Dirección Corporativa de Seguridad y Autoprotección y Aparcamientos de Concesión Municipal

Sistemas y subsistemas de seguridad electrónica

Sant Jordi Club y Palau Sant Jordi - Proyecto básico

Ajuntament de Barcelona

Mayo 2025

Videovigilancia (CCTV)

- Monitorización y grabación de espacios con cámaras IP. Incluye analítica de video: reconocimiento, detección de movimientos, lectura de matrículas, merodeo, etc.
- Instalación de cámaras inalámbricas si fuera necesario en zonas muy complejas de llegar con cable.
- Cobertura exhaustiva: Esencial para alcanzar máximos niveles de seguridad. Debe incluir:
- Accesos principales y secundarios, salidas de emergencia, pasillos, áreas deportivas, almacenes.
- El perímetro exterior.
- Accesos específicos como el de personal BSM, proveedores y descarga.
- Áreas críticas como salas de racks, salas eléctricas, CPD, Centro de Control de Seguridad (CCS).
- Puntos estratégicos interiores, como túnel de proveedores/trabajo o acceso proveedores específicos.

Videovigilancia (CCTV)

Requisitos técnicos clave: Cobertura y características de las cámaras

- El diseño debe alinearse con una estrategia de protección en profundidad, **definiendo anillos de seguridad (privativa, protegida, crítica)** y asegurando que el CCTV contribuya a cubrir los accesos y el perímetro de esos anillos.
- **Instalar cámaras IP de alta resolución**: Fundamentales para una identificación clara de individuos y actividades, ofreciendo calidad superior y funcionalidades avanzadas. Se recomienda el uso de cámaras IP antivandálicas en exteriores y zonas de alto riesgo.
- **Operación continua**: Las cámaras deben funcionar las 24 horas del día, los 7 días de la semana, con grabación continua.
- **Visión nocturna**: Es crucial garantizar el rendimiento en condiciones de baja iluminación. Es necesaria la instalación de cámaras con tecnología infrarroja (IR) para asegurar una vigilancia nocturna efectiva. Incrementar la iluminación exterior también mejora la visibilidad y efectividad del CCTV.
- **Resistencia y durabilidad**: Las cámaras, especialmente en exteriores y zonas vulnerables, deben ser resistentes al vandalismo (IK10) y a las

condiciones climáticas (IP67).

Videovigilancia (CCTV)

Dirección Corporativa de Seguridad y Autoprotección y Aparcamientos de Concesión Municipal

Requisitos técnicos clave: Cobertura y características de las cámaras

Ubicación	Cobertura	Tipos de cámara	Características
Entradas y salidas	Monitorizar el acceso y la salida de personas	Cámara IP Domo fija Cámara IP bala	Visión nocturna, posibilidad de LPR en accesos de vehículos
Área de Recepción	Supervisar interacciones con visitantes y control de acceso	Cámara IP Domo fija	Discreta, buena calidad de imagen para identificación facial
Pasillos y zonas de circulación	Rastrear movimientos internos y detectar presencias no autorizadas	Cámara IP Domo fija Cámara IP bala	Amplio campo de visión
Áreas deportivas (gimnasio, pistas, campos)	Garantizar la seguridad durante las actividades y prevenir el vandalismo	Cámara IP Domo fija Cámara IP PTZ	Resistente a impactos, amplio campo de visión, posibilidad de PTZ para cobertura extensa
Almacenes y áreas de equipos	Prevenir robos y accesos no permitidos	Cámara IP Domo fija Cámara IP bala	Buena calidad de imagen para identificación
Áreas de estacionamiento	Disuadir el robo y el vandalismo de vehículos	Cámara IP bala con IR Cámara IP con LPR	Resistente a la intemperie (IP rating), visión nocturna, posibilidad de LPR
Vallas y puertas perimetrales	Detectar intentos de entrada no autorizada	Cámara IP bala con IR (exterior)	Resistente a la intemperie (IP rating), amplio campo de visión
Áreas con equipos de alto valor	Vigilancia enfocada a activos sensibles	Cámara IP Domo fija de alta resolución	Máxima calidad de imagen para identificar detalles

Puntos de acceso vulnerables (secundarios)	Cubrir todos los posibles puntos de entrada Sistemas seguridad Sant Jordi Club y Palau 2025	Cámara IP Domo fija Cámara IP bala Sant Jordi - Proyecto básico. Mayo	Discreta si es necesario

Requisitos técnicos clave: Gestión, almacenamiento e integración

- **Sistema de gestión de vídeo (VMS)**: La integración con un VMS robusto y escalable es necesaria para la gestión, almacenamiento y recuperación eficiente. Un VMS permite visualización en tiempo real, búsqueda de acontecimientos y configuración. Las cámaras se integrarán con:
  - **El VMS XProtect de Milestone instalado en el CCS de Calàbria 66.**
  - **El VMS XProtect de Milestone instalado en el Palau Sant Jordi.**

- **Almacenamiento seguro y redundante:** Esencial para la disponibilidad de pruebas y para prevenir la pérdida de datos críticos. Es necesario establecer políticas de retención adecuadas. La redundancia del Centro de Control de Seguridad mejora la resiliencia del sistema de gestión.

- **Sincronización temporal:** Las grabaciones deben estar sincronizadas con marcas de tiempo y fecha precisas para su validez como evidencia.

- **Conectividad:** Evaluar el uso de conectividad inalámbrica para flexibilidad, y tecnología PoE para simplificar la instalación.

Requisitos técnicos clave: (CCTV) Gestión, almacenamiento e integración

- **Integración de sistemas**: El diseño ha de contemplar la integración del CCTV con otros sistemas de seguridad para una gestión centralizada y una respuesta eficaz.
  - ***Integración con PSIM (Physical Security Information Management)***: Centralizar todos los incidentes de seguridad (incluyendo vídeo) para mejorar la capacidad y rapidez de respuesta. Eso permitirá la integración con sistemas de detección de intrusión que también estén integrados con el PSIM, característica fundamental para permitir el posicionamiento automático de cámaras en el *videowall* o monitores ante la detección de acontecimientos de seguridad, facilitando la verificación y rápida respuesta.

  - ***Integración con sistemas de control de acceso:*** Permite la grabación automática cuando tienen lugar acontecimientos de acceso y facilita su gestión integrada.

