

3 Aplicaciones y casos de uso en eventos

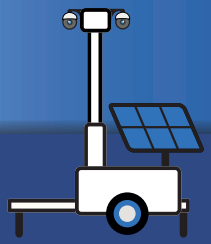
Escenarios de aplicación	Puede utilizarse en accesos, zonas de público, perímetros, aparcamientos, áreas restringidas, recorridos de evacuación y espacios de transición. Resulta aplicable a estadios, festivales, conciertos, ferias y celebraciones urbanas. Las cámaras corporales pueden emplearse por personal autorizado en controles de acceso, patrullas, intervenciones o atención de incidencias, conforme a procedimientos previamente definidos.
Ejemplos de uso operativo	Cuando el sistema detecta un incremento de densidad en un acceso, genera una alerta y muestra las cámaras relacionadas. El operador verifica la situación y puede solicitar la regulación del flujo o el envío de personal. Ante la comunicación de una persona extraviada, la búsqueda por color de ropa, dirección o franja temporal puede ayudar a revisar las grabaciones. Los resultados deberán comprobarse antes de movilizar recursos. Durante una intervención, una cámara corporal puede registrar la actuación conforme al protocolo establecido. La grabación aporta información contextual, pero su valor probatorio dependerá de las condiciones de obtención, conservación y eventual cadena de custodia.

4 Beneficios para los actores del evento

Para el Promotor	Amplía la capacidad de supervisión, facilita el análisis de incidencias y permite adaptar el despliegue de recursos. La información obtenida puede apoyar la evaluación posterior del evento.
Para el Responsable de Seguridad	Ayuda a detectar concentraciones, intrusiones y comportamientos que requieren atención. La integración de alarmas e imágenes facilita su verificación y la coordinación de la respuesta.
Para el Asistente	Puede contribuir a la detección temprana de situaciones de riesgo, a la localización de personas extraviadas y a una respuesta más ordenada ante incidencias.
Para la Administración	Facilita el intercambio autorizado de imágenes o alertas relevantes y aporta información para analizar flujos e incidentes, respetando las competencias y la protección de datos.



5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir cámaras adecuadas al entorno, gestión de vídeo, almacenamiento, analíticas configurables y herramientas de supervisión. Se definirán resolución, campo de visión, frecuencia de imagen, iluminación y periodo de conservación según cada finalidad. Las cámaras corporales deberán incorporar controles de activación, señalización de grabación, identificación del dispositivo, protección frente a manipulaciones y descarga segura.
Infraestructura necesaria	Requiere soportes, energía, comunicaciones y capacidad de procesamiento y almacenamiento. Las instalaciones temporales deberán considerar estabilidad, climatología, iluminación, cobertura y protección física. Se preverá grabación local o funcionamiento degradado ante pérdida de conectividad, así como terminales, baterías y sistemas de recarga para las cámaras corporales.
Estándares de interoperabilidad	Se recomienda compatibilidad con protocolos de vídeo IP, como ONVIF, y API documentadas para intercambiar vídeo, alarmas y estados con VMS, PSIM y plataformas operativas. La integración deberá conservar identificadores, marcas temporales y niveles de prioridad, evitando actuaciones automáticas sobre sistemas críticos sin la validación prevista.
Criterios de calidad y fiabilidad	• Cobertura y calidad de las imágenes. • Precisión de cada analítica. • Tasas de falsas alarmas y omisiones. • Latencia de transmisión y generación de avisos. • Capacidad con cámaras y usuarios simultáneos. • Disponibilidad y recuperación del sistema. • Autonomía de cámaras corporales. • Integridad, exportación y recuperación de grabaciones. • Funcionamiento con alta densidad, ruido visual o iluminación variable.
Compliance y seguridad	El tratamiento de imágenes deberá cumplir el RGPD, la legislación nacional de protección de datos y la normativa de seguridad privada aplicable. Se definirán finalidad, zonas captadas, información a los afectados, usuarios autorizados y plazos de conservación. La biometría o identificación individual requerirá una evaluación jurídica específica y no deberá activarse por defecto. La plataforma aplicará autenticación, cifrado, registros de acceso, actualización segura y protección frente a extracciones o modificaciones no autorizadas.



TORRES AUTÓNOMAS DE VIDEOVIGILANCIA TEMPORAL

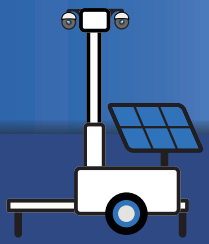
1 Definición y fundamentos técnicos

Concepto	Las torres autónomas de videovigilancia son sistemas móviles diseñados para supervisar temporalmente espacios sin infraestructura fija suficiente. Integran en un único conjunto cámaras, sensores, comunicaciones, almacenamiento y alimentación propia. Pueden desplegarse durante el montaje, celebración y desmontaje del evento para proteger perímetros, accesos secundarios, aparcamientos, zonas técnicas o áreas de almacenamiento.
Principios de funcionamiento	Las cámaras y detectores instalados sobre una torre o mástil captan imágenes y generan alertas ante movimientos, intrusiones o patrones configurados. La analítica puede diferenciar categorías básicas, como personas o vehículos, y enviar los avisos a un centro de control para su verificación. La energía se obtiene habitualmente mediante paneles solares y baterías, aunque puede complementarse con red eléctrica o generación auxiliar. Las comunicaciones utilizan redes móviles u otros enlaces inalámbricos, mientras que la grabación local permite conservar imágenes cuando se pierde la conectividad.

2 Funcionalidades y capacidades

Prestaciones clave	• Vigilancia temporal de perímetros y espacios exteriores. • Captación de vídeo fijo, panorámico o móvil. • Detección de personas, vehículos e intrusiones. • Verificación visual de alarmas. • Analítica para reducir avisos causados por fauna o vegetación. • Grabación local y transmisión remota. • Consulta de imágenes bajo demanda. • Supervisión del estado de baterías y comunicaciones. • Armado y desarmado remoto. • Integración con centros de control, VMS o PSIM. • Alimentación autónoma o híbrida. • Reubicación y reutilización en distintos emplazamientos.
Diferenciación	Frente a una instalación fija, estas torres reducen la necesidad de obra civil, cableado y acometidas permanentes. Su movilidad permite adaptar la vigilancia a los cambios del recinto y proteger también las fases de montaje y desmontaje. No sustituyen automáticamente la vigilancia presencial. Su eficacia depende del emplazamiento, el campo de visión, la estabilidad, la iluminación, la cobertura de comunicaciones, la autonomía energética y los procedimientos de respuesta disponibles.

TORRES AUTÓNOMAS DE VIDEOVIGILANCIA TEMPORAL



3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resultan adecuadas para festivales, conciertos, ferias, acontecimientos deportivos y celebraciones en espacios abiertos o recintos temporales. Pueden emplearse en perímetros extensos, aparcamientos, accesos de servicio, áreas VIP, zonas de proveedores y espacios técnicos. También pueden reforzar temporalmente instalaciones cuya videovigilancia permanente no cubra la configuración específica del evento.
Ejemplos de uso operativo	Durante el montaje, una torre supervisa el área de almacenamiento de equipos. Cuando los sensores detectan una entrada fuera del horario autorizado, la cámara envía imágenes al centro de control. El operador verifica la alerta y activa el procedimiento previsto. Durante el evento, otra unidad vigila un acceso secundario y permite comprobar concentraciones, aperturas no autorizadas o movimientos de vehículos. Si se pierde la red móvil, el sistema mantiene la grabación local y comunica la incidencia cuando recupera la conexión.

4 Beneficios para los actores del evento

Para el Promotor	Permite reforzar la protección sin ejecutar instalaciones permanentes y reutilizar los equipos en distintas fases o emplazamientos. Puede reducir tiempos de implantación y adaptar la inversión a la duración del evento.
Para el Responsable de Seguridad	Amplía la supervisión de zonas alejadas o con poca infraestructura y facilita la verificación remota de alarmas. La movilidad permite modificar el despliegue cuando cambia la configuración del recinto.
Para el Asistente	Contribuye a la vigilancia de aparcamientos, accesos y espacios comunes y puede favorecer una detección más temprana de determinadas incidencias.
Para la Administración	Facilita el despliegue temporal de medios de vigilancia y su integración autorizada con los dispositivos de coordinación, sin generar necesariamente infraestructura permanente en el espacio público.

5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	La solución deberá integrar una estructura estable para exteriores, cámaras adecuadas al escenario, sensores, grabación local, comunicaciones seguras y supervisión del estado del equipo. La autonomía se dimensionará según consumos, radiación solar prevista y duración de la operación. Podrá incorporar iluminación auxiliar, altavoz, cámara térmica o detección volumétrica cuando el análisis de riesgos lo justifique.
Infraestructura necesaria	Requiere una superficie estable, espacio de seguridad, campo de visión suficiente y cobertura de comunicaciones. El estudio previo deberá considerar viento, sombras, obstáculos, orientación solar, riesgo de impacto y acceso para mantenimiento. Se preverán procedimientos de recarga, sustitución de baterías, conexión auxiliar y recuperación ante fallos de energía o comunicaciones.
Estándares de interoperabilidad	Se recomienda compatibilidad con ONVIF y protocolos IP seguros, así como API documentadas para integrar vídeo, alarmas y estado del equipo con VMS, PSIM y plataformas de gestión. La solución deberá sincronizar sus marcas temporales y permitir exportar grabaciones y eventos en formatos utilizables por los sistemas autorizados.
Criterios de calidad y fiabilidad	• Estabilidad y resistencia frente a condiciones meteorológicas. • Cobertura, resolución y calidad de imagen. • Autonomía energética en condiciones desfavorables. • Capacidad de almacenamiento local. • Disponibilidad de las comunicaciones. • Precisión y falsas alarmas de las analíticas. • Tiempo de despliegue y recuperación. • Supervisión de baterías, sensores y enlaces. • Funcionamiento ante pérdida de conectividad. • Facilidad de mantenimiento y reubicación.
Compliance y seguridad	La instalación deberá cumplir los requisitos de seguridad estructural, eléctrica, compatibilidad electromagnética y marcado CE aplicables. Su ubicación no deberá obstruir recorridos ni generar riesgos por vuelco, impacto o acceso no autorizado. La captación de imágenes se ajustará a la normativa de protección de datos y seguridad privada. Se definirán zonas de visión, información al público, usuarios autorizados y conservación de grabaciones. Las comunicaciones y accesos remotos deberán estar cifrados, autenticados y registrados.

SENSORIZACIÓN IOT TEMPORAL Y MONITORIZACIÓN ESTRUCTURAL



1 Definición y fundamentos técnicos

Concepto	La sensorización IoT temporal comprende dispositivos conectados que miden variables del entorno, detectan cambios de estado o permiten emitir avisos desde diferentes puntos del evento. Su despliegue portátil facilita cubrir espacios sin instrumentación permanente. Puede incluir sensores ambientales, acústicos, estructurales, de ocupación, apertura, movimiento o presencia, además de balizas y pulsadores de emergencia.
Principios de funcionamiento	Los sensores transforman una magnitud física en datos digitales y los transmiten a una plataforma mediante redes como LoRaWAN, telefonía móvil, Wi-Fi, Bluetooth u otros protocolos inalámbricos. La plataforma compara las mediciones con umbrales previamente definidos, representa su evolución y genera alertas ante desviaciones. Los sensores estructurales pueden registrar inclinación, vibración, desplazamiento o deformación en elementos temporales, sin sustituir las inspecciones y certificaciones técnicas exigibles.

2 Funcionalidades y capacidades

Prestaciones clave	• Medición de temperatura, humedad y calidad del aire. • Supervisión de niveles sonoros. • Detección de humo, gases o sustancias específicas. • Control de apertura, movimiento o intrusión. • Medición de inclinación, vibración o deformación. • Avisos sobre viento en escenarios y estructuras temporales. • Pulsadores portátiles para emergencias médicas o de seguridad. • Detección de presencia u ocupación en zonas determinadas. • Identificación de equipos mediante balizas. • Generación de alertas por umbrales. • Representación de datos sobre mapas y cuadros de mando. • Funcionamiento autónomo mediante baterías.
Diferenciación	Frente a las inspecciones puntuales, los sensores permiten observar continuamente la evolución de determinadas variables y detectar cambios entre revisiones. Su carácter portátil facilita adaptar la instrumentación a la configuración temporal del evento. Las mediciones no constituyen por sí solas un diagnóstico estructural, sanitario o policial. Las alertas deberán verificarse y asociarse a procedimientos que establezcan responsables, umbrales y actuaciones.



