basque culinary center

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN PARA LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE SEGURIDAD ELECTRÓNICA DE ANTI INTRUSIÓN Y CCTV PARA EL EDIFICIO GOe DE BASQUE CULINARY CENTER FUNDAZIOA

ÍNDICE GENERAL

1 PLIEGO DE PRESCRIPCIONES TÉCNICAS 3
1.1 OBJETO Y ALCANCE DEL CONTRATO 3
1.2 CONDICIONES DEL SUMINISTRO E INSTALACIÓN 4
1.3 NORMATIVA DE APLICACIÓN 5
1.4 REQUISITOS DE APERTURA E INTEROPERABILIDAD 7
1.5 RECEPCIÓN, PRUEBAS Y VALIDACIÓN FINAL 9
1.5.1 PROCEDIMIENTO DE RECEPCIÓN 9
1.5.2 INFORME DE PRUEBAS 9
1.5.3 GARANTÍA DE LA CALIDAD FINAL 9
1.6 DOCUMENTACIÓN FINAL Y ENTREGA DE AS-BUILT 9
1.7 GARANTÍA, MANTENIMIENTO 10
1.8 REQUISITOS DE CIBERSEGURIDAD 10
1.9 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS 12
1.10 LEGALIZACIÓN FINAL Y GESTIONES ANTE ORGANISMOS 13
1.11 DOCUMENTACIÓN TÉCNICA ACREDITATIVA 13
1.12 CLÁUSULA DE EQUIPAMIENTO NUEVO 14
1.13 CLÁUSULA DE TRANSFERENCIA DE CONOCIMIENTO 14
1.14 CLÁUSULA “LLAVE EN MANO” 16
2 ANEXO 1. ESPECIFICACIONES DEL SISTEMA 18
2.1 TABLAS EQUIPOS Y MATERIALES A SUMINISTRAR 18
2.1.1 SISTEMA ANTI-INTRUSIÓN 18
2.1.2 SISTEMA DE VIDEO-VIGILANCIA IP 18
2.1.3 SISTEMA DE VMS 19
2.2 ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS A SUMINISTRAR 19
2.2.1 SISTEMA ANTI-INTRUSIÓN 19
2.2.1.1 CENTRAL DE SEGURIDAD Y ALARMAS 19
2.2.1.2 MÓDULO DE COMUNICACIÓN ETHERNET 21
2.2.1.3 TECLADO ALFANUMÉRICO 21
2.2.1.4 MÓDULO EXPANSOR 22
2.2.1.5 CONTACTO MAGNÉTICO SENCILLO 22
2.2.1.6 DOBLE DETECTOR MOVIMIENTO POR INFRARROJOS 23
2.2.1.7 SIRENA EXTERIOR 23
2.2.1.8 CANALIZACIONES Y CABLEADO DEL SISTEMA ANTI-INTRUSIÓN 24
2.2.1.9 CONFIGURACIÓN Y PUESTA EN MARCHA DE TODO EL SISTEMA ANTI-INTRUSIÓN 25
2.2.2 SISTEMA DE VIDEO-VIGILANCIA IP 28
2.2.2.1 GRABADOR DE 64 CANALES 28

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

2.2.2.2 DISCO DURO DE 10 TB 29
2.2.2.3 CÁMARA BULLET IP DE 4 MPX. 30
2.2.2.4 CÁMARA MINIDOMO IP DE 4 MPX. 31
2.2.2.5 CÁMARA DOMO MOTORIZADA PTZ IP DE 4 MPX. 32
2.2.2.6 UNIDAD DE LICENCIAMIENTO DE TODO EL SISTEMA DE VIDEOVIGILANCIA (VER PLATAFORMA VMS) 33
2.2.2.7 CANALIZACIONES Y CABLEADO HASTA CADA CÁMARA 35
2.2.2.8 CONFIGURACIÓN Y PUESTA EN MARCHA DE TODO EL SISTEMA DE VIDEOVIGILANCIA 35
2.2.3 SISTEMA DE VMS 36
2.2.3.1 PLATAFORMA VMS 37
2.2.3.2 WORKSTATION 39
2.2.3.3 INSTALACIÓN Y PUESTA EN MARCHA DEL VMS 40

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

1 PLIEGO DE PRESCRIPCIONES TÉCNICAS

1.1 OBJETO Y ALCANCE DEL CONTRATO

El objeto del contrato consiste en el suministro, instalación, configuración y puesta en marcha de un sistema integral de seguridad electrónica anti-intrusión y de videovigilancia IP y su integración en un VMS para el edificio GOe, situado en Av. de Navarra, nº 9, CP 20013, Donostia/San Sebastián (en adelante, "Edificio GOe"), donde desarrolla su actividad BASQUE CULINARY CENTER FUNDAZIOA (en adelante, "BCCF").

Las características técnicas del suministro al que hace referencia este pliego, se encuentran en el **ANEXO I** adscrito al final del presente Pliego de Prescripciones Técnicas.

El presente pliego define con precisión todas las funciones, responsabilidades y trabajos que el adjudicatario deberá llevar a cabo para garantizar una correcta y completa ejecución del contrato. Estas prescripciones técnicas son de obligado cumplimiento tanto durante la fase de licitación como durante la ejecución material de los trabajos.

La instalación contemplada será de tipo "llave en mano", debiendo quedar completamente montada, instalada, configurada, probada y operativa, incluyendo todas las certificaciones, documentación técnica, legalizaciones pertinentes y planos finales "as-built" según las normativas vigentes.

Los equipos y materiales objeto del suministro deberán ajustarse estrictamente a los planos de instalación y especificaciones técnicas incluidos en los Anexos I, II y III del presente pliego.

Las actividades y tareas incluidas en la presente licitación comprenden, como mínimo, las que se indican a continuación; su ejecución es de carácter obligatorio e ineludible para el adjudicatario:

- Revisión técnica in situ y replanteo inicial del proyecto, contrastando la correspondencia entre planos, mediciones y condiciones reales del edificio. Cualquier desviación detectada deberá documentarse y someterse a aprobación de la Dirección Facultativa (DF) antes de iniciar los trabajos.
- Suministro, instalación, configuración, integración y puesta en marcha del sistema completo (detección anti-intrusión, videovigilancia IP y plataforma VMS) con arreglo a las especificaciones y cantidades consignadas en el ANEXO 1.
- Despliegue y ajuste de todos los componentes físicos y lógicos: cámaras IP, NVR, clientes de vídeo, y accesorios, dejando cada elemento plenamente operativo y etiquetado.
- Integración funcional del nuevo equipamiento con la infraestructura de red, sistemas de seguridad existentes y, en su caso, con la Central Receptora de Alarmas (CRA), asegurando la interoperabilidad y el intercambio de eventos en tiempo real.
- Coordinación técnica continua con otras contratas y con la DF, planificando cortes, pruebas y accesos de forma que se minimice cualquier interferencia con la actividad ordinaria del BCCF.
- Ejecución de pruebas FAT/SAT: ensayos funcionales, operativos y de ciberseguridad (credenciales robustas, cifrado, logs) conforme al plan de pruebas aprobado; subsanación inmediata de no conformidades.
- Entrega de documentación final y legalización, incluyendo:
    - Certificados de instalación y conformidad normativa.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

- Manuales de usuario y servicio en castellano.
- Planos “as-built” y esquemas actualizados en PDF/DWG.
- Copia de seguridad de configuraciones y licencias activadas.
- Trámites ante Industria, Telecomunicaciones y AEPD, cuando proceda.
- Alta en seguridad privada

1.2 CONDICIONES DEL SUMINISTRO E INSTALACIÓN

Todas las actuaciones deberán ejecutarse llave en mano, cumpliendo la normativa europea, estatal y autonómica vigente (UNE-EN 62676, UNE 50131, REBT, CPR-EN 50575, RGPD, LOPDGDD, Ley 7/2022 de residuos, etc.). Cualquier texto que sustituya o modifique dichas normas será de igual obligado cumplimiento.

A. Cumplimiento normativo y certificaciones

- Todos los equipos y materiales deberán llegar a obra con:
  - Declaración UE de conformidad (marcado CE).
  - Certificados CPR, RoHS, ENEC y Grado 3 UNE 50131, según proceda.
- El adjudicatario entregará, a requerimiento de BCCF, trazabilidad de lotes y registros de control de calidad de fábrica.

B. Conformidad con los anexos técnicos

- Los equipos se ajustarán estrictamente a las especificaciones y ubicaciones de los Anexos I, II y III.
- Cualquier elemento indispensable omitido deberá suministrarse sin incremento de coste.

C. Verificación de la infraestructura existente

- Antes de instalar cada dispositivo, el adjudicatario comprobará que el punto de red existente soporta IEEE 802.3at/802.3bt y dispone de un budget ≥ 30 W ± 20 % por cámara.
- Toda incidencia se comunicará por escrito a la Dirección Facultativa (DF).

D. Instalación y puesta en servicio

- Entregar cada equipo con todos los patch-cords Cat 6A CPR Cca, accesorios de fijación y elementos de interconexión necesarios.
- Montar los dispositivos en su ubicación definitiva, dejándolos plenamente operativos y etiquetados.
- Ejecutar las pruebas FAT/SAT aprobadas; subsanar las no conformidades antes de la Recepción Provisional.