- ***Interconexión con otros dispositivos de entrada/salida (E/S) según el caso de***

BSM Videovigilancia (CCTV)

Funcionalidades avanzadas y optimización operativa

- **Analíticas de vídeo inteligentes (IA)**: Implementar analíticas para la detección proactiva de actividades sospechosas. Esto incluye ***detección de movimiento en áreas restringidas***, ***merodeo***, ***análisis de comportamiento***, ***conteo de personas***, ***identificación de objetos abandonados***. Las analíticas impulsadas por IA mejoran la seguridad al automatizar la detección de acontecimientos potenciales.

- **Acceso remoto**: Permitir el acceso remoto seguro para personal autorizado (seguridad, gestores) para facilitar la supervisión y la respuesta desde cualquier ubicación. Las aplicaciones móviles pueden permitir la visualización de transmisiones en vivo. Debe garantizarse la seguridad en el acceso a través de redes públicas.

- **Máscaras de privacidad**: Utilizar funciones de enmascaramiento para excluir de la grabación áreas que no son relevantes para la seguridad o donde la vigilancia sería desproporcionada.

- **Diseño ergonómico del Centro de Control**: Considerar la disposición y las herramientas del Centro de Control de Seguridad (CCS) para optimizar la eficiencia

operativa del personal que monitoriza el sistema de videovigilancia. Esto incluye la disposición de monitores y la automatización de la visualización ante acontecimientos.

Cumplimiento normativo y protección de datos (RGPD/AEPD/LOPDGDD)

- El diseño del sistema ha de cumplir rigurosamente las normativas de protección de datos y privacidad, como el RGPD, las directrices específicas de la AEPD y la LOPDGDD.
- **Protección de datos desde el diseño y por defecto (Privacy by Design/by Default):** La protección de datos debe estar presente en las primeras fases de concepción del proyecto. Eso se traduce en medidas técnicas y organizativas integradas en el diseño y especificaciones del sistema.
- **Deber información: Utilizar un sistema de información de doble capa.**
  - Es una obligación fundamental. El distintivo informativo (cartel) de la Instrucción 1/2006 es de uso obligatorio con fines de seguridad y ha de situarse en todos los accesos a las zonas vigiladas.
  - El cartel (primera capa) ha de indicar la existencia del tratamiento, la identidad del responsable, la posibilidad de ejercer los derechos (art. 15 a 22 RGPD) y dónde obtener más información. Un QR puede enlazar más detalles. La información adicional (segunda capa) se puede facilitar por otros medios, como una política de privacidad en la web o impresos disponibles.

Detección de amenazas físicas

- Incluye detectores de armas blancas y escáneres de personas, bolsas y/o equipajes mediante rayos X u ondas milimétricas.
- APP de comunicación de incidentes de seguridad en espacio en carga a los servicios de seguridad.
- Complementando el control de accesos, la detección proactiva de amenazas físicas es un pilar fundamental para garantizar un entorno seguro dentro del recinto, especialmente durante acontecimientos masivos y en las áreas sensibles del recinto.
- Los principios clave son:
  - Detección de armas en accesos masivos.
  - Control de la paquetería y objetos que llegan al recinto.
  - Gestión de alertas.
- Para un acceso ágil y seguro a los eventos, se implementarán detectores de armas de barras con tecnología magnética de banda ancha. Estos sistemas discriminarán eficazmente objetos cotidianos para focalizarse en amenazas reales, optimizando el flujo de personas y reduciendo las interrupciones por falsas alarmas.
- En la recepción en las oficinas del Palau Sant Jordi, disponer de un escáner de rayos X

para el control de la paquetería entrante.

Detección de amenazas físicas

Alertas

- Habría que disponer de una APP de comunicación de alertas a los equipos de seguridad con integración en el PSIM (Physical Security Information Management).
- Esta APP debe permitir generar alertas en tiempo real, visualización de la ubicación de la alerta, posibilidad de comunicar incidentes, etc.

Control de acceso

- El objetivo principal de los controles de accesos previstos es garantizar la seguridad de las personas, la protección de los bienes y la salvaguardia de la información, gestionando de manera eficiente y segura el flujo de individuos y vehículos en todas las áreas.
- **Los principios clave sobre los que debe diseñarse son**:
- **Seguridad por capas:** Implementar diferentes niveles de seguridad y tecnologías de identificación adaptados a la criticidad de cada zona.
- **Flexibilidad y escalabilidad:** Diseñar un sistema modular que permita adaptarse a las necesidades cambiantes y posibles futuras ampliaciones del recinto o de sus usos.
- **Trazabilidad:** Registrar de manera fiable y inalterable todos los accesos e intentos de acceso para propósitos de auditoría e investigación forense.
- **Integración:** Conectividad total con el sistema PSIM (Physical Security Information Management) existente para una gestión centralizada y correlación de acontecimientos con otros sistemas de seguridad (CCTV, alarmas, etc.).
- **Resiliencia:** Garantizar la operatividad del sistema ante posibles fallos técnicos o cortes de suministro eléctrico.
- Regular la entrada y salida de personas. Incluye tarjetas RFID y tornos motorizados.
- A partir de análisis específico, implantar cerraduras y llaves electrónicas, eliminando las llaves mecánicas en los edificios.
- Armarios electrónicos de llaves.

- Posibilidad operaciones en remoto de apertura, cierre y comprobación por cámara.
- Conexión a CRA y redundante con CCS Calàbria y Centro Control Palau Sant Jordi.

Control de acceso

Acceso con vehículos automatizado

- Lectura de matrículas (LPR/ANPR) para vehículos autorizados (proveedores, personal clave, etc.).
- Lectura de tarjetas/identificadores RFID de largo alcance para personal acreditado con vehículo.
- Integración con bases de datos de vehículos autorizados y listas negras.
- Incorporar *road blockers* en accesos estratégicos para reforzar la seguridad perimetral, de forma que permita mitigar los posibles ataques terroristas con vehículos. Han de ser dispositivos con capacidad de detener vehículos pesados a gran velocidad y han de poder ser controlados desde el CCS de Palau Sant Jordi, CCS de Calàbria, CRA y de forma local desde el punto de control en el acceso (si existe). Han de disponer de iluminación led para alertar de su presencia y evitar choques accidentales y de certificaciones de su robustez ante impactos.

Control de acceso

Pulsadores de pánico con interfonía

- Instalar pulsadores de pánico en zonas críticas, tanto de acceso del público a eventos como en zonas privadas, con sistemas de interfonía integrados en el PSIM.
- Estos equipos de interfonía han de tener una segunda funcionalidad: la de permitir generar alarmas de forma autónoma en caso de detectar ruidos inesperados según franjas horarias.