SENSORIZACIÓN IOT TEMPORAL Y MONITORIZACIÓN ESTRUCTURAL

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Puede utilizarse en festivales, ferias, conciertos, estadios, carpas, escenarios, gradas temporales, zonas de restauración, aparcamientos y espacios con condiciones ambientales cambiantes. Resulta especialmente útil en eventos al aire libre, instalaciones provisionales o zonas alejadas del centro de control en las que sea difícil realizar comprobaciones frecuentes.
Ejemplos de uso operativo	Un sensor instalado en una estructura temporal detecta un incremento de inclinación o vibración superior al umbral definido. El sistema genera una alerta, el responsable técnico inspecciona el elemento y determina si procede limitar el uso, reforzarlo o desalojar preventivamente la zona. En una carpa, varios sensores registran temperatura, humedad y concentración de determinados gases. La evolución conjunta permite advertir condiciones desfavorables y activar medidas como ventilación, reducción de ocupación o intervención técnica. Los pulsadores portátiles pueden permitir que el personal comunique una necesidad médica o de seguridad, identificando el dispositivo y la zona aproximada desde la que se emite el aviso.

4 Beneficios para los actores del evento

Para el Promotor	Permite desplegar monitorización temporal sin realizar instalaciones permanentes y facilita el seguimiento de condiciones ambientales, técnicas y operativas durante las distintas fases del evento.
Para el Responsable de Seguridad	Aporta alertas sobre cambios que pueden no ser visibles desde el centro de control y ayuda a priorizar inspecciones, movilizar recursos y comprobar la evolución de una incidencia.
Para el Asistente	Puede contribuir a detectar tempranamente condiciones ambientales adversas, fallos técnicos o necesidades de asistencia y favorecer una respuesta más rápida.
Para la Administración	Facilita la disponibilidad de datos agregados sobre ruido, ambiente u otras variables, siempre que su intercambio esté autorizado y se utilicen equipos adecuados para la finalidad prevista.



SENSORIZACIÓN IOT TEMPORAL Y MONITORIZACIÓN ESTRUCTURAL

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir sensores adecuados a cada magnitud, alimentación autónoma, comunicaciones, identificación individual y plataforma de supervisión. Cada dispositivo deberá informar de su estado, batería, última comunicación y calidad de señal. Los umbrales se definirán mediante criterios técnicos y operativos. Los sensores destinados a detectar sustancias deberán considerarse herramientas de indicación preliminar, sujetas a confirmación mediante procedimientos y equipos autorizados.
Infraestructura necesaria	El despliegue requiere estudiar ubicación, cobertura, fijación, protección frente a golpes, condiciones meteorológicas y acceso para mantenimiento. Podrán ser necesarias pasarelas de comunicaciones o repetidores para concentrar los datos. Se preverán baterías de sustitución, calibración, inventario, retirada posterior y procedimientos manuales cuando se pierdan sensores o comunicaciones.
Estándares de interoperabilidad	La solución deberá utilizar protocolos documentados y permitir el intercambio de mediciones, alarmas y estados con plataformas IoT, GIS, PSIM y sistemas de gestión operativa. Los datos deberán incorporar unidad de medida, ubicación, identificador, marca temporal, estado de calibración y nivel de calidad. Se evitará depender de formatos propietarios sin posibilidad de exportación.
Criterios de calidad y fiabilidad	• Rango, resolución y precisión de medida. • Frecuencia de muestreo y transmisión. • Tiempo de generación de alertas. • Autonomía y estado de las baterías. • Cobertura y pérdida de comunicaciones. • Resistencia ambiental y mecánica. • Estabilidad y deriva de los sensores. • Necesidades de calibración. • Tasas de falsas alarmas y omisiones. • Recuperación de datos almacenados localmente.
Compliance y seguridad	Los dispositivos deberán cumplir los requisitos aplicables de marcado CE, compatibilidad electromagnética, equipos radioeléctricos y seguridad eléctrica. En atmósferas con riesgo específico se utilizarán equipos adecuados al entorno. Cuando los datos permitan localizar o identificar personas, se aplicará la normativa de protección de datos. Las comunicaciones deberán estar autenticadas y cifradas, y la plataforma contará con control de accesos, actualizaciones seguras y protección frente a la manipulación de mediciones o alertas.



CONTROL DE ACCESOS, ACREDITACIÓN Y GESTIÓN DE LA OCUPACIÓN

1 Definición y fundamentos técnicos

Concepto	Estos sistemas permiten validar entradas y acreditaciones, registrar movimientos y estimar la ocupación total o sectorizada de un evento. Pueden combinar tornos, lectores portátiles, cámaras de conteo y plataformas de gestión. Las credenciales pueden emplear códigos de barras o QR, NFC, RFID u otras tecnologías. Su función es verificar los permisos asociados, sin garantizar por sí solas la identidad, presencia o ubicación real de una persona.
Principios de funcionamiento	Cada entrada o acreditación contiene un identificador que el sistema contrasta con una base de datos. La validación comprueba su vigencia, permisos, horario, zona autorizada y posibles usos anteriores. Los registros de entrada y salida, combinados con sensores o cámaras de conteo, permiten estimar la ocupación. Las reglas de control de reutilización pueden detectar duplicidades o intentos de acceder varias veces con la misma credencial.

2 Funcionalidades y capacidades

Prestaciones clave	• Emisión y validación de entradas y acreditaciones. • Asignación de permisos por zonas y horarios. • Lectura mediante tornos o terminales portátiles. • Registro de entradas, salidas y rechazos. • Control de reutilización de credenciales. • Estimación de ocupación total y por sectores. • Alertas por aproximación a umbrales establecidos. • Gestión de listas, invitaciones y acreditaciones profesionales. • Apertura o cierre operativo de accesos. • Supervisión del estado de lectores y tornos. • Funcionamiento local ante pérdidas de comunicación. • Integración con ticketing, VMS, PSIM y plataformas operativas.
Diferenciación	Frente al control visual o manual, la validación electrónica agiliza la comprobación de permisos, dificulta determinados fraudes y proporciona registros para estimar la ocupación. La fiabilidad del dato depende de que se controlen tanto las entradas como las salidas y de que no existan accesos sin instrumentar. Por ello, los registros deberán contrastarse con conteos y observaciones operativas.



3 Aplicaciones y casos de uso en eventos

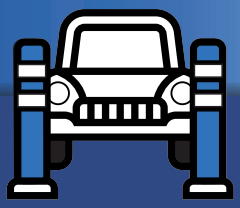
Escenarios de aplicación	Puede implantarse en estadios, conciertos, festivales, ferias, congresos y recintos con zonas diferenciadas. Resulta especialmente útil cuando existen áreas VIP, espacios técnicos, sectores con capacidades independientes o accesos reservados. Los terminales portátiles permiten cubrir entradas temporales, reforzar carriles saturados o mantener el control cuando no puedan instalarse tornos.
Ejemplos de uso operativo	Durante la entrada, el sistema detecta una utilización anterior de la misma credencial y genera un rechazo. El personal realiza una comprobación secundaria sin bloquear el resto del flujo. Si un sector se aproxima al umbral definido, el centro de control verifica la información mediante conteos complementarios y puede detener temporalmente el acceso, redirigir asistentes o habilitar otro espacio previsto. Ante una pérdida de conectividad, los lectores continúan validando mediante información local y sincronizan los registros cuando se recupera la red.

4 Beneficios para los actores del evento

Para el Promotor	Facilita la gestión de entradas, permisos y zonas, aporta datos sobre utilización del recinto y ayuda a detectar usos no autorizados o problemas de capacidad.
Para el Responsable de Seguridad	Proporciona información sobre accesos y ocupación, permite establecer umbrales y facilita la adopción temprana de medidas ante concentraciones o sectores próximos a su capacidad.
Para el Asistente	Puede agilizar la entrada, reducir comprobaciones repetitivas y facilitar una distribución más ordenada del público, siempre que los carriles estén correctamente dimensionados.
Para la Administración	Aporta información sobre ocupación y funcionamiento de los accesos cuando su comunicación esté prevista, sin sustituir las inspecciones ni las responsabilidades del organizador.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir credenciales, lectores, elementos de control físico y una plataforma para gestionar permisos, registros y ocupación. Los dispositivos mostrarán claramente las validaciones, rechazos, averías y funcionamiento fuera de línea. La apertura de emergencia y liberación de tornos deberá responder al Plan de Autoprotección y mantener prioridad sobre las funciones ordinarias de control.
Infraestructura necesaria	Requiere alimentación, comunicaciones, puestos de operación y espacio suficiente para formar carriles y realizar comprobaciones secundarias. El diseño deberá considerar caudales previstos, accesibilidad, evacuación y protección frente a la intemperie. Se dispondrá de terminales de reserva, baterías, conectividad alternativa y procedimientos manuales ante averías o saturación.
Estándares de interoperabilidad	La plataforma deberá disponer de API documentadas para intercambiar credenciales, permisos, estados y datos de ocupación con sistemas de ticketing, PSIM, VMS y gestión operativa. Las integraciones conservarán marcas temporales y evitarán duplicidades. Los sistemas de emergencia deberán poder actuar conforme a su lógica de seguridad, aunque la plataforma central no esté disponible.
Criterios de calidad y fiabilidad	• Capacidad de validaciones por minuto. • Tiempo de lectura y respuesta. • Tasas de rechazo incorrecto. • Precisión de los sistemas de conteo. • Disponibilidad y funcionamiento fuera de línea. • Sincronización tras recuperar la conexión. • Autonomía de terminales portátiles. • Accesibilidad y ergonomía. • Liberación segura ante emergencias. • Comportamiento en condiciones de máxima afluencia.
Compliance y seguridad	El tratamiento de datos deberá ajustarse al RGPD y a la normativa nacional aplicable, limitando la información asociada a cada credencial. Se definirán perfiles de acceso, conservación, cifrado y registro de consultas. El uso de biometría requerirá una justificación y evaluación jurídica específicas y no se considerará una función ordinaria. Los equipos deberán cumplir los requisitos aplicables de seguridad eléctrica, compatibilidad electromagnética, marcado CE, accesibilidad y evacuación.

PROTECCIÓN FRENTE A VEHÍCULOS HOSTILES Y CONTROL DE ACCESOS VIARIOS



1 Definición y fundamentos técnicos

Concepto	Estos sistemas tienen como finalidad impedir, limitar o controlar la entrada de vehículos en espacios ocupados por público. Incluyen bolardos, barreras, bloqueadores, elementos móviles certificados, controles de paso y medios de identificación de vehículos autorizados. Su diseño debe responder al análisis de riesgos, considerando posibles accesos, trayectorias, velocidad, tipo de vehículo, distancia de seguridad y necesidad de mantener el paso de emergencias y servicios.
Principios de funcionamiento	Los elementos de protección absorben, desvían o detienen la energía generada por el impacto de un vehículo. Su eficacia depende de la resistencia del dispositivo, la cimentación, el sistema de anclaje, la masa y velocidad del vehículo y el ángulo de aproximación. Los sistemas activos permanecen cerrados y se abren previa autorización, mientras que los pasivos protegen permanentemente el espacio. Las soluciones temporales pueden desplegarse sin obra permanente, siempre que se instalen conforme a las condiciones para las que hayan sido evaluadas.