E. Gestión ambiental y residuos

- Retirar embalajes, cables sobrantes y residuos al término de cada jornada.
- Gestionar RAEE y otros desechos conforme a Ley 7/2022 y RD 553/2020, aportando certificados de gestor autorizado.

F. Documentación y formación

- Durante la ejecución, el adjudicatario pondrá a disposición de la DF los manuales de instalación, fichas técnicas y guías de configuración preliminares, en formato PDF.

- Estos documentos son de uso operativo en obra y serán sustituidos o completados por el expediente final as-built regulado en el apartado 1.6.
- Impartirá, antes de la puesta en marcha, una formación inicial (≥ 4 h) sobre operación y mantenimiento básico.

G. Coordinación y seguridad en obra

- Mantener coordinación permanente con la DF y otras contratas, asistiendo a las reuniones convocadas.
- Ajustar planificación para no interferir la actividad docente/investigadora del centro.
- Cumplir sin coste extra el Plan de Seguridad y Salud, empleando medios auxiliares y EPI adecuados.

H. Derecho de rechazo de suministros

- BCCF y la DF podrán rechazar cualquier elemento que no acredite su conformidad o presente defectos; la reposición será a cargo del adjudicatario, sin repercusión económica ni ampliación de plazo.

Todos los compromisos anteriores tienen carácter de obligación esencial (art. 211.f LCSP) y su cumplimiento será verificado durante la Recepción Definitiva.

1.3 NORMATIVA DE APLICACIÓN

Las actividades incluidas en el presente contrato deberán ajustarse, en todo momento, a la legislación y normativa técnica vigente de ámbito europeo, estatal y autonómico. De manera no limitativa, se citan las disposiciones de referencia:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Ley 5/2014, de 4 de abril, de Seguridad Privada
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada
- Real Decreto 842/2002, de 2 de agosto, por el que se aprueba el Reglamento Electrotécnico para Baja Tensión (REBT)
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica
- Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada
- Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada y su personal y medios materiales
- Reglamento (UE) 305/2011 del Parlamento Europeo y del Consejo, de 9 de marzo, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción (CPR)

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

- Norma armonizada EN 50575:2024, Cables de energía, control y comunicación. Cables para aplicaciones generales en obras de construcción sujetos a requisitos de reacción al fuego
- Directiva 2014/35/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de material eléctrico destinado a utilizarse con determinados límites de tensión (LVD)
- Norma EN 62368-1:2024, Equipo de audio/vídeo, tecnologías de la información y de las comunicaciones. Requisitos de seguridad
- Directiva 2014/30/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la armonización de las legislaciones de los Estados miembros en materia de compatibilidad electromagnética (EMC)
- Normas EN 55032, EN 55035, EN 61000-6-2 y EN 61000-6-3, Compatibilidad electromagnética para equipos multimedia e industriales
- Directiva 2011/65/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos (RoHS)
- Directiva 2012/19/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, sobre residuos de aparatos eléctricos y electrónicos (RAEE)
- Normas UNE-EN 50131 (serie completa) Sistemas de alarma. Sistemas de alarma contra la intrusión y el atraco
- Norma UNE-EN 60839-11-1, Sistemas de alarma y de seguridad electrónica. Requisitos generales para sistemas de intrusión y atraco
- Norma UNE-EN 60839-11-2, Sistemas de alarma y de seguridad electrónica. Requisitos para los sistemas de transmisión
- Normas UNE-EN 50136-1-1 y UNE-EN 50136-1-2, Sistemas de alarma. Sistemas y equipos de transmisión de alarmas
- Normas UNE-EN 62676 (serie completa) Sistemas de videovigilancia por CCTV
- Normas UNE-EN 50518 (serie completa) Estaciones de recepción y gestión de alarmas
- Estándar ONVIF Profile M, Edición 2021, Servicios de metadatos y analítica de vídeo
- Norma UNE-CEN/TS 50136-7, Sistemas de alarma. Requisitos de servicio. Directrices para la verificación por vídeo de alarmas
- Normas UNE-EN 50173 (serie completa) Tecnologías de la información. Sistemas de cableado genérico
- Normas UNE-EN 50174 (serie completa) Tecnologías de la información. Instalación de cableado
- Norma UNE-EN 60529, Grados de protección proporcionados por las envolventes (códigos IP)
- Norma UNE-EN 62262, Grados de protección proporcionados por las envolventes contra impactos mecánicos externos (códigos IK)
- Normas UNE-EN 62305 (serie completa) Protección contra el rayo
- Norma ISO/IEC 27001:2022, Tecnología de la información. Sistemas de gestión de la seguridad de la información. Requisitos
- Norma ISO/IEC 27002:2022, Tecnología de la información. Código de buenas prácticas para controles de seguridad de la información
- Normas IEC 62443-4-1 e IEC 62443-4-2, Seguridad para sistemas de automatización y control industrial. Requisitos de componentes

- Guía de la Agencia Española de Protección de Datos «Tratamientos de videovigilancia» (edición 2023)
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2)
- Norma ISO 9001:2015, Sistemas de gestión de la calidad. Requisitos
- Norma ISO 14001:2015, Sistemas de gestión ambiental. Requisitos con orientación para su uso
- Norma ISO 50001:2018, Sistemas de gestión de la energía. Requisitos con orientación para su uso

En caso de derogación, modificación o sustitución de cualquier norma durante la vigencia del contrato, serán de obligado cumplimiento los textos que la sustituyan.

En relación con los materiales y certificaciones:

- Todos los equipos y materiales deberán ser de primeras marcas y contar con la documentación acreditativa (declaración CE, certificados de ensayo, fichas CPR, homologaciones UNE-EN / ISO) que demuestre su conformidad normativa.
- Queda prohibido suministrar material sin la aprobación previa y expresa de BCCF.

En relación con la cartelería de videovigilancia:

- El adjudicatario colocará, sin coste adicional, los carteles informativos de videovigilancia conforme al modelo recomendado por la Agencia Española de Protección de Datos (AEPD).
- Su diseño, dimensiones, contenido y ubicación requerirán la validación previa de BCCF y deberán garantizar la visibilidad clara para todas las personas afectadas.

El adjudicatario mantendrá a BCCF informada de forma continua sobre la normativa aplicable y sus modificaciones, indicando cómo afectan al alcance y a la ejecución del contrato.

La omisión de esta obligación informativa dará lugar a las responsabilidades que procedan; los trámites y costes de subsanación serán íntegramente por cuenta del adjudicatario.

1.4 REQUISITOS DE APERTURA E INTEROPERABILIDAD

A fin de garantizar la **independencia tecnológica** de BCCF y la **evolución futura** del sistema, todo el hardware y software suministrado (cámaras, NVR, VMS, módulos de intrusión, pasarelas y licencias asociadas) deberá cumplir los requisitos mínimos siguientes:

Nº	Exigencia	Alcance / detalle obligatorio
1	**Protocolos abiertos**	• Todos los flujos de vídeo IP deberán ser plenamente compatibles con ONVIF Perfil S (streaming), Perfil G (grabación) y Perfil M (metadatos y analítica).

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

		● Las alarmas de intrusión y los eventos de vídeo deberán poder intercambiarse mediante SIA DC-09 (Contact-ID sobre IP) o REST API/JSON estandarizado.
2	**API documentado**	● El VMS/NVR entregará API RESTful y/o SDK que exponga, como mínimo, las funciones de autenticación, consulta de cámaras, control PTZ, búsqueda/descarga de grabaciones, alta/baja de usuarios y recepción/emisión de eventos. ● La documentación (Developer Guide) se entregará en PDF y HTML en castellano o inglés, sin requerir registro previo en portales del fabricante.
3	**Licencias y costes**	● El SDK/API deberá suministrarse sin coste adicional, sin royalties ni cánones presentes o futuros. ● Cualquier clave, fichero de activación o librería necesaria para compilar o integrar aplicaciones de terceros formará parte del suministro “llave en mano”.
4	**Pruebas de interoperabilidad**	● El adjudicatario presentará, antes de la recepción provisional, un script de ejemplo (Postman collection o equivalente) que demuestre: ○ Alta de una cámara mediante API. ○ Consulta en tiempo real del estado de una alarma de intrusión. ○ Recuperación de metadatos ONVIF M (json/xml) de una analítica perimetral. ● Estas llamadas formarán parte de la checklist de aceptación.
5	**Derecho de uso perpetuo**	● BCCF dispondrá de licencia perpetua para utilizar la API/SDK en desarrollos propios o de terceros sin limitación de tiempos, usuarios ni puestos-cliente, salvo uso contrario a la ley o reventa del código fuente.
6	**Obsolescencia y versiones**	● El fabricante garantizará, por escrito, que las funciones expuestas en la API/SDK estarán soportadas durante al menos 5 años desde la fecha de recepción. ● Las nuevas versiones deberán mantener retrocompatibilidad o publicarse notas de migración.