Control de acceso

Zona de oficinas, salas técnicas y espacios restringidos (vestuarios, *backstage*, etc.)

- Instalar controles de acceso con lectores de tarjetas (donde sea posible ubicar tornos para acceder) tanto en las entradas como en las salidas de oficinas y equipamientos técnicos, tanto para los trabajadores propios del recinto como para las empresas subcontratadas. Estos lectores también tendrán que estar integrados en el PSIM.
- Mejorar la gestión de las llaves de las puertas para mejorar la trazabilidad y minimizar el riesgo de extravíos o usos indebidos; se propone un sistema con doble opción de apertura en cada puerta que permita mejorar el control de quien accede a cada ámbito:
  - Cerradura electrónica con apertura mediante tarjeta, *smartphone* o *smartwatch*.
  - Cerradura tradicional con apertura mediante llave que esté custodiada en armario inteligente de gestión de llaves. Esta segunda opción permitiría resolver posibles incidencias en casos excepcionales del primer sistema o por si a cierto personal no se le quisiera dar acceso al sistema.
  - Establecimiento de perfiles de usuario con permisos definidos para acceder a zonas específicas durante franjas horarias determinadas (personal de mantenimiento, limpieza, seguridad, personal de oficinas, organizadores de eventos, etc.).
  - Las puertas habrán de tener posibilidad de cierre remoto con visualización por cámara desde los centros de control.
  - Reforzar las medidas de seguridad en salas con activos de alta criticidad (salas de servidores, CCS, etc.) mediante cámaras que registren las personas que acceden a las mismas para tener un control forense en caso de cualquier incidencia.

- Los sistemas de acceso a las cerraduras electrónicas y armario inteligente habrán de estar integrados en el PSIM y deberán disponer de conexión con el CCS de Calàbria, CCS de Palau Sant Jordi y CRA.

Detección de intrusión

Requisitos clave del diseño: Normativa y grado de seguridad

- El diseño y la instalación del sistema de intrusión ha de cumplir estrictamente la normativa española aplicable en seguridad privada.
- Esto incluye la Ley 5/2014 de Seguridad Privada, el Reglamento de Seguridad Privada (RD 2364/1994) y las órdenes ministeriales correspondientes (INT/316/2011 e INT/314/2011).
- La instalación solo pueden realizarla empresas de seguridad debidamente autorizadas de acuerdo con la Orden INT/314/2011.
- Es fundamental el cumplimiento de las normas europeas UNE-EN de la serie 50131, que establecen requisitos generales para sistemas de alarma contra intrusión y atraco, así como especificaciones para sus componentes (detectores, centrales, interconexiones, fuentes de alimentación). También aplica la norma UNE-EN 50136 para la transmisión de señales.
- La normativa UNE-EN 50131 define diferentes grados de seguridad según el riesgo.
- El sistema debe ajustarse, como mínimo, al grado 2 (riesgo medio) según UNE-EN 50131-1. Este grado es adecuado para entornos con amenazas moderadas.
- Considerando el objetivo de máxima seguridad para la remodelación del pabellón, se puede requerir un nivel de protección superior, como el grado 3 (riesgo medio/alto), destinado a establecimientos con riesgo significativo o que requieran medidas avanzadas.
- Todos los componentes del sistema han de cumplir los estándares UNE-EN aplicables y tener certificados de homologación. El grado de seguridad general del sistema estará limitado por el componente de menor grado.

- Los sistemas conectados a una central receptora de alarmas (CRA), como será el caso, han de tener un grado de seguridad adecuado al riesgo (grado 2 o 3).

Detección de intrusión

- **Principales objetivos del sistema de detección de intrusión**
  - Conseguir una detección precoz y precisa (mediante la zonificación) de accesos no autorizados.
  - Cubrir los puntos de acceso perimetrales (puertas, ventanas, vallas) y el movimiento interno.
  - Asegurar una respuesta inmediata mediante la integración con una central de alarmas.
  - Proteger los activos críticos y las salas sensibles.
  - Garantizar la fiabilidad operativa (protección contra manipulaciones, redundancia, copia de seguridad).
  - Facilitar la gestión eficiente de incidencias a través de una plataforma centralizada.
  - Mejorar la protección general y eliminar las vulnerabilidades.
  - Cumplir con la normativa española pertinente.
- Sensores de movimiento, contactos magnéticos y barreras infrarrojas para detectar accesos no autorizados. Análisis de los espacios para definir tipologías.

- Conexión a CRA y redundante con CCS Calàbria y Centro Control Palau Sant Jordi.

Detección de intrusión

Dirección Corporativa de Seguridad y Autoprotección y Aparcamientos de Concesión Municipal

Requisitos clave del diseño: Arquitectura y componentes

- **Central de alarma**: Será el núcleo del sistema. Debe ser una central de intrusión con capacidad para gestionar alarmas por zonas y contar con funciones de autodiagnóstico, autoarmado, armado parcial/nocturno/temporizado y registro de acontecimientos. Debe permitir configuración, diagnóstico y mantenimiento remotos. Idealmente, la central debe estar certificada para grado 3.
- **Detectores**: Se instalarán para la detección temprana de accesos no autorizados tanto en el perímetro como en el interior.
  - Incluirán detectores volumétricos distribuidos estratégicamente según los niveles de seguridad y zonas de valor.
  - Se preverán detectores de doble tecnología (infrarrojos/microondas) con antienmascaramiento en puntos críticos como accesos, pasillos y zonas con activos valiosos. Podrán ser de largo alcance si es necesario. Los detectores volumétricos serán de tipo convencional.
  - Pueden contemplarse otros tipo de detectores específicos según la vulnerabilidad (contactos magnéticos, etc.).
- **Sirenas**: El sistema contará con dispositivos de aviso sonoro y/o visual.
  - Sirenas interiores, certificadas y con protección contra manipulación (*tamper*). Se recomiendan de bajo perfil.
  - Sirenas exteriores, óptico-acústicas y protegidas contra manipulación.
- **Control y acceso al sistema**: Se instalarán consolas con pantallas LCD y teclado alfanumérico para el control del sistema. El diseño debe asegurar que solo el usuario autorizado pueda armar y desarmar.
- **Interconexiones**: Las conexiones entre los componentes del sistema serán cableadas y dedicadas (no

compartidas con otros sistemas). El cableado ha de ser inaccesible, oculto, bien sujeto y cumplir las

especificaciones del fabricante y normativas de baja tensión. Se emplearán elementos de canalización libres.