2 Funcionalidades y capacidades

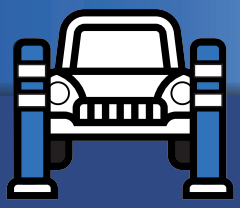
Prestaciones clave	• Cierre físico de vías de aproximación. • Protección de zonas peatonales y concentraciones. • Control de vehículos autorizados. • Apertura para emergencias y servicios. • Identificación mediante matrícula, tarjeta o credencial. • Registro de entradas, salidas y rechazos. • Operación local o remota de barreras activas. • Integración con videovigilancia y control de accesos. • Generación de alertas ante intentos de paso. • Implantación temporal o permanente. • Canalización de vehículos hacia puntos controlados. • Supervisión del estado de los dispositivos.
Diferenciación	Frente a vallas ligeras, vehículos estacionados u obstáculos improvisados, los sistemas evaluados frente a impacto aportan prestaciones conocidas bajo condiciones de ensayo. Las soluciones temporales permiten adaptar la protección a eventos puntuales. Ningún dispositivo elimina por sí solo el riesgo. La protección debe combinar barreras, distancia, geometría viaria, vigilancia, control de vehículos y procedimientos de respuesta.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resultan especialmente relevantes en conciertos, mercados, ferias, procesiones, cabalgatas, carreras y celebraciones desarrolladas en calles, plazas o explanadas. Pueden proteger accesos directos, cruces, vías con pendiente, zonas de espera, espacios de alta densidad y áreas próximas a escenarios o graderíos.
Ejemplos de uso operativo	Antes del evento se identifican las vías desde las que un vehículo podría alcanzar una concentración. Se instalan barreras temporales en los puntos prioritarios, manteniendo un acceso controlado para emergencias. Cuando llega un vehículo autorizado, el personal comprueba la matrícula o acreditación y confirma que el área interior permite su entrada. El elemento se abre durante el tiempo imprescindible y vuelve a la posición de protección. Si una barrera activa falla, se aplica el procedimiento alternativo previsto, que puede incluir cierre manual, refuerzo físico y vigilancia del punto afectado.

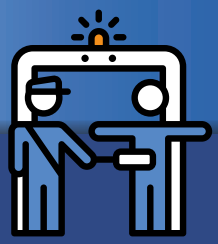
4 Beneficios para los actores del evento

Para el Promotor	Permite tratar de forma específica el riesgo derivado de accesos viarios y documentar los criterios utilizados para proteger las zonas de público y servicio.
Para el Responsable de Seguridad	Facilita la organización de puntos de control, reduce accesos no autorizados y permite mantener rutas diferenciadas para público, proveedores y emergencias.
Para el Asistente	Aumenta la separación física entre las concentraciones peatonales y los vehículos, reduciendo la exposición a entradas accidentales o deliberadas.
Para la Administración	Favorece la coordinación entre seguridad, movilidad, emergencias y gestión del espacio público, y permite utilizar soluciones temporales adaptadas al entorno urbano.



5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	El diseño deberá definir el tipo de dispositivo, nivel de prestación frente a impacto, anchura protegida, distancia entre elementos y modo de apertura. Los sistemas activos incorporarán accionamiento, señalización, detección de presencia y maniobra manual de emergencia. Los elementos temporales deberán utilizarse con la configuración, orientación, superficie y accesorios establecidos por el fabricante y la documentación de ensayo.
Infraestructura necesaria	Se requiere estudiar trazados, pendientes, radios de giro, velocidades posibles, servicios enterrados, pavimentos y espacio disponible. Las soluciones permanentes podrán necesitar cimentaciones, drenaje, energía y comunicaciones. El despliegue no deberá crear obstáculos peligrosos para peatones, afectar a la accesibilidad ni bloquear las rutas de evacuación o entrada de emergencias.
Estándares de interoperabilidad	Los sistemas activos podrán integrarse con control de accesos, lectura de matrículas, interfonía, videovigilancia y PSIM mediante interfaces documentadas. Las órdenes remotas deberán estar autenticadas y registradas. La apertura automática se limitará a supuestos evaluados y mantendrá procedimientos locales de control.
Criterios de calidad y fiabilidad	• Prestación frente al vehículo y velocidad de referencia. • Penetración observada en ensayos. • Adecuación de cimentaciones y anclajes. • Tiempo y seguridad de apertura y cierre. • Funcionamiento manual ante pérdida de energía. • Resistencia ambiental y mecánica. • Visibilidad, señalización y accesibilidad. • Tiempo de despliegue de soluciones temporales. • Inspección posterior a golpes o manipulaciones. • Disponibilidad de mantenimiento y repuestos.
Compliance y seguridad	Los dispositivos deberán cumplir los requisitos de producto, máquinas, electricidad y marcado CE que correspondan. Cuando se exijan prestaciones frente a impacto, se utilizarán ensayos y clasificaciones reconocidos, como los contemplados en ISO 22343 u otras normas aplicables. La lectura de matrículas y el registro de vehículos deberán respetar la normativa de protección de datos. La implantación en vía pública requerirá coordinación y autorización de los responsables de movilidad, seguridad y ocupación del espacio.



DETECCIÓN NO INVASIVA DE AMENAZAS Y OBJETOS PROHIBIDOS

1 Definición y fundamentos técnicos

Concepto	Estos sistemas permiten detectar objetos metálicos, armas, recipientes u otros elementos prohibidos sin realizar inicialmente un registro físico completo. Incluyen arcos detectores, equipos portátiles, sensores magnéticos, ondas milimétricas, inspección de bultos y tecnologías de detección de trazas. Su selección debe responder al tipo de amenaza, las condiciones del acceso, el caudal de asistentes y los procedimientos de comprobación secundaria.
Principios de funcionamiento	Los detectores analizan la alteración de campos electromagnéticos, la respuesta de determinados materiales o la imagen generada al atravesar o reflejar diferentes tipos de ondas. El sistema compara la señal obtenida con patrones y umbrales configurados y genera una alerta cuando identifica una posible anomalía. La alerta señala la necesidad de una comprobación adicional, pero no confirma por sí sola que el objeto sea peligroso o esté prohibido.

2 Funcionalidades y capacidades

Prestaciones clave	• Detección de objetos metálicos. • Identificación de anomalías bajo la ropa. • Inspección de bolsos, mochilas y paquetes. • Detección orientativa de determinadas sustancias o trazas. • Análisis de personas en movimiento, según la tecnología. • Localización aproximada de la zona que genera la alerta. • Configuración de niveles de sensibilidad. • Clasificación y registro de alarmas. • Integración con cámaras y control de accesos. • Generación de estadísticas sobre flujos y rechazos. • Funcionamiento mediante carriles fijos o equipos portátiles. • Apoyo a inspecciones secundarias dirigidas.
Diferenciación	Frente al registro manual generalizado, estas tecnologías permiten seleccionar las personas o pertenencias que requieren una inspección adicional. Esto puede reducir el contacto físico y mejorar la fluidez si el sistema y los carriles están correctamente dimensionados. Sus prestaciones varían según los materiales, la posición de los objetos, la ropa, la densidad del flujo y la configuración. Una sensibilidad excesiva puede aumentar las falsas alarmas y generar colas.



DETECCIÓN NO INVASIVA DE AMENAZAS Y OBJETOS PROHIBIDOS

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Pueden utilizarse en accesos a estadios, conciertos, festivales, recintos feriales, actos institucionales y eventos con restricciones específicas sobre armas, recipientes o determinados objetos. Los equipos portátiles permiten realizar controles secundarios, inspecciones aleatorias o comprobaciones en accesos temporales con menor volumen de público.
Ejemplos de uso operativo	En un acceso principal, los asistentes atraviesan una zona de detección en movimiento. Cuando el sistema genera una alerta, el personal deriva a la persona a un puesto lateral para efectuar una comprobación secundaria sin detener el resto del flujo. En la inspección de una mochila, el operador identifica una imagen o señal que requiere revisión. El bulto se separa del carril y se aplica el procedimiento establecido, evitando manipular un objeto potencialmente peligroso sin medios adecuados.

4 Beneficios para los actores del evento

Para el Promotor	Permite adaptar el nivel de inspección al análisis de riesgos y mejorar la capacidad de procesamiento de los accesos cuando el diseño está correctamente dimensionado.
Para el Responsable de Seguridad	Ayuda a seleccionar inspecciones, detectar determinados objetos y registrar incidencias. También facilita distribuir al personal entre control inicial y comprobación secundaria.
Para el Asistente	Puede reducir registros manuales innecesarios y favorecer accesos más fluidos, manteniendo procedimientos respetuosos con la intimidad y la accesibilidad.
Para la Administración	Puede reforzar las medidas preventivas y aportar información agregada sobre incidencias, siempre dentro de las competencias y procedimientos aplicables.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá seleccionarse según las amenazas que se pretenda detectar. Se definirán sensibilidad, dimensiones de paso, velocidad de procesamiento, tipos de objetos, señalización de alarmas y procedimiento de inspección secundaria. Los equipos de inspección de bultos deberán proporcionar una imagen adecuada y herramientas de apoyo al operador. No se utilizarán funciones de identificación personal que no estén expresamente justificadas.
Infraestructura necesaria	Se requiere espacio para organizar colas, carriles de paso, inspección secundaria y retirada segura de objetos. Deberán preverse alimentación, comunicaciones, protección meteorológica y rutas accesibles. El dispositivo contará con personal formado, equipos de reserva y procedimientos alternativos ante avería, saturación o evacuación. Los sistemas no deberán obstaculizar las salidas.
Estándares de interoperabilidad	xxxxxxxxxxLos equipos podrán integrarse con control de accesos, videovigilancia, VMS o PSIM mediante contactos, protocolos IP o API documentadas. La integración transmitirá alarmas y estados técnicos sin distribuir imágenes corporales a usuarios no autorizados. Las actuaciones sobre accesos requerirán la validación operativa prevista.
Criterios de calidad y fiabilidad	• Tipos y dimensiones de objetos detectables. • Probabilidad de detección. • Tasas de falsas alarmas. • Capacidad de personas o bultos por minuto. • Tiempo de inspección secundaria. • Estabilidad de la configuración. • Resistencia a interferencias ambientales. • Disponibilidad y recuperación. • Ergonomía y accesibilidad. • Formación y desempeño de los operadores.
Compliance y seguridad	Los equipos deberán cumplir los requisitos de producto, marcado CE, compatibilidad electromagnética y seguridad de las emisiones aplicables. Los sistemas que utilicen radiaciones estarán sujetos a las autorizaciones, inspecciones y medidas de protección correspondientes. La utilización deberá respetar la dignidad, intimidad, no discriminación y protección de datos. Se definirán criterios de selección, inspección secundaria, información al público, acceso a imágenes y conservación de registros.



VIGILANCIA AÉREA MEDIANTE UAS CONVENCIONALES Y DRONES CAUTIVOS

1 Definición y fundamentos técnicos

Concepto	Los sistemas UAS permiten captar imágenes y datos desde una plataforma aérea no tripulada. En eventos pueden utilizarse para supervisar superficies extensas, observar flujos, verificar incidencias y apoyar a los equipos desplegados. Los drones convencionales se desplazan mediante control remoto o vuelos programados. Los drones cautivos permanecen conectados al suelo mediante un cable que puede proporcionar alimentación, comunicaciones o sujeción, favoreciendo operaciones prolongadas en una posición determinada.
Principios de funcionamiento	La aeronave mantiene el vuelo mediante motores y sistemas electrónicos de estabilización, navegación y control. Las cámaras visuales o térmicas transmiten imágenes a una estación de pilotaje y, cuando se requiere, al centro de control. Los drones cautivos reciben energía desde una unidad terrestre y operan dentro del alcance del cable. Esta configuración aumenta la autonomía, pero requiere anclaje, protección del área terrestre y gestión de los riesgos asociados al propio cable.

2 Funcionalidades y capacidades

Prestaciones clave	• Observación aérea de zonas extensas. • Supervisión de entradas, salidas y flujos. • Detección visual de concentraciones o bloqueos. • Verificación de incendios e incidencias mediante imagen térmica. • Apoyo a la localización de personas o recursos. • Vigilancia de perímetros y zonas de difícil acceso. • Transmisión de vídeo al centro de control. • Registro de imágenes para análisis posterior. • Desplazamiento entre puntos de observación. • Vuelo estacionario prolongado mediante sistemas cautivos. • Incorporación de iluminación o megafonía cuando esté autorizada. • Integración con GIS, VMS o PSIM.
Diferenciación	Frente a las cámaras fijas, los UAS aportan una perspectiva elevada y adaptable y pueden observar áreas sin infraestructura permanente. Los drones convencionales ofrecen movilidad, mientras que los cautivos proporcionan mayor autonomía y estabilidad sobre una zona. Su utilización está condicionada por el espacio aéreo, la meteorología, la presencia de público, los obstáculos, la autonomía y las autorizaciones aplicables. No sustituyen la vigilancia terrestre ni garantizan una visión completa.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resultan especialmente útiles en festivales, conciertos al aire libre, acontecimientos deportivos, peregrinaciones, procesiones, carreras urbanas y eventos distribuidos en grandes superficies. Los drones cautivos pueden emplearse como punto elevado persistente sobre accesos, aparcamientos o zonas de concentración, mientras que los convencionales pueden revisar recorridos y áreas alejadas.
Ejemplos de uso operativo	Durante la salida de un concierto, un dron cautivo supervisa la evolución de los flujos hacia el transporte público. El operador detecta una concentración, verifica las imágenes y comunica la situación al centro de control para que valore la redistribución del público. En un evento itinerante, un UAS convencional inspecciona un tramo del recorrido tras recibirse un aviso de bloqueo. Las imágenes permiten confirmar la incidencia y orientar a los equipos terrestres, manteniendo la decisión operativa bajo responsabilidad del mando correspondiente.