La documentación a entregar por el adjudicatario en relación a lo anterior será la siguiente:

- Declaración de conformidad ONVIF (archivo. cert o carta del fabricante).
- Manual de integración (PDF) y enlace a repositorio de ejemplos.
- Listado de endpoints REST, parámetros y respuestas.
- Licencia de uso y confirmación de ausencia de costes futuros firmada por el fabricante/distribuidor.

La falta de cualquiera de los requisitos anteriores facultará a BCCF para rechazar la oferta o exigir su cumplimiento sin variación de precio, de acuerdo con la cláusula “Llave en mano”.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

1.5 RECEPCIÓN, PRUEBAS Y VALIDACIÓN FINAL

1.5.1 PROCEDIMIENTO DE RECEPCIÓN

- Plan de pruebas previo. Con una antelación mínima de 10 días naturales, el adjudicatario remitirá a BCCF y a la Dirección Facultativa (DF) un Plan de Pruebas que contendrá como mínimo:
  - Pruebas funcionales de cada subsistema (anti-intrusión, videovigilancia IP y VMS).
  - Ensayos de interoperabilidad (red IP, bus de intrusión, notificaciones, acciones cruzadas).
  - Verificación de calidad de imagen y analíticas inteligentes.
  - Comprobaciones básicas de ciberseguridad (credenciales robustas, cifrado HTTPS/TLS, registro de logs).
- Visita de validación. En la fecha acordada se efectuará la visita de recepción con la presencia de la DF y representantes de BCCF. Se ejecutará in situ la checklist aprobada y se verificará el cumplimiento íntegro de las prestaciones contractuales.
- Acta de recepción. Solo cuando todos los puntos resulten conformes se firmará el Acta de Recepción. Las no conformidades detectadas deberán solventarse en el plazo fijado por BCCF, sin coste adicional para la Propiedad.

1.5.2 INFORME DE PRUEBAS

Al finalizar los ensayos, el adjudicatario entregará a la DF un Informe de Validación firmado por su responsable técnico, que incluirá:

- Resultado “conforme / no conforme” de cada prueba.
- Evidencias gráficas (capturas de pantalla, fotografías, registros).
- Extracto de alarmas y eventos y su correcta visualización en consola y NVR/VMS.
- Informe resumido de ciberseguridad (usuarios, contraseñas, cifrado activo, logs).

1.5.3 GARANTÍA DE LA CALIDAD FINAL

La firma del Acta de Recepción no exime al adjudicatario de subsanar defectos ocultos o fallos de funcionamiento detectados dentro del período de garantía contractual. Cualquier intervención derivada de dichas incidencias será ejecutada sin coste para BCCF y sin interferir en la operativa del edificio.

1.6 DOCUMENTACIÓN FINAL Y ENTREGA DE AS-BUILT

A la finalización de los trabajos —y condición previa a la Recepción Provisional— el adjudicatario entregará un dossier definitivo con la siguiente estructura:

- Planos actualizados (PDF + DWG)
  - Trazado de canalizaciones y cableado.
  - Ubicación exacta de cámaras, detectores y armarios.
- Esquemas eléctricos, lógicos y topológicos firmados por técnico competente.
- Inventario detallado (XLS)

  - Modelo, nº de serie, firmware y ubicación de cada equipo.
- Copias de seguridad
  - Archivo “backup” de la configuración del sistema de intrusión.
  - Exportación de la base de datos y parámetros de la VMS.
- Manual de usuario definitivo (PDF)
  - Operativa básica: creación de usuarios, armado/desarmado, búsqueda de grabaciones.
- Manual técnico (PDF)
  - Procedimientos de calibración, mantenimiento preventivo y resolución de incidencias.
- Certificados y legalizaciones
  - Conformidad normativa (RD 2364/1994, UNE-EN 62676, UNE 50131).
  - Justificante de inscripción DGP/CRA y, cuando proceda, comunicaciones a la AEPD.
- Medio de entrega
  - Soporte USB o disco cifrado + enlace seguro para descarga.
  - Hasta dos copias impresas si BCCF lo solicita.

El dossier as-built será revisado por la Dirección Facultativa. La subsanación de deficiencias documentales es responsabilidad del adjudicatario y no interrumpirá los plazos de garantía.

1.7 GARANTÍA, MANTENIMIENTO

La garantía de la instalación global será de dos años mínimo, a partir de la recepción provisional positiva de la totalidad del sistema. La garantía incluirá durante todo el periodo la reparación y sustitución de componentes, con intervención de personal técnico in-situ, con un tiempo de respuesta (según oferta del instalador) a contar desde la notificación formal de la avería.

La empresa instaladora debe comprometerse a subsanar cualquier vicio oculto de la instalación y de los equipos sin cargo alguno para el Responsable del Contrato.

1.8 REQUISITOS DE CIBERSEGURIDAD

El sistema de videovigilancia IP y anti-intrusión deberá cumplir, como mínimo, los controles que se establecen a continuación, alineados con el Esquema Nacional de Seguridad (ENS, RD 311/2022) en nivel ALTO, la IEC 62443-4-1/4-2, la ISO/IEC 27002:2022 y las guías CCN-STIC aplicables. Todas las obligaciones aquí descritas se consideran esenciales a efectos del artículo 211.f) LCSP.

Bloque de control	Requisito prescriptivo
A. Gestión de credenciales	1. Todas las cámaras, grabadores, servidores VMS y consolas deberán disponer de credenciales únicas y robustas (≥ 12 caracteres, entropía equivalente, prohibidas cadenas por defecto).

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

	2. Se implementará autenticación multifactor (MFA) para accesos de privilegio a VMS/NVR y portal web. 3. Rotación obligatoria de contraseñas de cuentas administrativas cada 90 días.
B. Comunicación cifrada	1. Todo acceso de gestión se realizará mediante HTTPS/TLS 1.2 o superior con cifrado AES-256. 2. Las secuencias de vídeo ONVIF deberán ir encapsuladas en SRTP/TLS o HTTPS streaming. 3. Las conexiones remotas de mantenimiento se efectuarán exclusivamente a través de VPN IPSec IKEv2 o canal SSH con MFA y restringidas por lista blanca de IP.
C. Hardening de dispositivos	1. Deshabilitar protocolos y servicios no utilizados (Telnet, UPnP, HTTP, SNMPv1/2c, IPv6 si no procede). 2. Configurar arranque seguro, validación de firma de firmware y protección frente a downgrade. 3. Cambiar puertos por defecto y limitar intentos de login (Bloqueo tras 5 intentos fallidos / 15 min).
D. Registro, auditoría y sincronización	1. Los dispositivos generarán logs firmados digitalmente y los enviarán, en tiempo real, a un SIEM designado por el BCC mediante Syslog-TLS. 2. Se conservarán los registros 12 meses en almacenamiento WORM. 3. Todos los elementos sincronizarán fecha/hora mediante NTP autenticado.
E. Gestión de vulnerabilidades	1. El adjudicatario mantendrá el firmware y el software actualizados a la última versión estable. 2. Vulnerabilidades críticas (CVSS ≥ 9,0) deberán mitigarse en ≤ 15 días naturales; vulnerabilidades altas (CVSS 7,0–8,9) en ≤ 30 días. 3. Se entregará un SBOM (Software Bill of Materials) de cada dispositivo.
F. Monitorización y SOC	1. El servicio incluirá monitorización continua 24×7 (SOC) de eventos de seguridad, con generación de alertas en < 5 min. 2. Notificación de incidente de ciberseguridad al BCC en < 2 h desde su detección, conforme a la guía CCN-STIC-817.
G. Pruebas de penetración y aceptación	1. Antes de la recepción provisional, el adjudicatario aportará informe de pentest externo sobre cámaras, VMS/NVR y red de seguridad. 2. Todas las no conformidades críticas o altas deberán estar subsanadas antes de la FAT/SAT.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

H. Documentación y formación	1. Entrega de Plan de Seguridad Lógica (máx. 15 páginas) con arquitectura, controles, roles y procedimientos. 2. Manual de buenas prácticas de usuario (cambio de contraseñas, exportación de evidencias, políticas de borrado). 3. Sesión formativa específica (≥ 4 h) al personal designado por el BCC, con certificación de asistencia.

El incumplimiento de cualquiera de los puntos anteriores se considerará falta grave. El BCC aplicará las penalizaciones definidas en el PCAP (hasta el 20 % de la facturación mensual, acumulable), sin perjuicio de la posible resolución contractual y de las responsabilidades derivadas de daños o brechas de datos (art. 32 RGPD).

El adjudicatario deberá suministrar, junto con el plan de proyecto, un “Dossier de Evidencias de Seguridad” que incluya capturas de pantalla, listados de configuración y certificados de firmware. Dicho dossier será requisito para la firma del Acta de Recepción Definitiva.

1.9 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El adjudicatario se obliga a respetar la confidencialidad de toda la información, documentación, comunicaciones, configuraciones técnicas, datos personales o cualquier otro contenido que tenga carácter reservado o sensible, al que acceda como consecuencia de la ejecución del contrato, ya sea de forma directa o indirecta.

Asimismo, deberá dar cumplimiento a lo establecido en:

- El Reglamento (UE) 2016/679 (RGPD),
- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD),
- Y en el Esquema Nacional de Seguridad (ENS, RD 311/2022), cuando resulte de aplicación.