Detección de intrusión

Requisitos clave del diseño: Arquitectura y componentes

- **Comunicación**: La central ha de transmitir las señales a una CRA y al PSIM del CCS de Calàbria 66 y al PSIM del CCS del Palau Sant Jordi.
  - La vía principal será un módulo de comunicación bidireccional TCP/IP (Ethernet), que permite conexión a múltiples destinos y avisos.
  - Se contará con una vía de apoyo mediante un módulo de comunicación GPRS/3G para garantizar la comunicación en caso de fallo de la red IP.
- **Alimentación**: El sistema incluirá fuentes de alimentación supervisadas y batería de respaldo para asegurar el funcionamiento ante cortes de suministro eléctrico. La instalación eléctrica del sistema ha de cumplir el Reglamento Electrotécnico de Baja Tensión.
- Zonificación del sistema. Aunque las fuentes se centran en la zonificación para sistemas de detección de incendios, el principio es aplicable a la detección de intrusión: **dividir la instalación en áreas o zonas lógicas y físicas para localizar con precisión cualquier acontecimiento de alarma**.
- La zonificación permite optimizar la respuesta al incidente, ya sea por parte del personal interno (como el equipo de intervención en emergencias en un plan de autoprotección) o de los servicios externos.
- El diseño debe alinearse con los estándares locales, nacionales e internacionales, garantizando el cumplimiento de los requisitos de riesgo y nivel de protección. Aunque el documento menciona un mínimo de grado 2, la evaluación de riesgos y el objetivo de "máxima seguridad" pueden orientar hacia un grado 3 en función de las áreas a proteger y los activos presentes.

- La zonificación ha de tener en cuenta las características específicas de las instalaciones y

Detección de intrusión

Requisitos clave del diseño: Instalación y puesta en marcha

- **Diseño y planificación**: La empresa instaladora ha de presentar una propuesta de diseño del sistema y un plan de instalación (en su caso) basados en la norma UNE-EN 50131-7 y un estudio técnico detallado del lugar.
- **Instalación**: Los componentes han de instalarse según las recomendaciones del fabricante y ser adecuados para las condiciones ambientales. Se tomarán medidas para proteger los equipos durante la instalación y asegurar su accesibilidad futura para mantenimiento. La instalación eléctrica ha de cumplir la normativa vigente.
- **Calidad de materiales**: Todos los elementos del sistema han de estar aprobados u homologados de acuerdo con las normas europeas aplicables a cada tipo de componente.
- **Pruebas e inspección:** Una vez completada la instalación, el personal técnico realizará una inspección para confirmar que se ha ejecutado según la propuesta de diseño y el estudio técnico. Se llevarán a cabo ensayos para verificar el correcto funcionamiento de cada detector, componente y dispositivo de aviso.
- **Verificación de alarmas**: La CRA tendrá que implementar procedimientos de verificación (secuencial, vídeo, audio, personal) para confirmar la autenticidad de las señales de alarma antes de notificarlas a las

Fuerzas y Cuerpos de Seguridad del Estado (FCS). La CRA ha de disponer de como mínimo dos operadores y transmitir inmediatamente las alarmas reales a la policía. El sistema ha de ser capaz de diferenciar claramente entre una señal de alarma y una señal de sabotaje.

Detección de intrusión

Zonificación: Identificación de zonas potenciales

- La división en zonas permite adaptar las medidas de seguridad a las características y el nivel de riesgo de cada área.
- Algunas zonas potenciales a considerar incluyen:
  - **Áreas de acceso y recepción**: Punto principal de entrada/salida del edificio.
  - **Pista polideportiva**: El área de juego principal. Dependiendo de su tamaño, podría subdividirse.
  - **Graderíos y pasarelas para espectadores**: Zonas de alta ocupación durante acontecimientos, pero vacías y susceptibles a intrusión fuera de ellos.
  - **Vestuarios y lavabos**: Espacios auxiliares asociados a la práctica deportiva.
  - **Almacenes**: Áreas que suelen contener equipamiento deportivo u otros activos valiosos. Estas zonas pueden presentar un riesgo más elevado.
  - **Oficinas y áreas de administración**: contienen información y posiblemente equipos administrativos [Mencionado como área auxiliar en tipo de pabellones grandes, similar al Plan de autoprotección que sitúa la central de incendios en administración].
  - **Salas de instalaciones técnicas**: Incluyendo cuadros eléctricos, calderas, sistemas de acumulación, etc. Son áreas críticas por el potencial de sabotaje.
  - **Cafetería/Bar**: Zona de servicio con acceso público.
  - **Espacios exteriores**: Pistas exteriores, áreas de aparcamiento, perímetros.

Detección de intrusión

Zonificación: Criterios y componentes del sistema

- La definición de las zonas se basa en diversos criterios:
  - **Función y uso:** Agrupar áreas con propósitos parecidos (ej.: zonas de acceso, zonas deportivas, zonas técnicas).
  - **Nivel de riesgo**: Zonas que contienen activos valiosos o instalaciones críticas (almacenes, salas técnicas, oficinas) pueden requerir zonas separadas y posiblemente detectores más sensibles o redundancia.
  - **Posibilidades de armado/desarmado parcial**: Permitir la activación del sistema en ciertas áreas mientras otras están en uso (ej.: armar almacenes y oficinas mientras la pista está abierta).
  - **Facilidad de localización**: Cada zona debe corresponderse con un área fácilmente identificable en planos o en el terreno para una respuesta rápida y eficiente.
- **Delimitación física**: Las zonas han de respetar las barreras arquitectónicas y la compartimentación del edificio. Dentro de cada zona, deben instalarse detectores apropiados para el tipo de espacio (detectores de movimiento, contactos magnéticos en puertas y ventanas, detectores de rotura de cristal, etc.) que cumplan los estándares requeridos para el grado de seguridad definido.
- Las señales de alarma han de incluir información clara sobre la ubicación del sensor activado (la zona) para facilitar la verificación y respuesta inmediata.
- La integración con sistemas de videovigilancia puede permitir la verificación en tiempo real de las

intrusiones en la zona afectada.