4 Beneficios para los actores del evento

Para el Promotor	Permite ampliar temporalmente la cobertura de vigilancia sin instalar numerosos soportes fijos y adaptar la observación a las fases y configuración del evento.
Para el Responsable de Seguridad	Aporta una perspectiva general de flujos, perímetros e incidencias y facilita la verificación visual y la coordinación de recursos sobre el terreno.
Para el Asistente	Puede contribuir a detectar tempranamente concentraciones, incendios, bloqueos o necesidades de asistencia, favoreciendo una respuesta más organizada.
Para la Administración	Facilita una visión complementaria del evento y su entorno cuando la operación y el intercambio de imágenes estén autorizados y coordinados con los organismos competentes.



5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	La solución incluirá aeronave, estación de control, enlaces de mando y vídeo, sistemas de posicionamiento y cargas útiles adecuadas. Se definirán resolución, zoom, sensibilidad térmica, autonomía y resistencia al viento conforme a la misión. Los sistemas cautivos incorporarán unidad terrestre de alimentación, cable, carrete, anclaje y mecanismos de recuperación o descenso seguro.
Infraestructura necesaria	Se requiere una zona de despegue, aterrizaje u operación terrestre controlada, alimentación y comunicaciones. El estudio previo deberá considerar público, edificios, tendidos eléctricos, grúas, otras aeronaves, rutas de emergencia y condiciones meteorológicas. La operación contará con pilotos habilitados, observadores cuando proceda, baterías o alimentación de respaldo y procedimientos ante pérdida de enlace, energía o posicionamiento.
Estándares de interoperabilidad	El vídeo, la telemetría y las alertas podrán integrarse con VMS, GIS, PSIM y centros de control mediante protocolos y API documentadas. La integración deberá conservar marcas temporales, ubicación y origen de las imágenes, además de limitar las funciones de mando de la aeronave a los usuarios autorizados.
Criterios de calidad y fiabilidad	• Autonomía y tiempo efectivo de operación. • Calidad y estabilidad de imagen. • Alcance y disponibilidad de los enlaces. • Precisión de posicionamiento. • Resistencia al viento y condiciones ambientales. • Seguridad del cable y anclaje. • Tiempo de despliegue y recuperación. • Procedimientos ante pérdida de enlace o energía. • Formación y coordinación de la tripulación. • Integración con el centro de control.
Compliance y seguridad	La operación deberá cumplir la normativa europea y nacional sobre UAS, las condiciones del espacio aéreo y los requisitos establecidos por AESA. Se obtendrán las autorizaciones y coordinaciones necesarias y se mantendrán distancias y zonas de seguridad. La captación de imágenes respetará la normativa de protección de datos y seguridad privada. Las comunicaciones estarán protegidas frente a accesos no autorizados y se definirán los responsables, finalidades y plazos de conservación de las grabaciones.



SISTEMAS DE DETECCIÓN Y SEGUIMIENTO DE DRONES C-UAS

1 Definición y fundamentos técnicos

Concepto	xxxxxxLos sistemas C-UAS permiten detectar, localizar, clasificar y seguir aeronaves no tripuladas que se aproximan o acceden al espacio aéreo de un evento. Su finalidad es proporcionar una alerta temprana y apoyar la evaluación de posibles riesgos. Pueden combinar sensores de radiofrecuencia, receptores de identificación remota, radar y cámaras visuales o térmicas. Las medidas de interferencia o neutralización constituyen capacidades diferenciadas y quedan reservadas a los organismos legalmente habilitados.xxxxxx.
Principios de funcionamiento	Los sensores de radiofrecuencia analizan señales intercambiadas entre el dron y su estación de control. Los receptores Remote ID obtienen la información transmitida por aeronaves compatibles, mientras que el radar detecta objetos mediante la reflexión de ondas. Las cámaras permiten verificar visualmente el objetivo. Una plataforma de correlación combina los datos disponibles para estimar su posición, trayectoria y clasificación y presentar la alerta al operador.

2 Funcionalidades y capacidades

Prestaciones clave	• Detección de señales asociadas a determinados UAS. • Recepción de información Remote ID. • Localización estimada del dron. • Estimación de la posición del piloto, cuando sea técnicamente posible. • Seguimiento simultáneo de varios objetivos. • Detección mediante radar de aeronaves sin emisiones conocidas. • Verificación con cámaras visuales o térmicas. • Clasificación de vuelos conocidos o no autorizados. • Definición de zonas y reglas de alerta. • Representación de trayectorias sobre cartografía. • Registro de eventos para análisis posterior. • Integración con centros de control, GIS, VMS y PSIM.
Diferenciación	Frente a la vigilancia visual, estos sistemas pueden advertir determinados drones antes de que sean visibles y mantener su seguimiento sobre áreas amplias. La combinación de sensores reduce la dependencia de una única fuente. Ningún sensor detecta todos los modelos y condiciones de vuelo. El alcance y la precisión dependen del entorno, la orografía, los edificios, las emisiones del dron, su tamaño y las interferencias presentes.



3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Pueden emplearse en estadios, conciertos, festivales, actos institucionales, celebraciones populares y eventos próximos a infraestructuras sensibles. Resultan especialmente útiles cuando el análisis de riesgos identifica vuelos no autorizados, caída sobre el público, captación ilícita de imágenes, interferencia con operaciones autorizadas o transporte de objetos.
Ejemplos de uso operativo	Durante un acontecimiento deportivo, el sistema detecta una señal y representa una trayectoria de aproximación. El operador contrasta la alerta con los vuelos autorizados y utiliza una cámara para intentar verificar el objetivo. Si se confirma un vuelo no autorizado, el centro de control informa a las autoridades y aplica las medidas de protección previstas. La decisión podrá incluir vigilancia del recorrido, protección de una zona o interrupción de una actividad, sin activar automáticamente una evacuación.

4 Beneficios para los actores del evento

Para el Promotor	Permite incorporar el riesgo aéreo a la planificación, documentar alertas y mejorar la coordinación con las autoridades ante vuelos no autorizados.
Para el Responsable de Seguridad	Proporciona información anticipada sobre presencia, trayectoria y evolución de posibles UAS y facilita la adopción de medidas proporcionadas.
Para el Asistente	Puede reducir la exposición a caídas, colisiones o usos malintencionados de drones mediante una detección y respuesta más tempranas.
Para la Administración	Facilita información técnica para valorar la amenaza, localizar posibles operadores y coordinar las actuaciones de los organismos competentes.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución podrá integrar sensores RF, receptores Remote ID, radar, cámaras PTZ visuales o térmicas, servidor de correlación, cartografía y consola de operación. El diseño deberá definir área de cobertura, alturas, tipos de objetivos, precisión esperada, frecuencia de actualización y procedimiento de clasificación y verificación.
Infraestructura necesaria	Se requieren emplazamientos con cobertura adecuada, energía, comunicaciones IP seguras y campo de visión suficiente para los sensores. El estudio previo considerará edificios, estructuras, emisiones radioeléctricas y tráfico aéreo autorizado. Se preverán alimentación de respaldo, protección meteorológica, sincronización temporal y personal formado para interpretar alertas multisensor.
Estándares de interoperabilidad	La solución deberá permitir intercambiar posiciones, trayectorias, clasificaciones, imágenes y estados mediante API documentadas y formatos geográficos normalizados. Podrá integrarse con GIS, VMS, PSIM y plataformas de las autoridades cuando exista autorización. Los datos deberán indicar su fuente, marca temporal y nivel de confianza.
Criterios de calidad y fiabilidad	• Tipos de UAS detectables. • Alcance en el entorno real. • Precisión de posición y seguimiento. • Frecuencia y latencia de actualización. • Tasas de falsas alarmas y omisiones. • Capacidad de correlación multisensor. • Número de objetivos simultáneos. • Tiempo de verificación visual. • Disponibilidad y recuperación. • Registro y exportación de eventos.
Compliance y seguridad	El despliegue deberá cumplir la normativa aeronáutica, de telecomunicaciones, protección de datos y seguridad pública aplicable. La monitorización del espectro y el tratamiento de identificadores se limitarán a las funciones legalmente permitidas. La inhibición, suplantación, toma de control o neutralización no podrán ser ejecutadas por el organizador o la seguridad privada salvo habilitación legal expresa. Las comunicaciones estarán cifradas y el acceso a posiciones, imágenes y registros quedará restringido a usuarios autorizados.



MONITORIZACIÓN METEOROLÓGICA Y ALERTA AMBIENTAL

1 Definición y fundamentos técnicos

Concepto	Estos sistemas combinan predicciones y avisos meteorológicos oficiales con mediciones locales para detectar condiciones que puedan afectar a las personas, las estructuras temporales y la continuidad del evento. Pueden incluir estaciones meteorológicas, anemómetros, pluviómetros, sensores térmicos, detectores de actividad eléctrica y plataformas de alerta. Su finalidad es apoyar decisiones previamente definidas, no sustituir a los servicios meteorológicos ni al criterio técnico.
Principios de funcionamiento	Los sensores miden variables como viento, temperatura, humedad, precipitación, presión o radiación. La plataforma recibe estos datos y puede complementarlos con predicciones, radar meteorológico y avisos oficiales. Cuando una variable alcanza un umbral, el sistema genera una alerta para que el responsable verifique la situación y aplique el procedimiento establecido. Los umbrales deberán adaptarse al recinto, las estructuras, el público y las actividades previstas.

2 Funcionalidades y capacidades

Prestaciones clave	• Medición local de velocidad y dirección del viento. • Registro de temperatura y humedad. • Cálculo de indicadores de estrés térmico. • Medición de precipitación. • Detección o seguimiento de actividad eléctrica próxima. • Integración de avisos y predicciones oficiales. • Visualización de tendencias y evolución temporal. • Definición de umbrales por zonas o actividades. • Generación de alertas escalonadas. • Supervisión de sensores instalados en estructuras. • Registro de datos y decisiones asociadas. • Integración con PSIM y plataformas operativas.
Diferenciación	Frente a la consulta periódica de una previsión general, la monitorización local permite conocer las condiciones en el propio recinto y observar cambios rápidos que puedan afectar a escenarios, carpas o zonas expuestas. Una estación aislada no permite predecir por sí sola la evolución meteorológica. Sus datos deberán interpretarse junto con fuentes oficiales, radares, avisos y observaciones sobre el terreno.



3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta especialmente adecuada para festivales, conciertos, ferias, acontecimientos deportivos, procesiones y eventos celebrados al aire libre o en instalaciones temporales. También puede utilizarse en recintos con cubiertas ligeras, escenarios, gradas, elementos suspendidos, zonas arboladas o espacios con exposición significativa al calor.
Ejemplos de uso operativo	Un anemómetro instalado a una altura representativa detecta valores próximos al límite operativo de un escenario. El sistema emite una alerta preventiva, se suspenden determinadas operaciones y el responsable técnico revisa la estructura. Si se alcanza el umbral definido, se aplica el procedimiento de interrupción o desalojo. Ante una tormenta próxima, la plataforma combina información oficial y detección de actividad eléctrica. El centro de control restringe actividades expuestas, informa a los asistentes y dirige al público hacia los espacios de protección previstos. Durante un episodio de calor, la evolución del indicador térmico puede activar refuerzo de agua, sombra, información y recursos sanitarios.

4 Beneficios para los actores del evento

Para el Promotor	Permite incorporar criterios meteorológicos verificables a la planificación y documentar las decisiones adoptadas ante cambios ambientales.
Para el Responsable de Seguridad	Facilita la anticipación, el escalado de alertas y la coordinación de medidas como restricciones, suspensión temporal, evacuación o refugio.
Para el Asistente	Contribuye a reducir la exposición a viento, tormentas, calor, frío o precipitaciones y permite recibir instrucciones con mayor antelación.
Para la Administración	Facilita la coordinación con protección civil, servicios meteorológicos, sanidad y responsables municipales, utilizando información compartida y trazable.