En particular, cuando el adjudicatario deba acceder o tratar datos personales por cuenta del Basque Culinary Center (BCC), actuará como encargado del tratamiento, debiendo firmar un Anexo específico al contrato conforme al artículo 28 del RGPD. Este anexo incluirá:

- Objeto, duración, naturaleza y finalidad del tratamiento.
- Tipos de datos y categorías de interesados.
- Obligaciones y derechos del responsable (BCC) y del encargado.
- Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.
- Compromiso expreso de confidencialidad de todo el personal que acceda a los datos.
- Reversión y supresión de los datos al término del contrato.

El adjudicatario se comprometerá igualmente a:

- No destinar los datos a fines distintos de los derivados del objeto del contrato.
- No ceder ni comunicar los datos a terceros sin autorización expresa del BCC.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

- Implantar y mantener las medidas técnicas y organizativas exigidas por el ENS en nivel ALTO, cuando el tratamiento esté vinculado a sistemas públicos.

El incumplimiento de estas obligaciones podrá dar lugar a la imposición de penalizaciones, a la resolución anticipada del contrato, así como a las responsabilidades civiles, administrativas y/o penales que correspondan, conforme a la legislación vigente.

El VMS limitará la retención de imágenes a 30 días (art. 22 LOPDGDD), salvo requerimiento judicial o fuerza mayor debidamente acreditada. El parámetro será auditable y protegido frente a alteraciones no autorizadas.

1.10 LEGALIZACIÓN FINAL Y GESTIONES ANTE ORGANISMOS

- Si las características de la instalación lo requieren (ej. potencia eléctrica, seguridad en eventos públicos, etc.), el adjudicatario tramitará la memoria o proyecto ante la autoridad competente (Delegación de Industria o similar).
- Se realizarán inspecciones o boletines si el Reglamento Electrotécnico de Baja Tensión (REBT) o normativa local lo exige.
- El adjudicatario colaborará con BCCF en la inscripción, modificación o actualización del registro de actividades de tratamiento relativo a la videovigilancia, así como en la adecuación al RGPD vigente.
- Deberán consultarse las pautas oficiales de la Agencia Española de Protección de Datos (AEPD) para carteles informativos, tiempos de conservación de imágenes y control de accesos a la información.
- Alta y certificado de Seguridad Privada

1.11 DOCUMENTACIÓN TÉCNICA ACREDITATIVA

Las empresas licitadoras deberán incluir, junto con su oferta técnica, toda la **documentación justificativa del cumplimiento técnico** de los requisitos establecidos en el presente Pliego de Prescripciones Técnicas (PPT).

Esta documentación tendrá carácter **obligatorio** para todos los productos, servicios o soluciones ofertadas, y deberá estar correctamente organizada y referenciada. En particular, se deberá aportar, cuando proceda:

- Fichas y manuales técnicos oficiales de los equipos o plataformas ofertadas.
- Certificados de homologación, conformidad técnica o certificaciones oficiales (ISO, Common Criteria, AER, etc.).
- Informes de laboratorio, benchmarks o pruebas de interoperabilidad.
- Declaraciones firmadas del fabricante o integrador, en su caso.
- Licencias de software y condiciones de uso.
- Cualquier otro documento técnico solicitado expresamente en este PPT.

La documentación técnica aportada deberá permitir verificar, de forma directa y suficiente, la idoneidad, calidad y conformidad de las soluciones ofertadas respecto a los requisitos mínimos exigidos.

La falta total o parcial de esta documentación podrá dar lugar a su valoración como insuficiente o no conforme, sin perjuicio de las consecuencias que se establezcan en el correspondiente PCAP, conforme a los artículos 84.2 y 149 de la Ley 9/2017, de Contratos del Sector Público (LCSP).

1.12 CLÁUSULA DE EQUIPAMIENTO NUEVO

Todo el equipamiento, material, hardware, terminales y componentes que se integren o suministren en el marco de la ejecución del presente contrato deberán ser **completamente nuevos de fábrica**. Queda expresamente prohibido el uso de:

- Equipos previamente instalados, alquilados, reacondicionados, exhibidos o reconstruidos.
- Unidades procedentes de programas “demo”, “refurbished”, “remanufactured”, “end-of-life (EOL)”, “grey market” o cualquier canal no autorizado oficialmente por el fabricante.

En el momento de la entrega, el adjudicatario deberá presentar una **declaración responsable firmada digitalmente**, en la que certifique el carácter nuevo, original y sin uso previo de cada equipo, así como:

- La **declaración de conformidad CE** o equivalente del fabricante, conforme a la legislación aplicable.
- La **documentación oficial de garantía**, emitida a nombre del **Basque Culinary Center (BCC)** y con fecha efectiva desde el día de entrega.

El incumplimiento de esta cláusula facultará a la Dirección Facultativa o al responsable del contrato para:

- Rechazar formalmente el suministro no conforme.
- Exigir su **sustitución inmediata**, sin coste adicional ni ampliación de plazo.
- Iniciar, en su caso, los trámites de penalización o resolución contractual previstos en el PCAP y en la **Ley 9/2017, de Contratos del Sector Público (LCSP)**.

Esta condición se considera **obligación esencial del contrato**, conforme al artículo 211.f) de la LCSP.

1.13 CLÁUSULA DE TRANSFERENCIA DE CONOCIMIENTO

La presente cláusula tiene por finalidad garantizar que el adjudicatario transmita a la **Propiedad** —de forma completa, ordenada y dentro del plazo contractual— todos los conocimientos, procedimientos, configuraciones y recursos técnicos necesarios para la **correcta explotación, administración, mantenimiento y futura evolución** del sistema objeto del contrato, evitando cualquier **dependencia tecnológica injustificada o no autorizada**.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

A tal efecto, el adjudicatario se obliga a entregar, en **formatos abiertos, estructurados y editables**, la totalidad de la documentación técnica y funcional generada durante la ejecución del contrato. Esta documentación incluirá, con carácter mínimo, pero no limitativo:

- Memorias descriptivas del diseño y ejecución del sistema.
- Diagramas de bloques, planos “as-built”, esquemas lógicos y físicos.
- Archivos de configuración, scripts, plantillas y librerías de presets.
- Listados de licencias, claves de activación y credenciales de administración.
- Procedimientos operativos, instrucciones de mantenimiento y protocolos de recuperación.

Asimismo, el adjudicatario cederá a la Propiedad los **derechos de uso, reproducción, modificación, adaptación y cesión a terceros** del citado material, sin limitación territorial ni temporal, con el único fin de garantizar la continuidad técnica, ampliación o mejora del sistema. Esta cesión incluirá expresamente cualquier componente susceptible de ser reutilizado en futuras integraciones o migraciones.

La transferencia de conocimiento comprenderá igualmente la **impartición de sesiones formativas técnicas** dirigidas al personal del BCC responsable de la operación, soporte o administración de los sistemas implantados. Estas actividades:

- Deberán celebrarse antes de la firma del Acta de Recepción Definitiva.
- Se ajustarán a un temario previamente aprobado por la Dirección Facultativa.
- Incluirán materiales didácticos y ejercicios prácticos.
- Culminarán con la expedición de **certificados individuales de aprovechamiento** para cada asistente.

Además, durante los **noventa (90) días naturales siguientes** a la firma del Acta de Recepción Definitiva, el adjudicatario prestará, sin coste adicional, **asistencia técnica remota** para la resolución de dudas o incidencias relacionadas con la documentación y configuraciones entregadas, mediante acceso seguro vía **VPN o plataforma cloud** previamente autorizada por la Propiedad.

A la finalización del proceso, ambas partes suscribirán un **Acta de Entrega de Conocimiento**, que incluirá:

- Relación firmada de todos los documentos, archivos y materiales entregados.
- Registro de sesiones formativas impartidas, contenidos y asistentes.
- Declaración del BCC conforme al cumplimiento o deficiencias detectadas.

La firma de esta acta será requisito obligatorio para la liberación de la garantía definitiva y la liquidación final del contrato.

Toda la información entregada tendrá carácter confidencial y estará sujeta a lo dispuesto en la Cláusula de Confidencialidad y Protección de Datos del presente Pliego, sin perjuicio de su divulgación cuando así lo exija la normativa vigente.

El incumplimiento total o parcial de las obligaciones aquí descritas facultará a la Propiedad para:

- Retener hasta un diez por ciento (10 %) del importe de adjudicación en concepto de penalización.

- Ejecutar total o parcialmente la garantía definitiva.
- Reclamar, en su caso, los daños y perjuicios que resulten acreditados.

1.14 CLÁUSULA "LLAVE EN MANO"

El presente contrato se formaliza en **modalidad de prestación "llave en mano"**, lo que implica que el adjudicatario asume la responsabilidad completa de la **implantación, integración, configuración y puesta en funcionamiento operativo y conforme a normativa** de todos los sistemas objeto del contrato, sin que puedan derivarse costes adicionales para el **Basque Culinary Center (BCC)** por omisiones, errores de diseño o componentes no contemplados expresamente en los listados del PPT.