Detección de intrusión

Elementos de detección: Criterios de selección y tipos

- Los detectores son dispositivos clave que informan a la central de alarmas sobre las variaciones en las áreas protegidas.
- Existen varios tipos de detectores de intrusión, clasificados por su actitud (activos o pasivos), zona de vigilancia (puntuales, lineales, planares, volumétricos) y ubicación (perimetrales, periféricos, de interior).
- **Criterios clave para la elección del detector**:
  - **Tipo de material a proteger:** Materiales blandos (madera, cristal, ladrillo) *vs.* superficies duras (hormigón armado, acero estructural, cajas fuertes).
  - **Naturaleza del ataque potencial**: Ataques con herramientas contundentes o fuerza bruta (golpes, roturas) *vs.* ataques más sofisticados (taladros diamantados, sierras mecánicas, explosivos, herramientas térmicas).

- **Ubicación en el modelo de protección multicapa**: Perímetro, periferia o interior.

Detección de intrusión

Elementos de detección: Criterios de selección y tipo

- **Tipo de detectores relevantes:**
  - **Detectores de impacto/vibración/inerciales**: Identifican ataques físicos con herramientas contundentes sobre materiales como madera, cristal o ladrillo. Están regulados por la norma UNE-EN 50131-2-8. Se recomienda su uso en elementos estructurales vulnerables como puertas, ventanas o tabiques interiores. Son detectores pasivos y planares o puntuales, utilizados en áreas perimetrales/periféricas/interiores.
  - **Detectores sísmicos**: Captan vibraciones sutiles, de baja frecuencia y larga duración, generadas por ataques sofisticados como agujeros, sierras, explosivos o herramientas térmicas. Su aplicación está regulada por la norma alemana VdS 2331. Son imprescindibles en superficies duras expuestas a sabotajes complejos, como cajeros automáticos, cámaras acorazadas, cajas fuertes o muros de hormigón armado o acero estructural. Son detectores pasivos y superficiales, recomendados para áreas perimetrales.
  - **Detectores de movimiento (volumétricos)**: Detectan cambios de temperatura (pasivos infrarrojos - PIR) o emiten energía (microondas, ultrasonidos) para detectar irregularidades a través del efecto Doppler (activos). **Los detectores Dual Tec combinan tecnologías PIR y microondas para**

reducir falsas alarmas. Están diseñados para captar el desplazamiento del intruso a partir de las perturbaciones que origina ese movimiento en las condiciones ambientales. Son detectores volumétricos, principalmente interiores.

Detección de intrusión

Elementos de detección: Selección de detectores por zonas

Aplicación del modelo de protección multicapa y los criterios de selección:

- **Área perimetral**: La primera capa externa, definida por el perímetro.
  - Para detectar intentos de intrusión a través de la superficie o línea del contorno (vallas, muros exteriores).
  - Considerar detectores inerciales o de cable sensor para detección sobre vallas o muros.
  - Para muros de hormigón o acero, o áreas de alto riesgo en el perímetro, donde se esperen ataques sofisticados (perforación, corte), los detectores sísmicos son imprescindibles.
  - En espacios al aire libre dentro del perímetro, se pueden utilizar detectores de movimiento perimetrales activos (radares, sonares). Se recomienda instalar dos o más

anillos de seguridad perimetral con diferentes principios de funcionamiento y áreas de detección solapadas para instalaciones de alto riesgo.

– La vigilancia perimetral ofrece precocidad en la detección.

Detección de intrusión

Elementos de detección: Selección de detectores por zonas

Aplicación del modelo de protección multicapa y los criterios de selección:

- **Área periférica**: Superficies próximas a los edificios (contornos de las edificaciones).
  - Vulnerabilidades como puertas, ventanas, lucernarios, muros y superficies de cristal.
  - Para puertas y ventanas vulnerables a ataques con herramientas contundentes, utilizar detectores de impacto o vibración.
  - Complementar con contactos magnéticos en puertas y ventanas para detectar aperturas.
  - Utilizar detectores de rotura de cristal para ventanas.

– Estos detectores (impacto, magnéticos, rotura de cristal) pueden ser puntuales o superficiales y se utilizan en áreas perimetrales/periféricas/interiores.

Detección de intrusión

Elementos de detección: Selección de detectores por zonas

- **Área interior**: Diseñada para detectar intrusos que han penetrado capas externas.
  - Espacios cerrados como salas, oficinas, vestuarios, pasillos.
  - Los detectores volumétricos, principalmente detectores infrarrojos pasivos (PIR) y detectores de microondas (o combinados), son los más característicos para detectar el desplazamiento de personas.
  - En áreas de alto riesgo interior, como salas técnicas o zonas de almacenamiento de equipamiento valioso, la elección dependerá del tipo de ataque esperado y materiales a proteger, y también pueden requerirse detectores de impacto o sísmicos si se protegen elementos específicos como cajas fuertes.

– Los sistemas de videovigilancia (CCTV) son elementos irrenunciables en la protección interior para soporte, verificación, detección y análisis.

Detección de intrusión

Elementos de detección: Selección de detectores por zonas

- **General**: La certificación grado 3 o 4 implica requisitos específicos para los equipos y la instalación. En instalaciones de alto riesgo (grado 4), se espera que los intrusos tengan una completa gama de equipos, incluyendo medios de sustitución de componentes vitales, lo que exige medios para detectar retraso, modificación o sustitución de señales. Es crucial asegurar la fiabilidad de los sistemas, especialmente en grado 4, combinando detectores con lógicas como Y (And) para reducir falsas alarmas.

Detección de intrusión

Elementos de detección: Selección de detectores por zonas

Tipo de detector	Área de colocación recomendada	Consideraciones específicas
Contacto magnético	Puertas y ventanas exteriores y accesos internos restringidos	Protección contra manipulación
Detector de movimiento PIR	Pasillos internos, áreas deportivas principales, espacios abiertos	Ajustar sensibilidad para evitar falsas alarmas
Detector de doble tecnología (PIR y microondas)	Áreas de alto tráfico o ambientes con posibles falsas alarmas	Mayor inmunidad a falsas alarmas

Detector de rotura de cristales	Grandes superficies de cristal	Sensibilidad adecuada al tipo de cristal
Botón de pánico	Área de recepción, oficina del gerente, ubicaciones estratégicas	De fácil acceso en caso de emergencia

Detección de intrusión

Integración con otros sistemas: Ventajas clave

- **Validación visual de alarmas**: La integración con la videovigilancia (CCTV) permite que la Central Receptora de Alarmas (CRA) o el personal de seguridad visualicen en tiempo real qué ocurre cuando se activa una alarma de intrusión. Esto ayuda a verificar la autenticidad de la señal y reduce las falsas alarmas.
- **Respuesta coordinada y efectiva**: La conexión del sistema de intrusión con otros dispositivos de seguridad, tales como sensores de movimiento, alarmas y sistemas de control de acceso, a través de la integración (por ejemplo, mediante IoT), facilita una respuesta coordinada y efectiva ante cualquier incidente.
- **Seguridad perimetral completa**: Se puede conseguir un sistema de seguridad perimetral mediante el uso de sistemas combinados que incluyen detección de intrusión, videovigilancia y barreras físicas. La detección temprana de un intento de

intrusión puede activar la alarma y permitir la acción disuasoria.