5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir sensores adecuados, registro histórico, visualización, reglas de alerta y conexión con fuentes externas. Cada medición indicará ubicación, unidad, hora, estado del sensor y calidad del dato. Los umbrales se establecerán conforme a límites estructurales, condiciones de trabajo, exposición del público y protocolos del evento. Se definirán niveles de vigilancia, prealerta y actuación.
Infraestructura necesaria	Los sensores deberán instalarse en ubicaciones representativas, evitando obstáculos, fuentes de calor o turbulencias que alteren las mediciones. Algunos equipos requerirán mástiles, alimentación, comunicaciones y protección frente a descargas. Se preverán alimentación autónoma, comunicaciones alternativas, inspecciones y procedimientos de consulta manual de fuentes oficiales.
Estándares de interoperabilidad	La plataforma deberá permitir integrar datos de sensores, predicciones y avisos mediante API o formatos documentados. Podrá conectarse con PSIM, GIS, sistemas de megafonía y herramientas de gestión operativa. Las alertas conservarán la fuente, el umbral, la marca temporal y el estado de verificación, evitando activar automáticamente mensajes o evacuaciones sin la autorización prevista.
Criterios de calidad y fiabilidad	• Rango y precisión de cada sensor. • Ubicación y representatividad de la medida. • Frecuencia de actualización. • Latencia de avisos externos. • Calibración y mantenimiento. • Autonomía y comunicaciones. • Resistencia ambiental. • Detección de datos anómalos. • Disponibilidad de fuentes alternativas. • Pruebas de los procedimientos asociados.
Compliance y seguridad	Los equipos cumplirán los requisitos aplicables de marcado CE, compatibilidad electromagnética, seguridad eléctrica y utilización del espectro. Las instalaciones elevadas o expuestas deberán contemplar puesta a tierra, protección frente a descargas y seguridad estructural. Las fuentes oficiales, como AEMET, se utilizarán conforme a sus condiciones. La organización conservará la responsabilidad de interpretar los avisos y activar las medidas previstas en el Plan de Autoprotección.



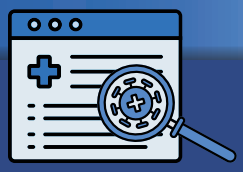
VIGILANCIA SANITARIA Y DETECCIÓN TEMPRANA DE PATRONES

1 Definición y fundamentos técnicos

Concepto	Estos sistemas recopilan y analizan información sobre asistencias sanitarias, síntomas, intoxicaciones y capacidad de los recursos médicos durante un evento. Su finalidad es detectar incrementos o agrupaciones anómalas que puedan indicar un riesgo colectivo. Trabajan preferentemente con datos agregados o seudonimizados y complementan la valoración de los profesionales sanitarios y los sistemas oficiales de salud pública.
Principios de funcionamiento	Los puntos asistenciales registran de forma estructurada datos como motivo de consulta, síntomas, ubicación, hora, gravedad y atención prestada. La plataforma agrupa los registros por categorías, zonas y periodos y compara su evolución con umbrales previamente definidos. Cuando se detecta un patrón, el sistema genera una alerta para su valoración clínica y epidemiológica. Una agrupación de síntomas no confirma por sí sola un brote, intoxicación o consumo de una sustancia determinada.

2 Funcionalidades y capacidades

Prestaciones clave	• Registro estructurado de asistencias sanitarias. • Clasificación por síntomas, gravedad y posible causa. • Seguimiento de intoxicaciones alimentarias o etílicas. • Identificación de patrones asociados al consumo de sustancias. • Detección de agrupaciones de síntomas compatibles. • Representación temporal y geográfica de incidencias. • Control de ocupación de puestos sanitarios. • Seguimiento de recursos y capacidad asistencial. • Generación de alertas por umbrales. • Elaboración de informes agregados. • Intercambio autorizado con salud pública y emergencias. • Integración con plataformas operativas y centros de control.
Diferenciación	Frente al recuento manual o al análisis posterior, estas herramientas permiten observar durante el evento la evolución conjunta de asistencias registradas en distintos puestos. La tecnología no realiza un diagnóstico colectivo automático. La interpretación requiere personal sanitario, definiciones homogéneas, calidad suficiente de los registros y contraste con información clínica, ambiental y epidemiológica.



3 Aplicaciones y casos de uso en eventos

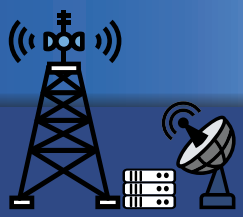
Escenarios de aplicación	Puede utilizarse en festivales, acontecimientos deportivos, ferias, peregrinaciones y eventos de varios días o con numerosos puntos de restauración y asistencia. Resulta especialmente útil ante altas temperaturas, consumo de alcohol o drogas, enfermedades transmisibles, contaminación de alimentos o agua y concentraciones de personas con necesidades sanitarias específicas.
Ejemplos de uso operativo	Varios puestos registran en un periodo breve síntomas gastrointestinales entre asistentes que han utilizado una misma zona de restauración. La plataforma detecta la agrupación y avisa al responsable sanitario, que verifica los casos e informa a la autoridad competente para valorar medidas de control. Durante un festival aumenta el número de asistencias por alteración de conciencia. El responsable revisa la distribución, gravedad y posible relación con alcohol, drogas o calor, refuerza los recursos y coordina la información preventiva. La aplicación del evento puede permitir comunicar una necesidad médica, pero el aviso deberá validarse y derivarse al recurso apropiado.

4 Beneficios para los actores del evento

Para el Promotor	Facilita el seguimiento del dispositivo sanitario, permite detectar tendencias y aporta información para revisar recursos, restauración, agua, sombra y medidas preventivas.
Para el Responsable de Seguridad	Proporciona una visión agregada de las incidencias sanitarias que pueden afectar a la continuidad, los flujos o la seguridad general del evento.
Para el Asistente	Puede contribuir a detectar antes una situación colectiva, reforzar la capacidad sanitaria y difundir recomendaciones preventivas adaptadas a la incidencia observada.
Para la Administración	Facilita la comunicación temprana y estructurada con emergencias y salud pública y aporta datos agregados para valorar medidas y analizar posteriormente el evento.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá disponer de formularios sanitarios estructurados, categorías homogéneas, marcas temporales, ubicación, gestión de recursos, reglas de alerta y cuadros de mando. Los umbrales deberán definirse con responsables sanitarios y adaptarse al tamaño, duración y perfil del evento. La plataforma distinguirá entre casos sospechosos, confirmados y descartados cuando esa clasificación resulte aplicable.
Infraestructura necesaria	Requiere terminales seguros en los puestos asistenciales, conectividad, plataforma central y procedimientos para registrar datos cuando se pierda la red. El diseño deberá contemplar usuarios sanitarios autorizados, formación, respaldo de la información y coordinación con los sistemas oficiales. Se evitará mostrar información clínica individual en pantallas operativas generales.
Estándares de interoperabilidad	La solución deberá permitir exportar datos agregados y, cuando esté autorizado, intercambiar registros mediante formatos sanitarios documentados. La integración con plataformas de emergencias, PSIM o sistemas públicos deberá limitarse a la información necesaria para cada finalidad. Los avisos conservarán su fuente, hora, clasificación y estado de verificación.
Criterios de calidad y fiabilidad	• Homogeneidad de las categorías registradas. • Integridad y actualización de los datos. • Tiempo entre asistencia, registro y alerta. • Sensibilidad y especificidad de los umbrales. • Detección de duplicidades. • Capacidad de usuarios simultáneos. • Funcionamiento sin conexión. • Disponibilidad y recuperación. • Claridad de los cuadros de mando. • Validación por profesionales sanitarios.
Compliance y seguridad	Los datos de salud tienen especial protección. Su tratamiento deberá contar con base jurídica suficiente, finalidad definida, minimización, control de accesos y plazos de conservación adecuados. Se aplicarán cifrado, autenticación robusta, registro de consultas, copias de respaldo y separación entre información clínica y operativa. El intercambio con autoridades sanitarias se realizará mediante los canales y procedimientos establecidos, evitando comunicar datos identificativos cuando resulten suficientes datos agregados o seudonimizados.

REDES DE CONECTIVIDAD Y RADIOCOMUNICACIONES DE MISIÓN CRÍTICA



1 Definición y fundamentos técnicos

Concepto	Estas redes proporcionan comunicaciones de voz y datos a los equipos responsables de seguridad, emergencias y operación del evento. Pueden utilizar tecnologías como DMR, TETRA, LTE o 5G privados y servicios de comunicación de grupo sobre redes móviles. Su diseño debe priorizar las funciones esenciales, mantener una estructura de grupos y permitir la operación mediante canales alternativos ante saturación, interferencias o pérdida de infraestructura.
Principios de funcionamiento	Las redes de radiocomunicación transmiten voz y datos mediante estaciones base, repetidores y terminales portátiles. Los grupos de llamada permiten organizar las comunicaciones por funciones, zonas o niveles de mando. Las redes de banda ancha añaden imágenes, telemetría, mensajes y localización. Los mecanismos de prioridad y calidad de servicio reservan capacidad para determinados usuarios o aplicaciones, aunque su disponibilidad dependerá de la arquitectura y condiciones del servicio.

2 Funcionalidades y capacidades

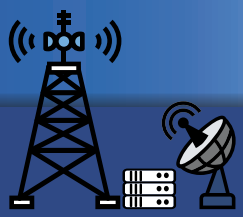
Prestaciones clave	• Comunicaciones de voz individuales y de grupo. • Llamadas prioritarias y de emergencia. • Pulsador de alarma en terminales. • Organización de canales por funciones o sectores. • Transmisión de mensajes, alertas y telemetría. • Envío de imágenes o vídeo en redes compatibles. • Localización de terminales. • Grabación autorizada de comunicaciones. • Consolas de despacho en el centro de control. • Accesorios manos libres y cancelación de ruido. • Supervisión de cobertura y estado de equipos. • Funcionamiento mediante infraestructura fija o temporal.
Diferenciación	Frente a la telefonía móvil convencional, las redes profesionales permiten comunicaciones de grupo, prioridad, pulsadores de emergencia y control centralizado. Las redes privadas reducen la competencia con el tráfico del público, mientras que los servicios sobre redes comerciales pueden aprovechar infraestructuras existentes. Ninguna modalidad garantiza por sí sola cobertura o disponibilidad total. La solución deberá combinar tecnologías y procedimientos según el riesgo y las condiciones del evento.

3 Aplicaciones y casos de uso en eventos

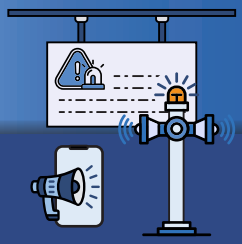
Escenarios de aplicación	Pueden emplearse en estadios, festivales, conciertos, ferias, procesiones, carreras urbanas y eventos con numerosos equipos o sectores. Son especialmente relevantes en entornos con alto ruido, elevada concentración de usuarios, espacios subterráneos, estructuras cerradas o necesidad de coordinar recursos distribuidos.
Ejemplos de uso operativo	Un vigilante activa el pulsador de emergencia de su terminal. La consola identifica el equipo, muestra su última posición disponible y concede prioridad a la llamada. El centro de control verifica la situación y moviliza los recursos previstos. Durante una incidencia, el responsable crea o activa un grupo específico para los equipos afectados, manteniendo separados los canales ordinarios. Si falla la infraestructura principal, los terminales pasan al canal o modo alternativo definido. En una intervención sanitaria, los accesorios manos libres permiten mantener la comunicación mientras se presta asistencia o se traslada a una persona.

4 Beneficios para los actores del evento

Para el Promotor	Facilita la coordinación de los servicios contratados y reduce la dependencia de comunicaciones móviles ordinarias durante periodos de gran demanda.
Para el Responsable de Seguridad	Permite organizar grupos, priorizar avisos y mantener contacto con los equipos desplegados. Las consolas facilitan la asignación de recursos y el seguimiento de incidencias.
Para el Asistente	Puede contribuir a que los avisos lleguen con mayor rapidez a los equipos adecuados y a que la respuesta se mantenga incluso cuando las redes públicas estén saturadas.
Para la Administración	Favorece la coordinación con el dispositivo del evento y puede facilitar el enlace con otros organismos mediante procedimientos y pasarelas autorizados.