Asimismo, el adjudicatario deberá asumir, dentro del alcance del contrato, las posibles modificaciones necesarias en la ubicación de dispositivos (como cámaras, sensores u otros elementos) que se deriven de ajustes durante la ejecución de la obra, siempre que dichas modificaciones no supongan una alteración sustancial del alcance funcional del sistema. Estas adaptaciones, incluso cuando supongan cambios sobre los planos inicialmente facilitados, se considerarán inherentes a la modalidad "llave en mano" y no darán lugar a compensación económica adicional.

a) Obligación de integración completa

El adjudicatario deberá verificar, con carácter previo a la presentación de su oferta, que el diseño técnico previsto en el PPT incluye todos los elementos imprescindibles para el montaje, interconexión, configuración y puesta en marcha del sistema. La ausencia de cualquier componente, accesorio o recurso en el inventario o memoria no eximirá al adjudicatario de su suministro cuando dicho elemento sea **necesario para garantizar la operatividad completa, la seguridad funcional o el cumplimiento de normativa técnica o legal vigente**.

b) Alcance implícito del suministro

Se consideran incluidos, a título orientativo y no limitativo:

- Latiguillos, adaptadores, módulos transceptores, SFPs y convertidores.
- Elementos de gestión térmica o protección eléctrica.
- Fuentes de alimentación auxiliares y elementos de fijación.
- Licencias software necesarias para activar funcionalidades básicas o avanzadas.
- Soportes especiales, regletas, bandejas, carriles DIN, tacos, tornillería o elementos de ensamblaje.
- Consumibles y recursos auxiliares para una instalación funcional y conforme.

c) Repercusión económica

Todos los componentes, tareas o servicios no especificados explícitamente pero que resulten **indispensables para garantizar el funcionamiento pleno del sistema**, deberán ser suministrados e integrados **sin repercusión económica adicional para el BCC**, salvo que medie:

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

- Una modificación contractual justificada conforme al artículo 202 de la **Ley 9/2017, de Contratos del Sector Público (LCSP)**, y
- Aprobación previa, por escrito, del órgano de contratación.

d) Revisión de integridad técnica

Antes del inicio de los trabajos de instalación, el adjudicatario deberá presentar a la Dirección Facultativa un **documento de revisión de integridad técnica del suministro**, en el que:

- Se identifiquen todos los elementos no previstos inicialmente, pero necesarios para la instalación,
- Se justifique su necesidad funcional o normativa,
- Y se confirme su provisión sin impacto económico o, en su caso, se proponga su incorporación mediante expediente de modificación contractual.

La firma de este documento, junto con el Plan de Proyecto y los planos de instalación “as-built”, formará parte del expediente técnico de validación. Esta cláusula tiene como finalidad garantizar la **integridad técnica, funcional y jurídica del suministro contratado**, evitando vacíos que puedan comprometer la legalización, seguridad, interoperabilidad o continuidad operativa del sistema.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

2 ANEXO 1. ESPECIFICACIONES DEL SISTEMA

2.1 TABLAS EQUIPOS Y MATERIALES A SUMINISTRAR

En las tablas siguientes se detallan las cantidades específicas de materiales, equipos, suministros y tareas que la empresa adjudicataria deberá incluir en su oferta. Cada uno de los elementos indicados en dichas tablas representa un requerimiento obligatorio que deberá ser considerado y cumplido en su totalidad, tanto en el suministro como en la instalación, configuración y puesta en marcha del sistema objeto del presente contrato. Las cantidades indicadas tienen carácter vinculante, siendo responsabilidad exclusiva del adjudicatario asegurar que su oferta contempla adecuadamente todos los recursos y trabajos especificados para garantizar la completa funcionalidad y operatividad del sistema según las exigencias técnicas establecidas en este pliego.

2.1.1 SISTEMA ANTI-INTRUSIÓN

Código	Descripción	Cantidad
INTR-01	Central de seguridad	1
INTR-02	Módulo de comunicación Ethernet	1
INTR-03	Teclado Alfanumérico	1
INTR-04	Módulo expansor	14
INTR-05	Contacto magnético sencillo	56
INTR-06	Detector movimiento por infrarrojos	52
INTR-07	Sirena exterior	1
INTR-08*	Canalizaciones y cableado del sistema anti-intrusión	1
INTR-09	Configuración y puesta en marcha de todo el sistema anti-intrusión	1

*Todas las necesarias para todos los elementos dimensionados.

2.1.2 SISTEMA DE VIDEO-VIGILANCIA IP

Código	Descripción	Cantidad
VVIP-01	Grabador de 64 canales	3
VVIP-02	Disco duro especial Videovigilancia 10Tbyte	12
VVIP-03	Cámara Bullet IP de 4 Mpx.	19
VVIP-04	Cámara Minidomo IP de 4 Mpx.	105
VVIP-05	Cámara Domo motorizada PTZ IP de 4 Mpx.	5

VVIP-06	Unidad de Licenciamiento para las 134 cámaras dimensionadas	1
VVIP-07*	Canalizaciones y cableado hasta cada cámara *El edificio GOe ya dispone de las canalizaciones y el cableado de red necesario para la alimentación y soporte de cada cámara IP.	*
VVIP-08	Configuración y puesta en marcha de todo el sistema de Video-vigilancia IP	1

2.1.3 SISTEMA DE VMS

Código	Descripción	Cantidad
VMS-01	Plataforma VMS	1
VMS-02	Workstation	1
VMS-03	Instalación, configuración y puesta en marcha del VMS	1

2.2 ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS A SUMINISTRAR

En el presente apartado se establecen las especificaciones técnicas y funcionales mínimas obligatorias que deberán cumplir los distintos equipos, sistemas, componentes, materiales, licencias y tareas incluidas en la oferta del adjudicatario.

Estas especificaciones constituyen los requisitos base e inderogables del suministro e instalación, y son condición necesaria para la validez técnica de la propuesta.

El adjudicatario deberá garantizar que cada elemento ofertado cumple, como mínimo, con las prestaciones, niveles de calidad, compatibilidad, integración e interoperabilidad requeridos, siendo inadmisible cualquier equipo o sistema que no alcance estas exigencias.

En todo caso, la oferta podrá mejorar las características mínimas definidas, pero nunca reducirlas o modificarlas en perjuicio de la funcionalidad, seguridad o integrabilidad del sistema.

El incumplimiento de cualquiera de estas especificaciones supondrá la inadmisión automática de la solución técnica ofertada en la fase de análisis y valoración.

2.2.1 SISTEMA ANTI-INTRUSIÓN

2.2.1.1 CENTRAL DE SEGURIDAD Y ALARMAS

INTR-01	Central de seguridad y alarmas

Descripción general	El sistema de control de intrusión deberá incorporar un panel de intrusión de altas prestaciones, adecuado para instalaciones medianas y grandes, con capacidad híbrida (cableado e inalámbrico), integración con control de accesos, y gestión remota centralizada. Compatible con sistemas de software de gestión de seguridad unificada.

Especificaciones mínimas	• Capacidad del sistema:
	  ○ Hasta 264 zonas de detección
	  ○ Hasta 64 puertas controladas
	  ○ Gestión de hasta 32 grupos de partición
	  ○ Soporte para 1.000 usuarios programables
	  ○ Hasta 67 horarios semanales configurables
	• Funciones avanzadas:
	  ○ Integración con software de gestión de seguridad (control de intrusión y accesos en múltiples paneles)
	  ○ Control de acceso mediante lectores de tarjeta vinculados a zonas e identificación automática
	  ○ Gestión centralizada remota de usuarios y eventos
	  ○ Asociación de eventos con planos gráficos para identificación rápida de incidencias
	  ○ Acceso a puertas condicionado por estado del sistema y plantillas de usuario
	• Arquitectura del sistema:
	  ○ Funcionamiento por cable, inalámbrico o mixto
	  ○ Incluye módulo de comunicación PSTN
	  ○ Integrable con sistemas de vídeo, control de accesos y gestión técnica
	• Grado de seguridad:
	  ○ Conforme a EN 50131-1 Grado 3, apto para entornos de riesgo medio/alto

Resumen funcional	El panel de control deberá constituir el núcleo del sistema de seguridad electrónica, permitiendo la gestión integral de la detección de intrusión y del control de accesos. Su arquitectura deberá ser escalable y flexible, apta para instalaciones de tamaño medio o grande, con posibilidad de funcionamiento por cable, vía radio o en configuración híbrida. Deberá permitir la configuración segmentada en grupos, control de múltiples usuarios y programación de calendarios de acceso, además de soportar la gestión remota de usuarios y eventos, integración con plataformas gráficas de gestión y supervisión, y sincronización entre varios paneles. El equipo deberá contar con marcador telefónico (PSTN) integrado, compatibilidad con lectores de control de acceso, y permitir automatismos vinculados a zonas protegidas, todo ello cumpliendo con los requisitos técnicos y de seguridad establecidos por la norma UNE-EN 50131-1 para sistemas de Grado 3.