Detección de intrusión

Integración con otros sistemas: Ventajas clave

- **Mejora de la gestión de accesos**: Los sistemas de control de acceso regulan la entrada y salida de personas autorizadas, lo que complementa la seguridad del sistema de intrusión al prevenir activamente el acceso no autorizado a áreas sensibles. La integración permite, por ejemplo, que una detección de intrusión en una zona de acceso active una verificación de acceso o restrinja la salida.
- **Información integral para la toma de decisiones**: La combinación de información de diferentes sistemas (intrusión, CCTV, control de accesos) proporciona una visión más completa de la situación, mejorando la capacidad de respuesta y la gestión de la seguridad en general.
- **Potencial para la automatización**: la integración permite automatizar respuestas; por ejemplo, una alarma de intrusión puede activar cámaras específicas para grabar o

enfocar la zona afectada, o desencadenar acciones en el sistema de control de acceso.

Detección de intrusión

Integración con otros sistemas: Requisitos para el sistema de intrusión

- **Conexión a Central Receptora de Alarmas (CRA)**: Para ser plenamente operativo y permitir una gestión profesional de las señales, el sistema de intrusión debe estar conectado a una CRA debidamente registrada y autorizada. Esto es fundamental para la recepción, verificación y gestión de alarmas las 24 horas. Las comprobaciones de mantenimiento de un sistema de intrusión incluyen el test de conexión a la CRA.
- **Infraestructura de red y cableado adecuados**: Un cableado correcto y una infraestructura de red apta son cruciales para el ejercicio y la gestión de los sistemas de seguridad, incluido el de intrusión. Los problemas y errores en los equipos a menudo se deben a infraestructuras deficientes o de baja calidad. Es vital utilizar materiales de calidad y bajo estándares normativos para asegurar una mayor seguridad y evitar pérdidas o ruidos en la señal.
- **Soporte para comunicación bidireccional**: La evolución de los sistemas de intrusión incluye centrales bidireccionales avanzadas. La comunicación bidireccional es importante para que la

CRA pueda monitorizar el estado del sistema, verificar señales (incluyendo videoverificación) y gestionar el sistema remotamente.

Detección de intrusión

Integración con otros sistemas: Requisitos para el sistema de intrusión

- **Capacidad de integración con otros sistemas**: el sistema de intrusión debe tener la compatibilidad o las interfaces necesarias para integrarse con otros sistemas de seguridad como la videovigilancia (VMS), la gestión de información de la seguridad física (PSIM) y las plataformas IoT. Esto permite que los sistemas intercambien información y actúen de manera conjunta.
- **Fiabilidad de los elementos de detección y control**: la eficacia de la integración depende de la fiabilidad de los elementos individuales. Los sistemas modernos de intrusión utilizan detectores de doble tecnología con microprocesadores que confirman la señal antes de emitirla, mejorando la eficiencia.
- **Mantenimiento regular del sistema**: un requisito fundamental para asegurar el correcto funcionamiento y la integración eficaz es el mantenimiento regular del

sistema de intrusión, así como de los sistemas de videovigilancia y control de accesos con los que se integra.

Control de aforo

- Sistema de control de aforo en tiempo real y sectorización por zonas o utilización según usos del espacio.
- Aplicación para su control a partir de dispositivos móviles y en el Centro de Control del Palau Sant Jordi y en el CCS Calàbria.
- La gestión eficiente y segura del aforo es esencial, especialmente en un recinto que acoge eventos masivos. El control preciso de la densidad de personas en las diferentes zonas es crucial para garantizar la seguridad, facilitar la evacuación en caso de emergencia y optimizar la experiencia del público.

- Los principios clave serán:

  - Control en tiempo real y sectorización dinámica.
  - Gestión inteligente de colas.
  - Generación automática de alarmas.
  - Monitorización y visualización.
  - Capacidad de generación de informes con patrones de movimiento y distribución del público según la tipología del evento.
- Sistema inteligente de control de aforo en tiempo real con sectorización dinámica por zonas (por ejemplo, gradas divididas por secciones en un partido o zona de pista segmentada por tipo de entrada en un concierto).
- Gestión inteligente de colas en los accesos del Palau Sant Jordi y el Sant Jordi Club, con capacidad para contabilizar personas y estimar tiempos de espera.
- El sistema se basa en inteligencia artificial (IA) aplicada al análisis de vídeo.
- Control y monitorización accesibles desde dispositivos móviles y el Centro de Control del Palau Sant Jordi y el CCS Calàbria, con integración en el sistema de gestión de vídeo (VMS) existente.

Sistema de control de aforo

Funcionamiento del sistema

- Generación automática de alarmas al detectar exceso de aforo en sectores específicos (áreas de gradas o sectores de la pista).
- Generación automática de alarmas al detectar acumulaciones inusuales de personas en las colas o sobrepasar una cierta longitud.
- El sistema generará mapas de calor en tiempo real para una visualización intuitiva e inmediata de la densidad del aforo en todo el recinto.
- Deberá proporcionar informes estadísticos sobre patrones de movimiento, densidad y distribución del público durante cada evento. Estos informes deberán alertar si durante los eventos se ha sobrepasado el aforo en algún sector.

Sistema de control de aforo

Informes

- Deberá proporcionar métricas clave sobre la eficiencia de los accesos, como el promedio de personas procesadas por cola por unidad de tiempo (por ejemplo, personas por minuto por cola), para identificar posibles cuellos de botella.
- El sistema generará un *dashboard* con el análisis agregado del comportamiento de varios eventos similares (como conciertos) para identificar patrones que optimicen la seguridad, los recursos y la experiencia del público en el futuro.