5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá definir tecnología, bandas, canales, grupos, prioridades, cobertura, capacidad y terminales. Podrá incluir estaciones base, repetidores, antenas, consolas, grabadores, servidores y accesorios de audio. Los terminales deberán disponer de autonomía suficiente, resistencia adecuada al entorno, identificación individual y funciones de emergencia acordes con cada perfil.
Infraestructura necesaria	Se requiere estudiar cobertura, altura y ubicación de antenas, alimentación, enlaces, frecuencias disponibles y zonas con sombra. Podrán instalarse repetidores temporales o sistemas de cobertura interior. Se preverán SAI, baterías, terminales de reserva, cargadores, accesorios y procedimientos alternativos. Las pruebas deberán considerar el ruido y la ocupación previstos.
Estándares de interoperabilidad	Se priorizarán tecnologías y protocolos normalizados, interfaces documentadas y mecanismos de conexión con plataformas de despacho, PSIM y sistemas de gestión operativa. La interoperabilidad con redes de otros organismos se tratará en la ficha específica de pasarelas y requerirá autorización técnica y operativa.
Criterios de calidad y fiabilidad	• Cobertura interior y exterior. • Capacidad de usuarios y grupos simultáneos. • Tiempo de establecimiento de llamada. • Calidad e inteligibilidad de voz. • Latencia y capacidad de datos. • Autonomía de terminales. • Disponibilidad de estaciones y enlaces. • Comportamiento ante saturación o interferencias. • Funcionamiento de canales alternativos. • Recuperación tras pérdida de energía o red.
Compliance y seguridad	El uso de frecuencias y equipos radioeléctricos deberá ajustarse a la normativa de telecomunicaciones, las licencias y autorizaciones aplicables. Los equipos cumplirán los requisitos de marcado CE y compatibilidad electromagnética. Las comunicaciones y plataformas aplicarán autenticación, cifrado, control de accesos, actualizaciones seguras y registros. La grabación de voz y la localización de terminales deberán responder a una finalidad legítima, proporcionada y conocida por los usuarios afectados.



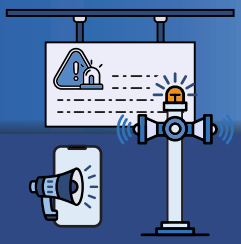
MEGAFONÍA, SEÑALIZACIÓN, NOTIFICACIÓN MASIVA Y APP DE EMERGENCIA

1 Definición y fundamentos técnicos

Concepto	Estos sistemas permiten comunicar instrucciones, avisos y recomendaciones al público mediante canales acústicos, visuales y digitales. Pueden combinar megafonía de emergencia, pantallas, señalización dinámica, aplicaciones móviles y plataformas de notificación. Su finalidad es proporcionar información clara y coordinada antes, durante y después de una incidencia, incluyendo a personas con diferentes necesidades de comunicación y accesibilidad.
Principios de funcionamiento	La megafonía distribuye mensajes de voz mediante amplificadores, líneas y altavoces organizados por zonas. Los sistemas visuales muestran textos, pictogramas o rutas, mientras que las plataformas digitales envían notificaciones a aplicaciones o dispositivos conectados. Los mensajes se preparan o generan conforme a procedimientos autorizados. Su difusión puede realizarse en todo el recinto o limitarse a los sectores afectados, manteniendo coherencia entre los distintos canales.

2 Funcionalidades y capacidades

Prestaciones clave	• Emisión de mensajes en directo o pregrabados. • Difusión general o por zonas. • Mensajes en varios idiomas. • Avisos visuales mediante pantallas y señalización. • Representación de rutas o accesos alternativos. • Notificaciones digitales segmentadas. • Comunicación de incidencias por los asistentes. • Avisos sobre necesidades médicas o personas extraviadas. • Supervisión de líneas, amplificadores y altavoces. • Priorización de mensajes de emergencia. • Alimentación y comunicaciones de respaldo. • Integración con PSIM y plataformas operativas.
Diferenciación	Frente a las sirenas o avisos por un único canal, la combinación de voz, texto, elementos visuales y personal de apoyo facilita la comprensión de las instrucciones y reduce la dependencia de un solo sistema. Las aplicaciones móviles permiten comunicación segmentada y bidireccional, pero requieren terminal, batería, cobertura y configuración adecuada. Por ello, complementan la megafonía y nunca deben constituir el único medio de aviso.



3 Aplicaciones y casos de uso en eventos

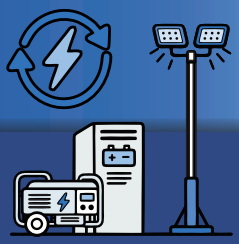
Escenarios de aplicación	Puede utilizarse en estadios, conciertos, festivales, ferias, procesiones, carreras y celebraciones urbanas. Resulta especialmente relevante en espacios con alto ruido, sectores diferenciados, público internacional o recorridos extensos. Las aplicaciones pueden resultar útiles en eventos con inscripción previa o canales digitales consolidados, siempre que su utilización por los asistentes sea voluntaria.
Ejemplos de uso operativo	Ante el bloqueo de una salida, el centro de control verifica la incidencia y autoriza un mensaje dirigido al sector afectado. La megafonía y las pantallas indican la ruta alternativa, mientras el personal orienta al público sobre el terreno. Un asistente comunica mediante la aplicación una necesidad médica o la pérdida de un acompañante. El centro de control recibe la ubicación aproximada, verifica el aviso y lo asigna al equipo correspondiente. Si falla la conectividad móvil, los avisos continúan mediante megafonía, señalización y comunicación directa del personal.

4 Beneficios para los actores del evento

Para el Promotor	Facilita una comunicación coherente y planificada, reduce improvisaciones y permite utilizar los mismos canales para información preventiva y gestión de incidencias.
Para el Responsable de Seguridad	Permite difundir instrucciones por zonas, coordinar mensajes con las actuaciones operativas y conocer incidencias comunicadas directamente por los asistentes.
Para el Asistente	Mejora el acceso a instrucciones claras y puede facilitar la solicitud de ayuda, la localización de servicios y la comunicación de situaciones de riesgo.
Para la Administración	Favorece la coordinación de la información pública y la difusión de mensajes coherentes entre el recinto, los servicios municipales y el entorno urbano.

5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	La solución deberá definir zonas de difusión, niveles acústicos, inteligibilidad, prioridades, idiomas y responsables de activación. Los sistemas visuales deberán utilizar mensajes y pictogramas comprensibles. Las aplicaciones deberán permitir avisos, confirmación de entrega cuando sea posible y comunicación sencilla de incidencias, evitando recopilar identidad o ubicación permanente si no resultan necesarias.
Infraestructura necesaria	La megafonía requiere altavoces, amplificadores, líneas supervisadas, puestos de control y alimentación de respaldo. El diseño considerará ruido ambiental, acústica, distribución del público y espacios exteriores. Los sistemas digitales necesitarán servidores, conectividad y capacidad suficiente. Se dispondrá de medios portátiles y procedimientos alternativos ante fallos.
Estándares de interoperabilidad	La solución podrá integrarse con detección de incendios, PSIM, señalización, aplicaciones y plataformas municipales mediante interfaces documentadas. Las prioridades deberán impedir que mensajes ordinarios bloqueen avisos de emergencia. Las activaciones automáticas con incidencia sobre el público requerirán las confirmaciones o interbloqueos definidos.
Criterios de calidad y fiabilidad	• Cobertura e inteligibilidad acústica. • Visibilidad y legibilidad de mensajes. • Tiempo de activación. • Funcionamiento por zonas. • Supervisión de líneas y equipos. • Autonomía de respaldo. • Capacidad y latencia de notificaciones. • Entrega y confirmación cuando estén disponibles. • Accesibilidad e idiomas. • Funcionamiento en modo degradado.
Compliance y seguridad	La megafonía de emergencia deberá cumplir las normas aplicables según su función, incluidas las partes correspondientes de UNE-EN 54 o UNE-EN 50849 cuando proceda. Las aplicaciones respetarán la normativa de protección de datos, aplicando voluntariedad, minimización, conservación limitada y control de accesos. Las plataformas deberán utilizar comunicaciones cifradas, autenticación segura y protección frente a la emisión de mensajes falsos o no autorizados.



ENERGÍA DE RESPALDO, ILUMINACIÓN Y CONTINUIDAD DE SERVICIO

1 Definición y fundamentos técnicos

Concepto	Estos sistemas mantienen las funciones esenciales del evento ante microcortes, pérdidas de suministro o fallos parciales de la instalación eléctrica. Incluyen SAI, baterías, grupos electrógenos, cuadros de conmutación, iluminación de emergencia y sistemas de supervisión energética. Su diseño parte de la identificación y priorización de las cargas críticas, asignando a cada una la autonomía y el nivel de respaldo necesarios.
Principios de funcionamiento	Los SAI proporcionan energía inmediata mediante baterías y estabilizan la alimentación de equipos sensibles. Los grupos electrógenos u otras fuentes alternativas asumen las cargas seleccionadas cuando se pierde la red principal. Los sistemas de conmutación transfieren la alimentación y las protecciones aíslan los fallos. La iluminación de emergencia dispone de alimentación propia o centralizada para facilitar la orientación y evacuación.

2 Funcionalidades y capacidades

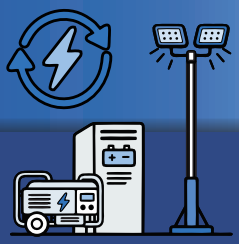
Prestaciones clave	• Protección frente a microcortes y variaciones de tensión. • Alimentación inmediata de sistemas críticos. • Generación eléctrica alternativa. • Conmutación automática o manual de fuentes. • Priorización y desconexión ordenada de cargas. • Iluminación de emergencia y balizamiento. • Supervisión de baterías y autonomía. • Control de combustible y carga de generadores. • Alarmas por averías o pérdida de suministro. • Registro de consumos y eventos eléctricos. • Alimentación temporal de centros y nodos móviles. • Recuperación controlada del servicio.
Diferenciación	Frente a una única acometida, una arquitectura de respaldo reduce la probabilidad de que un fallo eléctrico afecte simultáneamente a comunicaciones, accesos, megafonía, iluminación y centro de control. No es necesario mantener todas las cargas del evento. El dimensionamiento debe priorizar las funciones de seguridad y considerar el tiempo necesario para gestionar la incidencia, evacuar o realizar una parada segura.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta aplicable a cualquier evento dependiente de sistemas eléctricos, especialmente en recintos temporales, espacios exteriores, instalaciones con suministro limitado o actividades nocturnas. Puede proteger centros de control, comunicaciones, videovigilancia, control de accesos, megafonía, puestos sanitarios, iluminación y sistemas de detección de incendios.
Ejemplos de uso operativo	Ante un corte de red, los SAI mantienen los equipos esenciales mientras arranca el grupo electrógeno. El sistema de conmutación transfiere las cargas priorizadas y comunica su estado al centro de control. Si la autonomía disponible disminuye por debajo del umbral previsto, el responsable desconecta cargas no esenciales y activa el procedimiento correspondiente. Cuando falla parte de la iluminación ordinaria, el alumbrado de emergencia y los equipos portátiles mantienen visibles las salidas y recorridos prioritarios.

4 Beneficios para los actores del evento

Para el Promotor	Reduce las interrupciones derivadas de fallos eléctricos y permite planificar la continuidad de las actividades y servicios esenciales.
Para el Responsable de Seguridad	Mantiene disponibles los sistemas necesarios para supervisar, comunicar y coordinar la respuesta, y proporciona información sobre autonomía y cargas.
Para el Asistente	Contribuye a conservar la iluminación, orientación, información y asistencia durante una pérdida de suministro.
Para la Administración	Facilita el mantenimiento de las funciones de autoprotección y reduce la dependencia de actuaciones improvisadas ante fallos de la red.