2.2.1.2 MÓDULO DE COMUNICACIÓN ETHERNET

INTR-02	Módulo de comunicación Ethernet
Descripción general	El sistema de control de intrusión deberá incluir un módulo de comunicación IP diseñado para integrarse con paneles de control de intrusión de Grado 3. Este módulo permitirá la transmisión de alarmas y eventos a través de red IP, garantizando conectividad rápida, segura y supervisada con las centrales receptoras de alarma (CRA).

Especificaciones mínimas	• Normativa de aplicación:
	  ○ EN 50131-3:2009 (Requisitos funcionales del sistema)
	  ○ EN 50131-6:2008 (Alimentación del sistema de seguridad)
	  ○ PD6662:2010 (Especificación británica que armoniza EN 50131)
	• Grado de seguridad: Grado 3 según EN 50131 (instalaciones de riesgo medio-alto)
	• Clase ambiental: Clase II (uso en interior en condiciones moderadas)
	• Clase de transmisión (ATS): Clase 4 (comunicaciones IP con supervisión avanzada).

Resumen funcional	El módulo IP ofertado deberá ser completamente integrable en el bus de datos del panel, permitir la transmisión de eventos a CRA conforme a protocolos estándar (SIA, Contact ID o equivalentes), y cumplir con los niveles de seguridad y fiabilidad exigidos por normativa europea para entornos críticos o de alta sensibilidad.

2.2.1.3 TECLADO ALFANUMÉRICO

INTR-03	Teclado Alfanumérico
Descripción general	El sistema de control de intrusión deberá contar con al menos un teclado LCD alfanumérico retroiluminado, destinado a la interacción local con el panel de control, para armado/desarmado, visualización de estados y programación del sistema. Deberá permitir una instalación remota y estar dotado de medidas de protección frente a manipulaciones indebidas.
Especificaciones mínimas	• Pantalla: LCD retroiluminada con capacidad alfanumérica mínima de 32 caracteres • Montaje remoto: Distancia de instalación desde el panel de control de hasta 1.000 metros • Protección contra sabotaje: Detección de apertura de carcasa o manipulación física no autorizada • Grado de seguridad: Grado 3 según norma UNE-EN 50131-1
Resumen funcional	El teclado deberá ser compatible con paneles de intrusión de Grado 3, permitir una navegación clara por menús, supervisar su conexión con el

	panel y estar fabricado conforme a los estándares europeos de seguridad para sistemas de detección de intrusión y atraco.

2.2.1.4 MÓDULO EXPANSOR

INTR-04	Módulo expansor
Descripción general	El sistema de control de intrusión deberá incluir módulos de expansión de entradas/salidas (E/S) para ampliar la capacidad de supervisión y control del panel principal. Estos módulos se instalarán en ubicaciones remotas y deberán comunicarse directamente con el bus del sistema de alarma.
Especificaciones mínimas	• Zonas de entrada: Mínimo 8 zonas totalmente programables e independientes • Salidas: Mínimo 4 salidas programables para activación de elementos de aviso o control • Protección contra manipulación: Supervisión de apertura de carcasa y sabotaje • Grado de seguridad: Grado 3, conforme a norma UNE-EN 50131-1 • Compatibilidad: Integración directa con el panel de intrusión a través del bus de datos
Resumen funcional	Los módulos ofertados deberán ser ampliaciones nativas o totalmente compatibles con el sistema central, aptos para ubicaciones distribuidas y configurables desde el panel principal o software de gestión, garantizando el cumplimiento de los estándares de seguridad en instalaciones de riesgo medio-alto.

2.2.1.5 CONTACTO MAGNÉTICO SENCILLO

INTR-05	Contacto magnético sencillo
Descripción general	Elemento de detección perimetral de apertura para puertas o ventanas, en formato cableado y de montaje en superficie, destinado a uso en interiores. Formará parte del sistema de intrusión, conectado a una zona del panel de control o módulo de expansión.
Especificaciones mínimas	• Tipo de instalación: Montaje en superficie, conexión cableada • Uso: Exclusivo para interior • Distancia de activación (apertura): ≥ 15 mm • Protección contra sabotaje (tamper): Incorporada • Grado de seguridad: Grado 2 según UNE-EN 50131-2-6
Resumen funcional	Este dispositivo detectará la apertura no autorizada de elementos móviles (puertas, ventanas, registros, etc.) mediante el cambio de estado magnético. Estará conectado al sistema de alarma y generará señal de

	intrusión o sabotaje según su configuración, cumpliendo con los niveles de seguridad requeridos para instalaciones de riesgo bajo o medio.

2.2.1.6 DOBLE DETECTOR MOVIMIENTO POR INFRARROJOS

INTR-06	Detector movimiento por infrarrojos
Descripción general	Dispositivo de detección volumétrica por infrarrojos pasivos (PIR) con tecnología cuádruple, diseñado para uso interior. Ofrece mayor inmunidad frente a falsas alarmas mediante doble procesamiento de señal.
Especificaciones mínimas	• Tecnología: PIR cuádruple con doble sensor y doble canal de procesamiento • Alcance de detección: 12 × 12 metros • Uso interior: Carcasa con autocierre, óptica y electrónicas selladas • Apto para mascotas: Inmunidad a animales pequeños • Señalización: LED indicador de activación (azul) • Conectividad: Salida por relé para señal de alarma • Resistencia física: Carcasa resistente a impactos • Grado de seguridad: Grado 2, conforme a UNE-EN 50131-2-2
Resumen funcional	Este detector garantiza una detección precisa de movimiento en interiores, minimizando las falsas alarmas mediante verificación cruzada entre sensores. Es ideal para viviendas, oficinas y locales con presencia ocasional de mascotas, y cumple con los requisitos normativos para instalaciones de riesgo bajo o medio según normativa europea.

2.2.1.7 SIRENA EXTERIOR

INTR-07	Sirena exterior
Descripción general	Dispositivo acústico y luminoso de señalización de alarmas para exteriores, diseñado para ser instalado en fachada o paramento vertical. Con alimentación a 12 V CC, incorpora batería de respaldo y sistema de autodiagnóstico. Compatible con sistemas de intrusión de Grado 3.
Especificaciones mínimas	• Nivel sonoro: ≥ 112 dB a 1 metro • Tonos disponibles: Mínimo 4 tonos seleccionables (doble piezoeléctrico) • Duración de señal acústica: Programable entre 3 y 15 minutos • Señalización visual: Flash LED con doble barra (estado de armado/desarmado y alarma) • Funciones adicionales: Confirmación acústica/luminosa de armado y desarmado • Protección anti-sabotaje: Tamper frontal y trasero • Alimentación: 12 V CC

	• Batería interna de respaldo: 6 V, 1,3 Ah (incluida) • Grado de seguridad: Grado 3, conforme a UNE-EN 50131-4
Resumen funcional	La sirena deberá emitir señal acústica y visual de forma clara y potente en caso de alarma. Además, debe ofrecer señalización disuasoria permanente y confirmación de armado/desarmado del sistema. Su construcción deberá garantizar alta robustez frente a sabotajes físicos y condiciones ambientales adversas, conforme a normativa europea para sistemas de seguridad de riesgo medio-alto.

2.2.1.8 CANALIZACIONES Y CABLEADO DEL SISTEMA ANTI-INTRUSIÓN

INTR-08	Canalizaciones y cableado del sistema anti-intrusión
Descripción general	Unidad destinada a la ejecución completa del cableado y canalizaciones necesarios para la alimentación eléctrica, comunicación de datos y señalización de todos los elementos del sistema de detección de intrusión: panel de control, teclados, detectores, sirenas, módulos de expansión, fuentes auxiliares y dispositivos periféricos. El cableado deberá ejecutarse conforme a la normativa vigente en materia de seguridad, instalaciones eléctricas y sistemas de detección de intrusión, incluyendo todos los materiales auxiliares, canalizaciones, tubos, cajas, conectores, fijaciones y etiquetado necesarios, y garantizando su perfecta integración, continuidad eléctrica y compatibilidad electromagnética.