Detección y alarma de incendios

- Detectar humo, calor o gas. Incluir alarmas acústicas y visuales, integradas con sistemas de evacuación.
- Elementos cortafuegos y de confinamiento.
- Conexión a CRA y redundancia en el Centro de Control del Palau Sant Jordi y CCS Calàbria. Integración en *scada* y en PSIM.

Detección y alarma de incendios

Contexto, objetivo y normativa aplicable

- **Objetivo:**
  - Establecer reglas y procedimientos para cumplir las exigencias básicas de seguridad en caso de incendio.
  - La correcta aplicación del conjunto del Documento Básico SI (DB SI) satisface el requisito básico "Seguridad en caso de incendio".
- **Normativa aplicable:**
  - Código Técnico de la Edificación (CTE) - Documento Básico SI (DB SI). Su aplicación es obligatoria en el ámbito establecido para el CTE.
  - Reglamento de Instalaciones de Protección contra Incendios (RIPCI) (Real Decreto 513/2017), que cubre diseño, instalación, mantenimiento e inspección.
  - Normas UNE, UNE-EN, UNE-EN ISO, que son fundamentales para la aplicación del DB SI. La normalización apoya la protección contra incendios.

Detección y alarma de incendios

Criterios de diseño

- **Cumplimiento normativo:**
  - El diseño del sistema debe cumplir los requisitos establecidos en el CTE-DB SI (sección SI 4) y en el RIPCI.
  - El contenido del proyecto debe ser conforme a lo establecido en la norma UNE 157001, sin perjuicio de lo que establezcan las administraciones competentes.
- **Soporte en normas UNE:**
  - Las normas UNE y UNE-EN, como las de la serie UNE-EN 54 (implicada en el Anexo SIG que lista normas relacionadas con la aplicación del DB SI), son fundamentales para el diseño.
- **Enfoques de diseño:**
  - Se puede seguir un enfoque prescriptivo basado en el cumplimiento directo de las especificaciones normativas.
  - Se puede optar por un diseño basado en prestaciones (DBP), que es una metodología única

para cada edificio analizado.

Detección y alarma de incendios

Criterios de diseño

- **Comunicación**: La central debe transmitir las señales a una CRA y al PSIM del CCS de Calàbria 66 y al PSIM del CSS del Palau Sant Jordi.
  - La vía principal será un módulo de comunicación bidireccional TCP/IP (Ethernet), que permite conexión a múltiples destinos y avisos.
  - Se contará con una vía de apoyo mediante un módulo de comunicación GPRS/3G para garantizar la comunicación en caso de fallo de la red IP.
- **Alimentación**: El sistema incluirá fuentes de alimentación supervisadas y batería de respaldo para asegurar su funcionamiento ante cortes de suministro eléctrico. La instalación eléctrica del sistema debe cumplir el Reglamento Electrotécnico de Baja Tensión.

Detección y alarma de incendios

Diseño basado en prestaciones (DBP)

- **Concepto de DBP:**
  - Es una metodología de trabajo estructurada aplicable a cualquier estudio prestacional.
  - Permite el estudio preciso de las consecuencias de un incendio en un edificio concreto.
- **Metodología del DBP:**
  - Fase inicial de análisis de los riesgos del incendio, a menudo mediante una evaluación probabilística.
  - Generación de una matriz de riesgo para ubicar riesgos y asignar un índice de riesgo global.
  - Evaluación de los escenarios más desfavorables con un índice de riesgo global severo.
- **Pilares del análisis prestacional:**
  - Uso de métodos analíticos o modelos informáticos (modelos de zona) para obtener temperaturas y leyes tiempo-temperatura.
  - Consideración de parámetros como la geometría, características de cierres y propiedades del combustible.

Detección y alarma de incendios

Zonificación y áreas de detección obligatoria

- **Propósito de la zonificación:**
  - La zonificación del sistema de alarma de incendio facilita la rápida identificación de la ubicación del incendio por parte de los servicios de emergencia.
  - Permite una notificación rápida a los ocupantes.
- **Criterios generales de zonificación:**
  - El sistema debe zonificarse para corresponder con la distribución del edificio.
  - Esto puede incluir la zonificación por planta o por área de uso.
  - Se recomienda crear zonas separadas para el pabellón deportivo principal, las salas auxiliares y las áreas exteriores.

Detección y alarma de incendios

Elementos de detección: Tipos de detectores y detección de gases

- **Tipologías de detectores de incendio:**
  - **Detectores de humo**: Incluyen iónicos, fotoeléctricos y de detección por aspiración (ASD). Cruciales para la detección temprana del humo.
  - **Detectores de calor**: De temperatura fija o velocidad de aumento. Adecuados donde el humo no es apropiado.
  - **Detectores multisensor**: Combinan tecnologías de humo y calor.
  - **Detectores de llama**: Detectan la presencia de llamas.
- **Dispositivos de activación manual:**
  - Es necesario instalar puntos de llamada manuales (pulsadores).
  - Ubicación: cerca de todas las salidas y en ubicaciones estratégicas a lo largo de las rutas de evacuación.
- **Consideración de detección de gases:**
  - Los detectores de monóxido de carbono (CO) son importantes en áreas con fuentes potenciales de CO, como por ejemplo en aparcamientos interiores o subterráneos.

Detección y alarma de incendios

Elementos de detección: Selección y ubicación por zonas

Zona	Tipo de detector recomendado	Justificación de la selección
Pabellones	Detector de humo fotoeléctrico o detector multisensor	Detección temprana de incendios latentes en grandes áreas
Oficinas	Detector de humo fotoeléctrico	Detección temprana en áreas de oficina
Cocinas/*Office*	Detector de calor (velocidad de aumento)	Menos propenso a falsas alarmas por vapor o humo
Vestuarios con duchas	Detector de calor (temperatura fija)	Adecuado para ambientes húmedos
Almacenes de equipos	Detector de humo fotoeléctrico, o detector de humo por aspiración (ASD) para áreas de alto valor	Detección temprana en materiales almacenados, ASD para detección muy temprana de activos

Pasillos y zonas de circulación	Detector de humo fotoeléctrico o detector multisensor	Detección temprana en rutas de evacuación

Detección y alarma de incendios

Integración con otros sistemas: Sistemas complementarios

- **Integración con la seguridad general:**
  - El diseño de la seguridad en grandes pabellones deportivos incluye la evaluación de riesgos en áreas como emergencia y evacuación.
  - La detección es parte del plan general de seguridad.
- **Integración con sistemas de evacuación:**
  - La detección de incendios está estrechamente ligada a los sistemas de evacuación.
  - Los planes de evacuación son relevantes y mencionados en el contexto del RIPCI.
  - Las rutas de evacuación deben detallarse en el proyecto.
- **Sistemas de señalización y alumbrado de emergencia:**
  - El RIPCI considera los sistemas de señalización luminiscente. Los instaladores se pueden encargar de colocar señales y planos de evacuación.
  - La señalización debe ser coherente con la evacuación.
  - El alumbrado de emergencia debe entrar en funcionamiento ante fallos de tensión, y es crucial en las rutas de evacuación. Los itinerarios accesibles para personas con discapacidad requieren señalización específica.