5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	El diseño deberá elaborar un inventario de cargas, definir su prioridad y calcular potencia, autonomía, corriente de arranque y secuencia de recuperación. Los SAI se dimensionarán conforme a los equipos y al tiempo de transición previsto. Los grupos electrógenos incorporarán protecciones, arranque, conmutación, control de combustible y supervisión. La iluminación de emergencia deberá cubrir recorridos, salidas, equipos de protección y zonas definidas.
Infraestructura necesaria	Se requieren cuadros independientes, canalizaciones, protecciones, puesta a tierra, ventilación y emplazamientos seguros para baterías y generadores. Deberán considerarse inundaciones, incendios, impactos, ruido, gases de escape y acceso para repostaje. Se preverán combustible, repuestos, mantenimiento y personal autorizado. Los circuitos de seguridad se separarán de las cargas de producción cuando resulte necesario.
Estándares de interoperabilidad	Los equipos podrán comunicar tensión, carga, autonomía, combustible, alarmas y estado de conmutación mediante protocolos documentados y sistemas de supervisión. La integración con PSIM o plataformas operativas no deberá impedir el control local. Las órdenes remotas estarán autenticadas, limitadas y registradas.
Criterios de calidad y fiabilidad	• Potencia disponible y cargas prioritarias. • Autonomía de baterías y combustible. • Tiempo de conmutación. • Selectividad de protecciones. • Ausencia de puntos únicos de fallo. • Estado y vida útil de baterías. • Calidad del suministro. • Funcionamiento con carga representativa. • Recuperación tras el retorno de red. • Operación manual y modo degradado.
Compliance y seguridad	La instalación deberá cumplir el Reglamento Electrotécnico para Baja Tensión, la normativa de instalaciones temporales, prevención de incendios, grupos generadores e iluminación de emergencia que resulte aplicable. Los equipos dispondrán de marcado CE y mantenimiento documentado. El almacenamiento y repostaje de combustible, la ventilación, los gases de escape y el acceso a cuadros y baterías deberán gestionarse mediante procedimientos seguros y personal autorizado.



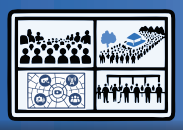
PLATAFORMAS DE GESTIÓN DE SEGURIDAD INTEGRADA, PSIM

1 Definición y fundamentos técnicos

Concepto	Una plataforma PSIM es una capa de software que integra información procedente de diferentes sistemas de seguridad y operación. Puede reunir videovigilancia, control de accesos, incendios, intrusión, megafonía, ocupación, localización y sensores en una interfaz común. No sustituye a los subsistemas conectados. Su función es relacionar sus eventos, facilitar una visión operativa compartida y apoyar la aplicación de los procedimientos establecidos.
Principios de funcionamiento	La plataforma recibe alarmas y estados mediante protocolos, API o adaptadores específicos. El motor de correlación vincula la información por ubicación, tiempo, tipología o prioridad y la presenta al operador junto con planos, cámaras y procedimientos. Los flujos de trabajo pueden recomendar acciones, generar avisos y asignar tareas. Las actuaciones con impacto sobre accesos, evacuación o información pública deberán mantener las confirmaciones humanas o interbloqueos definidos.

2 Funcionalidades y capacidades

Prestaciones clave	• Integración de subsistemas de distintos fabricantes. • Visualización geográfica de alarmas y recursos. • Correlación de eventos relacionados. • Priorización y clasificación de incidencias. • Presentación de procedimientos operativos. • Asignación y seguimiento de actuaciones. • Visualización de cámaras asociadas. • Gestión de estados y confirmaciones. • Cuadros de mando e indicadores. • Registro cronológico de eventos y decisiones. • Elaboración de informes posteriores. • Integración con centros fijos, móviles o remotos.
Diferenciación	Frente a la supervisión mediante aplicaciones y pantallas independientes, el PSIM reduce la dispersión de información y facilita que el operador relacione alarmas procedentes de varios sistemas. La plataforma no corrige los errores de los sensores ni garantiza que una alerta sea verdadera. La calidad de la visión operativa depende de los datos recibidos, la configuración de las reglas y la formación del personal.





PLATAFORMAS DE GESTIÓN DE SEGURIDAD INTEGRADA, PSIM

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta especialmente útil en estadios, festivales, recintos feriales, pabellones y eventos con numerosos subsistemas, zonas o equipos de intervención. También puede utilizarse en eventos itinerantes o distribuidos, mediante cartografía y conexiones con centros móviles o plataformas municipales.
Ejemplos de uso operativo	Una alarma de puerta forzada llega al PSIM. La plataforma muestra su ubicación, abre la cámara relacionada y presenta al operador el procedimiento aplicable. Tras verificar la situación, el operador asigna una misión al equipo correspondiente. Ante una alarma de incendio, el sistema reúne las señales de detección, las cámaras próximas, la ocupación estimada y los recursos disponibles. El responsable utiliza esta información para valorar las actuaciones previstas, sin delegar la decisión crítica en el automatismo.

4 Beneficios para los actores del evento

Para el Promotor	Permite aprovechar e integrar sistemas existentes, facilita la supervisión del dispositivo y proporciona información consolidada para evaluar su funcionamiento.
Para el Responsable de Seguridad	Reduce la necesidad de consultar plataformas independientes, ayuda a priorizar alarmas y facilita la coordinación y trazabilidad de las actuaciones.
Para el Asistente	Puede contribuir a una detección y respuesta más ordenadas al presentar conjuntamente la información relevante a los responsables del evento.
Para la Administración	Facilita el intercambio autorizado de alertas y datos con centros públicos, manteniendo diferenciadas las competencias y responsabilidades de cada organización.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá incluir conectores, motor de correlación, gestión de procedimientos, cartografía, usuarios, auditoría e informes. La arquitectura podrá implantarse localmente, en la nube o de forma híbrida. Se definirán los sistemas integrados, datos intercambiados, reglas, prioridades y acciones permitidas. Las automatizaciones deberán probarse y contar con mecanismos de control y reversión.
Infraestructura necesaria	Requiere servidores o servicios de procesamiento, almacenamiento, red segura y puestos de operación. La capacidad se dimensionará según sistemas, eventos, vídeo, usuarios y periodos de conservación. Se preverán redundancia, copias de respaldo, monitorización y procedimientos alternativos ante pérdida de la plataforma central.
Estándares de interoperabilidad	Se priorizarán API documentadas y protocolos como ONVIF para vídeo, OPC o BACnet para determinados sistemas técnicos y SNMP para supervisión de red, según su aplicabilidad. Los adaptadores propietarios deberán estar documentados y mantenerse durante el ciclo de vida. Cada integración conservará origen, marca temporal, estado y calidad del dato.
Criterios de calidad y fiabilidad	• Número y tipo de sistemas integrables. • Latencia de recepción y presentación. • Capacidad de eventos y usuarios simultáneos. • Disponibilidad y recuperación. • Redundancia de componentes. • Gestión de errores de integración. • Usabilidad y carga de información. • Trazabilidad de alarmas y decisiones. • Mantenimiento de conectores. • Funcionamiento en modo degradado.
Compliance y seguridad	La plataforma deberá aplicar autenticación robusta, control de acceso por funciones, segmentación, cifrado, registros de auditoría, copias de respaldo y gestión de vulnerabilidades. El tratamiento de imágenes, identidades, ubicaciones y registros cumplirá la normativa aplicable de protección de datos y seguridad privada. El ENS se aplicará cuando la organización o el servicio estén dentro de su ámbito. La integración no atribuye por sí sola valor probatorio a los registros ni garantiza el cumplimiento legal del evento.



GEMELOS DIGITALES Y SIMULACIÓN DE ESCENARIOS

1 Definición y fundamentos técnicos

Concepto	Un gemelo digital es una representación estructurada y actualizable de un recinto, sus infraestructuras, espacios, recursos y condiciones operativas. Puede incorporar modelos bidimensionales o tridimensionales y datos procedentes de distintos sistemas. En eventos de masas permite visualizar información, analizar flujos y comparar escenarios antes o durante la celebración. No constituye necesariamente una réplica exacta ni reproduce con certeza el comportamiento de las personas.
Principios de funcionamiento	La plataforma combina cartografía, modelos de edificios, inventarios y reglas de simulación. Puede incorporar datos de ocupación, accesos, cámaras, sensores, movilidad y recursos para actualizar la representación. Los motores de simulación utilizan hipótesis sobre velocidades, capacidades, recorridos y comportamiento colectivo para estimar la evolución de diferentes escenarios. Los resultados deben interpretarse dentro de sus márgenes de incertidumbre.

2 Funcionalidades y capacidades

Prestaciones clave	• Representación digital del recinto y su entorno. • Visualización de accesos, salidas y sectores. • Localización de recursos y activos críticos. • Integración de ocupación y datos de sensores. • Simulación de entradas, salidas y evacuaciones. • Identificación de posibles cuellos de botella. • Comparación de configuraciones y recorridos. • Evaluación de salidas bloqueadas o zonas restringidas. • Análisis de accesos para emergencias. • Representación temporal de la evolución del evento. • Apoyo a ejercicios y formación. • Registro y reproducción de escenarios.
Diferenciación	Frente a los planos estáticos, el gemelo digital permite relacionar geometría, datos y reglas operativas en un entorno común. Facilita comparar alternativas antes de modificar físicamente el recinto. Las simulaciones son estimaciones condicionadas por los datos y supuestos utilizados. No sustituyen las inspecciones, cálculos reglamentarios, simulacros ni decisiones de los responsables.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta especialmente útil en estadios, recintos feriales, festivales, edificios con varias plantas, espacios con desniveles y acontecimientos que modifican temporalmente la configuración urbana. También puede utilizarse en la fase de diseño para comparar vallados, accesos, sectores, recorridos y distribución de recursos.
Ejemplos de uso operativo	Antes del evento se simulan diferentes patrones de salida, incluyendo el bloqueo de una puerta. Los resultados muestran una posible concentración en un corredor y permiten revisar el recorrido, la señalización y la distribución del personal. Durante el evento, los datos de ocupación se representan por sectores. Cuando una zona muestra una densidad elevada, el operador contrasta la información con cámaras y equipos sobre el terreno antes de adoptar medidas. Ante una emergencia, el modelo ayuda a consultar accesos, hidrantes, cuadros eléctricos, puestos sanitarios y rutas alternativas.

4 Beneficios para los actores del evento

Para el Promotor	Permite comparar configuraciones, documentar decisiones de diseño y reutilizar el modelo en futuras ediciones o cambios del recinto.
Para el Responsable de Seguridad	Facilita una visión espacial de riesgos, recursos e incidencias y ayuda a preparar y evaluar escenarios de respuesta.
Para el Asistente	Puede contribuir a mejorar la configuración de accesos, recorridos, señalización y evacuación mediante análisis previos más completos.
Para la Administración	Facilita la coordinación territorial, la evaluación de impactos y el intercambio autorizado de modelos e información con servicios municipales y de emergencia.



5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	La solución deberá gestionar geometría, cartografía, activos, escenarios, parámetros y fuentes de datos. Podrá incluir visualización 2D o 3D, motor de simulación, series temporales y herramientas de análisis. El nivel de detalle se adaptará a la finalidad. Los elementos relevantes para seguridad deberán estar identificados, actualizados y vinculados con su fuente.
Infraestructura necesaria	Se requieren planos, cartografía, modelos o levantamientos fiables, además de capacidad de procesamiento y almacenamiento. La actualización dinámica necesitará comunicaciones e integración con sensores y plataformas. Deberán definirse responsables del modelo, procesos de actualización, control de versiones y funcionamiento con datos parciales o sin conexión.
Estándares de interoperabilidad	Se priorizarán formatos geográficos y de construcción documentados, como GeoJSON, GML, CityGML o IFC, cuando resulten adecuados, junto con servicios y API interoperables. La plataforma podrá integrarse con GIS, BIM, PSIM, IoT y plataformas de ciudad. Cada dato conservará origen, unidad, referencia espacial, marca temporal y nivel de calidad.
Criterios de calidad y fiabilidad	• Correspondencia geométrica con el recinto. • Actualización y control de versiones. • Calidad y frecuencia de los datos. • Hipótesis de comportamiento utilizadas. • Calibración con observaciones o ejercicios. • Sensibilidad de los resultados. • Tiempos de procesamiento. • Capacidad de escenarios simultáneos. • Representación de incertidumbres. • Disponibilidad y recuperación.
Compliance y seguridad	La plataforma deberá proteger modelos, ubicaciones de activos críticos, credenciales y datos operativos mediante control de accesos, cifrado, registros y copias de respaldo. Cuando incorpore posiciones o imágenes de personas, se aplicará la normativa de protección de datos. También deberán definirse la titularidad, licencias y derechos de uso de cartografía, modelos y datos aportados por terceros. Los resultados no se considerarán certificación automática de la seguridad ni única base para decisiones críticas.