Especificaciones mínimas	• Tipología de cableado incluido:
	  ○ Cableado de alimentación en baja tensión (12 V / 24 V DC) para todos los dispositivos del sistema, desde panel o fuentes auxiliares.
	  ○ Cableado de comunicación (bus de datos serie tipo RS-485, RS-232 Ethernet, según protocolo del fabricante).
	  ○ Cableado de conexión de zonas para detectores, pulsadores, contactos magnéticos, módulos de entrada/salida, etc.
	• Características técnicas de los cables:
	  ○ Todos los cables serán libres de halógenos (LSZH), con cumplimiento del Reglamento CPR según su uso:
	  ○ Alimentación: sección mínima 2 × 1,5 mm², Cca-s1b,d1,a1 o superior
	  ○ Bus de comunicación: cable apantallado de par trenzado, especificado por fabricante
	  ○ Zonas y dispositivos: cable multipar apantallado tipo FPL/CL2 o equivalente
	  ○ Longitudes calculadas conforme a caída de tensión y distancias máximas permitidas por el fabricante
	• Canalizaciones auxiliares:

	○ Tubo rígido o corrugado de diámetro mínimo 20/25 mm o canal técnico vista/empotrada, según la instalación. ○ Material: LSZH e ignífugo, clase II según entorno. ○ Integración con bandejas y registros existentes en el edificio GOe ○ Cruces entre compartimentos EI realizados con elementos intumescentes homologados. • Instalación y montaje: ○ Guiado y tendido de cables según trazado definido en planos ○ Fijación mediante bridas, clips o grapas compatibles ○ Protección mecánica en zonas expuestas ○ Etiquetado normalizado en origen y destino (UNE-EN 50174) ○ Reservas técnicas: 30 cm mín. en cuadros y 1 m en cabezales de zonas • Verificación técnica: ○ Comprobación de continuidad, aislamiento, polaridad, ausencia de cortocircuitos y señales parásitas ○ Medición de tensión en dispositivos extremos ○ Comprobación de funcionamiento del bus de datos y respuesta del sistema a cada dispositivo • Documentación: ○ Esquema de cableado final y rutas ○ Identificación de todos los tramos y puntos de conexión ○ Certificados de conformidad de los materiales instalados (CPR, CE).
Resumen funcional	Esta unidad comprende la infraestructura física de cableado y canalizaciones necesarias para el correcto funcionamiento del sistema anti-intrusión, garantizando la alimentación estable, la comunicación eficaz entre dispositivos, y la correcta señalización de los elementos periféricos. Los materiales utilizados deberán cumplir con las normativas de seguridad eléctrica, reacción al fuego y compatibilidad electromagnética, y su instalación deberá asegurar una vida útil prolongada, fácil mantenimiento y fiabilidad. Se exigirá la verificación completa de continuidad y funcionalidad antes de la conexión de dispositivos, dejando la instalación lista para la puesta en marcha.

2.2.1.9 CONFIGURACIÓN Y PUESTA EN MARCHA DE TODO EL SISTEMA ANTI-INTRUSIÓN

INTR-09	Configuración y puesta en marcha de todo el sistema anti-intrusión
Descripción general	Esta unidad comprende la configuración, parametrización, comprobación funcional y puesta en marcha de todos los elementos que componen el sistema anti-intrusión descrito en el presente pliego: panel de control,

	teclados, detectores, contactos, sirenas, módulos de expansión, software de gestión (si aplica) y elementos auxiliares. Incluye la programación lógica del sistema, la comprobación de funcionalidad zona a zona, la integración con sistemas de control de accesos o videovigilancia, la generación de documentación técnica final, y la formación básica al personal designado por la propiedad.

Especificaciones mínimas	• Programación inicial del panel de control, incluyendo:
	  ○ Definición y asignación de zonas
	  ○ Alta de módulos, teclados y expansores
	  ○ Segmentación en grupos/particiones
	  ○ Programación de horarios, usuarios y niveles de acceso
	  ○ Configuración de entradas y salidas programables
	• Activación de comunicaciones (IP, PSTN, GPRS, etc.)
	• Integración con lectores y control de accesos, si aplica
	• Ajuste de temporizaciones, retardos, sensibilidad y filtros de detección
	• Verificación funcional completa:
	  ○ Comprobación de la conexión, detección y supervisión de todos los dispositivos
	  ○ Simulación de activaciones y alarmas reales
	  ○ Verificación de salidas acústicas, visuales y de transmisión
	  ○ Pruebas de detección y sabotaje (tamper)
	  ○ Pruebas de comunicaciones hacia centro de control, CRA o software de gestión
	• Seguridad lógica:
	  ○ Creación de usuarios con permisos diferenciados
	  ○ Asignación de códigos, claves y etiquetas
	  ○ Activación de protecciones anti-sabotaje y contra accesos no autorizados
	  ○ Registro de eventos y configuración de auditoría
	• Documentación a entregar:
	  ○ Informe completo de configuración y programación
	  ○ Certificado de puesta en marcha firmada por técnico acreditado
	  ○ Plano de zonas y dispositivos codificado
	  ○ Fichero de usuarios y niveles
	  ○ Manuales en castellano y listado de contraseñas iniciales en sobre cerrado
	  ○ Registro de pruebas y resultados de verificación
	• Formación básica a usuarios finales:
	  ○ Explicación del sistema, funcionamiento y activaciones
	  ○ Simulación de escenarios de uso

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

	○ Formación para operaciones básicas: armado/desarmado, reconocimiento de incidencias, exportación de eventos, cambio de claves
Resumen funcional	Esta unidad contempla la puesta en servicio del sistema anti-intrusión en condiciones reales de funcionamiento, garantizando que todos los componentes estén correctamente configurados, operativos y verificados según la estrategia de seguridad definida en proyecto. El adjudicatario deberá realizar una puesta en marcha técnica completa y demostrable, asegurando el cumplimiento de los requisitos funcionales, normativos y de seguridad, y entregando toda la documentación técnica que certifique que la instalación está correctamente configurada, probada y lista para entrar en servicio.

2.2.2 SISTEMA DE VIDEO-VIGILANCIA IP

2.2.2.1 GRABADOR DE 64 CANALES

VVIP-01	Grabador de 64 canales
Descripción general	El sistema de videovigilancia deberá contar con un videograbador de red (NVR) de alto rendimiento, diseñado para instalaciones de gran tamaño y elevada densidad de cámaras. Deberá gestionar hasta 64 canales IP en alta resolución, permitir grabación continua con almacenamiento redundante, y ofrecer capacidades de reproducción avanzada y gestión inteligente del vídeo. Compatible con cámaras especializadas y funciones analíticas, y preparado para condiciones de red exigentes y operación 24/7.

Especificaciones mínimas	• Capacidades técnicas:
	  ○ Hasta 64 canales IP, compatible con cámaras de hasta 12 MP (Ultra HD)
	  ○ Resoluciones de salida: HDMI 1 hasta 8K, HDMI 2 y VGA hasta 4K/1080p
	  ○ Ancho de banda entrante/saliente: 400 Mbps
	  ○ Reproducción simultánea de hasta 16 canales, decodificación hasta 32 MP
	  ○ Salidas de vídeo simultáneas independientes en diferentes monitores
	• Almacenamiento:
	  ○ Hasta 8 discos SATA internos, 16 TB por unidad (máx. 128 TB)
	  ○ Compatible con sistemas RAID 0, 1, 5, 6, 10 y N+1 hot spare
	  ○ Interfaz eSATA adicional para almacenamiento externo
	• Funciones avanzadas:
	  ○ Compatible con cámaras con funciones inteligentes: conteo de personas, ANPR, ojo de pez
	  ○ Tecnología de transmisión optimizada para redes inestables
	  ○ Audio bidireccional, soporte para múltiples códecs de audio y vídeo
	  ○ Entradas/salidas de alarma: 16 E / 9 S, con control de alimentación para actuadores externos
	• Compatibilidad e interoperabilidad:
	  ○ Compatible con ONVIF v2.5, protocolos TCP/IP, RTSP, HTTPS, IPv6, SNMP, NTP, entre otros
	  ○ Interfaz de red: 2 puertos RJ45 (10/100/1000 Mbps)
	  ○ Integrable en plataformas de gestión de vídeo (VMS) de terceros mediante SDK y API
	• Seguridad lógica y ciberseguridad:

	○ Acceso por niveles de usuario, cifrado HTTPS, protección por contraseña ○ Registro de eventos, logs de auditoría y acceso remoto seguro • Interfaces y conectividad: ○ USB 2.0 / 3.0, puertos serie RS-232 y RS-485, eSATA ○ Salida de vídeo analógica adicional (CVBS) para visualización auxiliar • Grado profesional y robustez: ○ Formato 2U rack ○ Fuente de alimentación redundante conmutada ○ Funcionamiento 24/7 en entornos de misión crítica • Certificaciones: CE, FCC, conforme a normativas de compatibilidad electromagnética y seguridad eléctrica
Resumen funcional	El grabador deberá permitir la gestión centralizada y segura de hasta 64 canales IP, garantizando una grabación continua y fiable, con múltiples opciones de visualización, reproducción y análisis. Será adecuado para infraestructuras críticas, edificios institucionales o grandes instalaciones, ofreciendo alta capacidad de almacenamiento, redundancia RAID y protección frente a fallos. Deberá ser compatible con cámaras analíticas, integrarse con plataformas de terceros mediante protocolos estándar, y disponer de interfaces múltiples para gestión remota, salida de alarmas, control de dispositivos y acceso físico a datos. Su diseño deberá ser robusto y profesional, preparado para entornos 24/7, con alimentación redundante, seguridad lógica y cumplimiento normativo total.