Detección y alarma de incendios

Integración con otros sistemas: Requisitos para el sistema de incendios

- **Conexión a Central Receptora de Alarmas (CRA)**: Para ser plenamente operativo y permitir una gestión profesional de las señales, el sistema de detección de incendios debe estar conectado a una CRA debidamente registrada y autorizada. Esto es fundamental para la recepción, verificación y gestión de alarmas las 24 horas. Las comprobaciones de mantenimiento de un sistema de detección de incendios incluyen el test de conexión a la CRA.
- **Infraestructura de red y cableado adecuados**: Un cableado correcto y una infraestructura de red apta son cruciales para el ejercicio y la gestión de los sistemas de seguridad, incluido el de detección de incendios. Los problemas y errores en los equipos a menudo se deben a infraestructuras deficientes o de baja calidad. Es vital utilizar materiales de calidad y bajo estándares normativos para asegurar una mayor seguridad y evitar pérdidas o ruidos en la señal.
- **Soporte para comunicación bidireccional**: La evolución de los sistemas de detección de incendios incluye centrales bidireccionales avanzadas. La comunicación bidireccional es importante para que la CRA pueda monitorizar el estado del sistema, verificar señales

(incluyendo videoverificación) y gestionar el sistema remotamente.

Detección y alarma de incendios

Integración con otros sistemas: Requisitos para el sistema de incendios

- **Capacidad de integración con otros sistemas**: el sistema de detección de incendios debe tener la compatibilidad o las interfaces necesarias para integrarse con otros sistemas de seguridad como la videovigilancia (VMS), la gestión de información de la seguridad física (PSIM) y el control de procesos (SCADA). Esto permite que los sistemas intercambien información y actúen de manera conjunta.
- **Fiabilidad de los elementos de detección y control**: la eficacia de la integración depende de la fiabilidad de los elementos individuales.
- **Mantenimiento regular del sistema**: Un requisito fundamental para asegurar el correcto funcionamiento y la integración eficaz es el mantenimiento regular del sistema de detección de incendios, así como de los sistemas de videovigilancia y

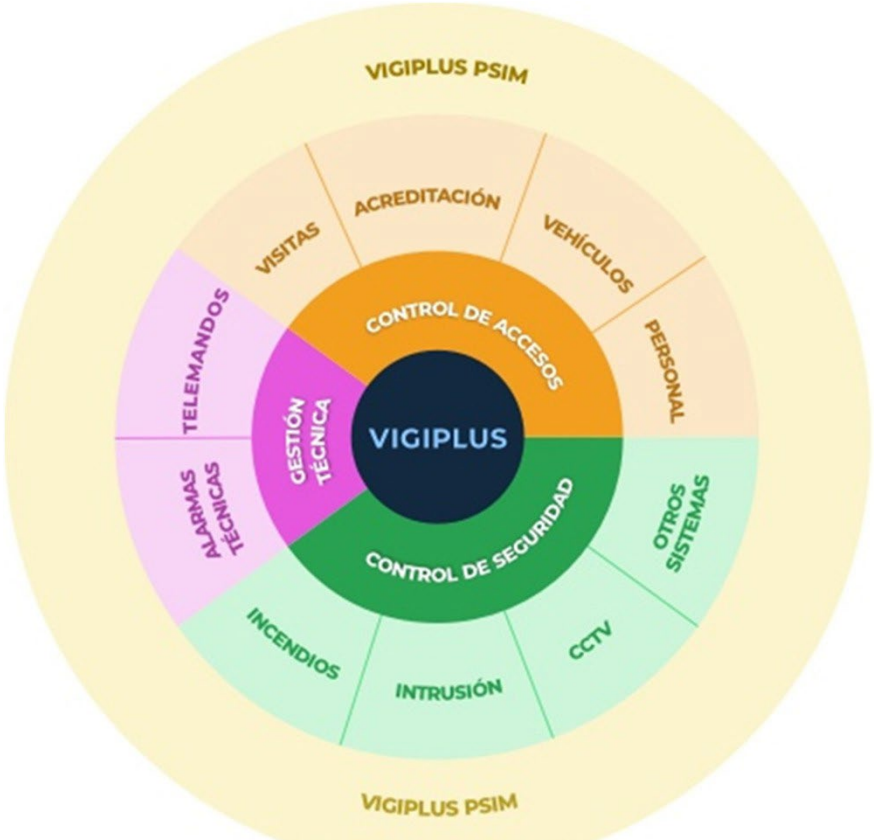
control de accesos con los que se integra.

Subsistemas auxiliares

- Incluye SAI, servidores Milestones, Racs, Switz y otros elementos de TIC y sistemas.
- Barreras y puertas automáticas para operar en remoto.
- Portaarmas e integración con sistemas inteligentes de edificios (BMS).
- Otros subsistemas auxiliares a concretar.

PSIM
(Physical Security Information Management)

- Plataforma de gestión que integra todos los subsistemas en una única interfaz para el control y análisis de incidentes (Vigiplus)



Centro de Control de Seguridad: Comunicaciones y gestión centralizada

- Centros de control con interfaces gráficas para la gestión remota y coordinada de la seguridad.
- Renovación Centro de Control Palau Sant Jordi de toda la Anella Olímpica (Estadi Olímpic, Palau Sant Jordi, Sant Jordi Club, Explanada Olímpica).
- Conexión con el Centro de Control de Seguridad de Calàbria y Servicio Central con las Operaciones. Operaciones en remoto.
- Creación UCO en el Sant Jordi Club.
- Mejora y renovación UCO del Palau Sant Jordi.