REDES INTEROPERABLES Y PASARELAS DE COMUNICACIÓN ENTRE ORGANISMOS

1 Definición y fundamentos técnicos

Concepto	Estas soluciones permiten intercambiar voz, alertas y datos entre organizaciones que utilizan redes, terminales o tecnologías diferentes. Pueden conectar las comunicaciones del evento con protección civil, servicios sanitarios, Fuerzas y Cuerpos de Seguridad u otros organismos autorizados. La interoperabilidad puede resolverse mediante pasarelas técnicas, grupos compartidos, terminales de enlace o puestos de coordinación. No requiere necesariamente interconectar directamente todas las redes.
Principios de funcionamiento	Las pasarelas reciben comunicaciones de una red y las adaptan para transmitirlas a otra, convirtiendo protocolos, formatos o servicios. Las soluciones de radio sobre IP pueden enlazar canales mediante redes de datos, mientras que las plataformas de banda ancha permiten crear grupos entre radios, móviles y consolas. La configuración determina qué usuarios pueden comunicarse, qué información se comparte y qué prioridades se aplican. La cadena de mando y los procedimientos continúan bajo responsabilidad de cada organismo.

2 Funcionalidades y capacidades

Prestaciones clave	• Enlace entre redes de radio diferentes. • Creación de grupos de coordinación autorizados. • Integración de radios, teléfonos y consolas. • Intercambio de voz, mensajes y alertas. • Transmisión de posiciones o imágenes cuando proceda. • Conexión con centros de control públicos. • Utilización de terminales compatibles con redes de emergencias. • Pasarelas temporales mediante radio sobre IP. • Gestión de usuarios, grupos y prioridades. • Supervisión de enlaces y canales. • Grabación autorizada de comunicaciones. • Activación de rutas alternativas ante fallos.
Diferenciación	Frente a la transmisión de avisos mediante intermediarios, una pasarela puede permitir la comunicación directa entre grupos autorizados y reducir repeticiones o errores. No todas las redes pueden o deben interconectarse. Las diferencias de cifrado, cobertura, protocolos y competencias pueden hacer preferible utilizar terminales de enlace o mantener la coordinación a través de los centros de control.



3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resulta útil en grandes eventos deportivos, festivales, celebraciones urbanas, procesiones, cumbres y acontecimientos con participación de numerosos organismos. Es especialmente relevante cuando conviven redes privadas del organizador, radiocomunicaciones profesionales, redes públicas de emergencias y servicios de banda ancha.
Ejemplos de uso operativo	Ante una incidencia relevante, se activa un grupo de coordinación autorizado entre el centro de control, protección civil y servicios sanitarios. Cada organismo mantiene sus canales internos y utiliza el grupo común para la información necesaria. Un equipo de seguridad privada comunica un aviso a través de su red. La pasarela lo transmite al puesto de enlace, que verifica la información antes de trasladarla a la red pública correspondiente. Si falla la conexión principal entre centros, el dispositivo utiliza un enlace móvil alternativo o terminales de radio previamente asignados.

4 Beneficios para los actores del evento

Para el Promotor	Facilita la coordinación del dispositivo con los organismos públicos sin exigir la sustitución completa de las redes existentes.
Para el Responsable de Seguridad	Permite compartir información esencial con otros responsables, manteniendo grupos, prioridades y procedimientos claramente definidos.
Para el Asistente	Puede favorecer una respuesta más coordinada al reducir retrasos en la transferencia de avisos entre los servicios intervinientes.
Para la Administración	Facilita la colaboración público-privada, preservando el control de las redes públicas, los perfiles autorizados y las competencias de cada organismo.

5	Requerimientos y especificaciones técnicas
Especificaciones técnicas	La solución deberá identificar redes, terminales, protocolos, grupos, usuarios, prioridades y datos que se pretenden intercambiar. Podrá incluir pasarelas, servidores, consolas, routers, enlaces móviles y equipos de grabación. Las funciones de conexión y desconexión deberán estar controladas y permitir aislar una red ante averías, uso indebido o incidentes de ciberseguridad.
Infraestructura necesaria	Se requieren interfaces compatibles, energía de respaldo, conectividad IP segura y emplazamientos con cobertura suficiente. En eventos de gran concurrencia se coordinará con los operadores el posible refuerzo de las redes móviles. Se valorará la disponibilidad de banda ancha para emergencias y terminales compatibles. También se preverán equipos de sustitución y canales alternativos.
Estándares de interoperabilidad	Se utilizarán protocolos y API documentadas, radio sobre IP y estándares de comunicaciones de misión crítica cuando resulten aplicables. La integración deberá conservar identidad del grupo, prioridad, marcas temporales y origen de la comunicación. Las funciones de cifrado deberán ser compatibles o mantenerse separadas mediante puntos de enlace autorizados.
Criterios de calidad y fiabilidad	• Compatibilidad entre redes y terminales. • Calidad e inteligibilidad de voz. • Latencia introducida por la pasarela. • Capacidad de grupos simultáneos. • Cobertura de los enlaces. • Disponibilidad y redundancia. • Recuperación tras pérdida de conexión. • Gestión de prioridades. • Aislamiento de redes afectadas. • Funcionamiento de procedimientos alternativos.
Compliance y seguridad	El acceso a redes, frecuencias y servicios públicos requerirá autorización de sus responsables y cumplimiento de la normativa de telecomunicaciones y seguridad aplicable. Las pasarelas deberán aplicar autenticación, cifrado, control de acceso, segmentación, registro y actualización segura. La grabación y transmisión de posiciones, voz, imágenes o datos personales se limitará a las finalidades y usuarios autorizados.



PLATAFORMAS DE CIUDAD INTELIGENTE Y GESTIÓN DEL ENTORNO URBANO

1 Definición y fundamentos técnicos

Concepto	Las plataformas de ciudad inteligente permiten integrar información procedente del evento con sistemas municipales de movilidad, transporte, seguridad, emergencias, medioambiente y servicios urbanos. Su finalidad es ampliar la visión operativa más allá del recinto y facilitar la coordinación entre la organización y las administraciones competentes. Estas plataformas no sustituyen a los sistemas especializados ni transfieren competencias entre organismos. Actúan como una capa de intercambio, contextualización y visualización de información relevante para gestionar el impacto del evento sobre la ciudad.
Principios de funcionamiento	La plataforma recibe datos mediante interfaces, servicios web o pasarelas de integración. La información se normaliza, se relaciona con su ubicación geográfica y se presenta mediante mapas, cuadros de mando, indicadores y alertas. Las reglas configuradas permiten identificar situaciones como saturación viaria, acumulación de personas, interrupciones del transporte o incidencias en servicios urbanos. El intercambio podrá ser bidireccional cuando existan autorización, procedimientos y responsabilidades previamente definidos.

2 Funcionalidades y capacidades

Prestaciones clave	• Integración de información sobre ocupación y flujos de asistentes. • Visualización del evento y su entorno mediante cartografía digital. • Consulta del estado del tráfico, aparcamientos y transporte público. • Incorporación de datos meteorológicos y ambientales. • Integración con centros municipales de operaciones y emergencias. • Seguimiento de incidencias en vías, alumbrado y servicios urbanos. • Coordinación de cortes de tráfico y restricciones de acceso. • Difusión de información mediante paneles, aplicaciones y canales oficiales. • Configuración de cuadros de mando adaptados a cada organismo. • Generación de alertas por zonas y niveles de criticidad. • Registro de actuaciones y decisiones compartidas. • Análisis posterior del impacto territorial del evento.
Diferenciación	Frente a las herramientas limitadas al perímetro del evento, estas plataformas permiten relacionar la situación interior con las condiciones existentes en estaciones, calles, aparcamientos, intercambiadores y vías de evacuación. Su eficacia depende de la actualidad y calidad de los datos recibidos. La integración no implica que todos los organismos deban compartir toda su información ni que una plataforma municipal pueda asumir automáticamente el control de los sistemas del evento.

3 Aplicaciones y casos de uso en eventos

Escenarios de aplicación	Resultan especialmente útiles en estadios, festivales urbanos, carreras populares, procesiones, desfiles, celebraciones simultáneas y acontecimientos que afectan a distintos barrios o infraestructuras de transporte. También pueden utilizarse en eventos distribuidos, con varios recintos o zonas de actividad, cuya seguridad depende de la coordinación con movilidad, policía local, protección civil, transporte y servicios municipales.
Ejemplos de uso operativo	Antes de finalizar un concierto, la plataforma combina la previsión de salida con el estado del transporte público, los aparcamientos y las vías próximas. Si detecta una posible saturación, el centro de control coordina con los responsables municipales el refuerzo de recursos y la difusión de itinerarios alternativos. Durante un evento urbano, una incidencia obliga a cerrar una calle prevista como ruta de acceso. La información se comparte con los centros competentes y, tras verificar la capacidad del recorrido alternativo, se actualizan los paneles, las aplicaciones y las instrucciones al personal desplegado. Ante una emergencia, la plataforma puede facilitar a los servicios públicos la ubicación confirmada del incidente, los accesos disponibles y las restricciones existentes.

4 Beneficios para los actores del evento

Para el Promotor	Facilita la coordinación con los servicios municipales, mejora la planificación del impacto exterior y permite documentar las medidas adoptadas sobre movilidad, accesibilidad y continuidad de los servicios.
Para el Responsable de Seguridad	Proporciona una visión territorial complementaria sobre accesos, rutas de emergencia, transporte y concentraciones próximas, favoreciendo decisiones coordinadas con los organismos competentes.
Para el Asistente	Contribuye a recibir información coherente sobre accesos, transporte, restricciones e itinerarios alternativos, reduciendo la incertidumbre antes, durante y después del evento.
Para la Administración	Permite incorporar el evento a la gestión ordinaria de la ciudad, coordinar servicios y analizar sus efectos sobre la movilidad, el espacio público y las infraestructuras urbanas.



5 Requerimientos y especificaciones técnicas

Especificaciones técnicas	La solución deberá disponer de capacidades de integración, procesamiento de eventos, cartografía, cuadros de mando, gestión de alertas, control de usuarios y registro de actividad. Cada dato deberá conservar su fuente, ubicación, marca temporal, estado y nivel de calidad. Los cuadros de mando diferenciarán la información confirmada de las estimaciones o predicciones.
Infraestructura necesaria	Se requieren comunicaciones seguras, entornos de integración, servicios cartográficos y sistemas con capacidad suficiente para atender incrementos puntuales de datos y usuarios. La organización deberá definir responsables técnicos y operativos, acuerdos de intercambio de información y procedimientos alternativos ante la indisponibilidad de la plataforma o la pérdida de conectividad.
Estándares de interoperabilidad	La plataforma deberá utilizar API documentadas y formatos abiertos que faciliten el intercambio con PSIM, GIS, sistemas de movilidad, transporte y gestión de emergencias. Podrán emplearse servicios OGC, GeoJSON, NGSI-LD, MQTT u otros estándares adecuados a cada integración. Se evitarán dependencias innecesarias de soluciones propietarias. Cada interfaz deberá establecer su finalidad, frecuencia de actualización, responsable, disponibilidad y procedimiento de gestión de errores.
Criterios de calidad y fiabilidad	• Disponibilidad y capacidad de recuperación. • Latencia y frecuencia de actualización. • Exactitud, integridad y procedencia de los datos. • Escalabilidad ante concentraciones de usuarios. • Calidad de la representación cartográfica. • Gestión de datos duplicados o contradictorios. • Trazabilidad de accesos, cambios y decisiones. • Compatibilidad con los sistemas participantes. • Pruebas de integración y carga. • Funcionamiento de los procedimientos alternativos.
Compliance y seguridad	El intercambio de información deberá respetar la normativa de protección de datos y las obligaciones de ciberseguridad aplicables, incluido el Esquema Nacional de Seguridad cuando corresponda. Los acuerdos establecerán finalidades, responsables, categorías de datos, accesos y plazos de conservación. La plataforma aplicará autenticación robusta, cifrado, segmentación, registro de actividad y gestión de vulnerabilidades. Ninguna alerta deberá activar automáticamente actuaciones sobre el público, el tráfico o los servicios urbanos sin la validación y autorización previstas.



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_