2.2.2.2 DISCO DURO DE 10 TB

VVIP-02	Disco duro de 10 TB
Descripción general	El adjudicatario deberá suministrar discos duros internos de 3,5″, 10 TB de capacidad, diseñados específicamente para sistemas de videovigilancia y grabación continua en NVR. Estos discos deberán integrarse en el chasis del grabador y garantizar alta fiabilidad y rendimiento bajo cargas de escritura ininterrumpida.
Especificaciones mínimas	• Capacidad: 10 TB • Formato: 3.5-Inch • Conector: SATA • Interfaz: SATA • Velocidad de transferencia: Hasta 175MB/s • Recording Technology: CMR • Tamaño de cache: 256MB • Temp. Operativa: 0°C to 65°C

	• Non-Operating Temperature: -40°C to 70°C • Certificaciones BSMI, ICES-003/NMB-003, CE, FCC, KC, Maghreb, RCM, UKCA, VCCI, CB-Scheme, TUV, UL
Resumen funcional	• Diseñado para grabación 24/7, soportando ciclos de escritura continuos sin degradación prematura. • Compatible con NVR de 64 canales y flujos múltiples H.265+/H.264+. • Soporta funciones SMART y gestión de errores para detección proactiva de fallos. • Optimizado para baja vibración y alta resistencia a cargas térmicas en entornos de alta densidad de discos. • Permite retención de grabaciones según requisitos del pliego (p. ej. 30–60 días) sin pérdida de datos.

2.2.2.3 CÁMARA BULLET IP DE 4 MPX.

VVIP-03	Cámara Bullet IP de 4 Mpx.
Descripción general	La cámara de videovigilancia deberá ser del tipo bullet IP exterior, con resolución mínima de 4 megapíxeles, lente Varifocal motorizada y funciones avanzadas de análisis de vídeo basadas en inteligencia artificial. Estará diseñada para aplicaciones en exteriores, con visión nocturna IR de largo alcance, protección contra condiciones ambientales severas y capacidad de almacenamiento local cifrado.

Especificaciones mínimas	• Resolución: 4 Megapíxeles (2688 × 1520 px)
	• Lente: Varifocal motorizada (2,7 – 13,5 mm), con enfoque y zoom remoto
	Campo de visión horizontal: desde 102,4° hasta 31,2°.
	• Compresión vídeo: H.265+, H.264+
	• Visión nocturna (IR): Hasta 60 m
	• WDR Real: 120 dB, imágenes nítidas frente a fuerte contraluz
	• Audio: Micrófono integrado, compresión audio G.711 / AAC, reducción de ruido ambiente.
	• Funciones inteligentes (Deep Learning):
	  ○ Detección específica (humanos y vehículos)
	  ○ Protección perimetral (intrusión, cruce de línea)
	  ○ Captura facial
	  ○ Análisis inteligente de comportamientos (merodeo, objetos abandonados, retirada de objetos)
	• Conectividad y seguridad: Compatible ONVIF Perfil S/G, protocolo HTTPS, IPv4/IPv6, protección avanzada por contraseña.
	• Almacenamiento local: Ranura MicroSD hasta 512 GB, cifrado de almacenamiento
	• Protección y robustez: Exterior IP67 (agua/polvo), antivandálica IK10
	• Alimentación: PoE IEEE 802.3at o 12 V CC.

	• Temperatura operación: -30 °C a +60 °C • Certificaciones principales: CE-EMC, CE-LVD, UL, RoHS, RAEE, IK10, IP67
Resumen funcional	La cámara deberá proporcionar una imagen de alta calidad en entornos exteriores exigentes, tanto de día como de noche, gracias a su sensor de 4 MP, lente Varifocal motorizada y visión IR inteligente de hasta 60 metros. Permitirá el análisis avanzado de vídeo en tiempo real, incluyendo detección de intrusión y cruce de línea, reconocimiento de comportamiento anómalo y captura facial, contribuyendo a una vigilancia proactiva. Estará diseñada para condiciones climáticas adversas y entornos de alta seguridad, cumpliendo con normativas de protección física y eléctrica, y permitiendo su integración en plataformas de gestión de vídeo estándar gracias a su compatibilidad ONVIF y funciones de ciberseguridad. La cámara incluirá almacenamiento local cifrado y audio ambiental integrado, optimizando su rendimiento en instalaciones críticas, institucionales o industriales.

2.2.2.4 CÁMARA MINIDOMO IP DE 4 MPX.

VVIP-04	Cámara Minidomo IP de 4 Mpx.
Descripción general	La cámara deberá ser de tipo minidomo IP para instalación interior o exterior, con óptica fija gran angular, resolución de 4 megapíxeles y capacidad de análisis inteligente basado en aprendizaje profundo. Deberá incorporar visión nocturna IR, protección antivandálica, audio ambiental y funciones avanzadas de clasificación de objetivos, cumpliendo normativa europea de videovigilancia profesional.

Especificaciones mínimas	• Resolución: 4 MP (2688 × 1520 px)
	• Óptica fija: 2,8 mm (gran angular), apertura F1.4
	• Sensor: CMOS 1/3", tecnología de imagen para baja iluminación (color desde 0,003 Lux)
	• Visión nocturna IR: Hasta 40 metros
	• WDR real: 120 dB para contraluz
	• Codificación: H.265+, H.264+
	• Audio: Micrófono integrado
	• Almacenamiento: Ranura microSD hasta 512 GB
	• Analítica avanzada (IA):
	  ○ Clasificación de personas y vehículos
	  ○ Protección perimetral (intrusión, cruce de línea, etc.)
	  ○ Detección de objetos abandonados/retirados
	  ○ Captura facial y conteo de personas
	• Conectividad:
	  ○ 1 puerto RJ45 10/100 Mbps
	  ○ Compatible ONVIF Perfil S/G
	  ○ Acceso multiusuario, cifrado HTTPS

	• Protección:
	  ○ IP67 (exterior)
	  ○ IK10 (antivandálica)
	• Alimentación:
	  ○ PoE (IEEE 802.3af) o 12 V CC
	  ○ Consumo máximo: 9 W
	• Certificaciones: CE, EN 55032, EN 62368-1, RoHS, RAEE

Resumen funcional	La cámara deberá ofrecer cobertura de vigilancia fija de alta definición en interiores o exteriores, con una imagen estable, nítida y con gran angular tanto en condiciones diurnas como nocturnas. Su óptica fija y compacto diseño facilitarán la instalación en falsos techos, entradas o pasillos. Mediante sus funciones inteligentes de análisis de vídeo (IA), permitirá detectar y clasificar eventos relevantes de seguridad, como intrusiones, comportamientos anómalos, conteo de personas o gestión de perímetros. Estará equipada con audio ambiente, grabación local cifrada y conectividad segura, y será compatible con plataformas de gestión de vídeo estándar mediante ONVIF. Cumplirá con los requisitos técnicos, funcionales y normativos exigibles a sistemas de videovigilancia en entornos de riesgo medio y profesional.

2.2.2.5 CÁMARA DOMO MOTORIZADA PTZ IP DE 4 MPX.

VVIP-05	Cámara Domo motorizada PTZ IP de 4 Mpx.
Descripción general	La cámara requerida será del tipo dome IP motorizada PTZ (Pan-Tilt-Zoom) con óptica motorizada de gran alcance, doble canal (cámara fija + PTZ), visión nocturna IR extendida y funciones de disuasión activa. Estará equipada con inteligencia artificial para análisis de vídeo, seguimiento automático, clasificación de objetivos y captura facial. Adecuada para entornos exteriores con condiciones severas, garantizará vigilancia activa y cobertura continua de amplias áreas.

Especificaciones mínimas	• Resolución: 4 MP (2560 × 1440 px) en ambos canales
	• Sensor de imagen: CMOS 1/1.8” (bullet y PTZ)
	• Lente:
	  ○ Fija bullet: 4 mm (visión amplia)
	  ○ PTZ: 5,9 a 188,8 mm (zoom óptico 32×)
	• Visión nocturna:
	  ○ IR hasta 200 m (PTZ) / Luz blanca hasta 30 m (bullet)
	• Zoom: Óptico 32× + digital 16× (canal PTZ)
	• Movilidad: Giro 360° / Inclinación -15° a 90°, patrullas programables, 300 presets
	• Compresión: H.265, H.264, MJPEG / Multistreaming
	• Audio: Entrada/salida de audio y micrófono, con reducción de ruido
	• Almacenamiento local: Ranura MicroSD hasta 256 GB

	• Eventos inteligentes:
	  ○ Detección de movimiento, intrusión, cruce de línea, audio anómalo
	  ○ Seguimiento automático y manual (PTZ)
	  ○ Disuasión activa: luz estroboscópica + alarma sonora
	• Funciones de IA:
	  ○ Clasificación de personas y vehículos
	  ○ Captura facial (solo canal PTZ)
	• Protecciones y condiciones de uso:
	  ○ Exterior IP66 / Antivandálica IK10
	  ○ Temperatura de operación: -30 °C a +65 °C
	  ○ Protección contra sobretensiones, rayos y transitorios
	• Alimentación: 24 V CA o Hi-PoE
	  ○ Consumo máx.: 42 W (con calefactor y luz IR activa)
	• Interfaz de red: RJ45 10/100 Mbps, ONVIF Perfil S/G, 20 accesos simultáneos
	• Certificaciones: CE, IP66, IK10, protección contra rayos y picos eléctricos

Resumen funcional	La cámara PTZ requerida deberá permitir la vigilancia activa de grandes áreas exteriores, ofreciendo tanto visión general constante a través del canal fijo como detección dirigida y seguimiento automático mediante el canal PTZ. Gracias a su zoom óptico 32×, su visión nocturna IR de largo alcance y sus capacidades de disuasión, será especialmente útil para perímetros, accesos o zonas de alto tránsito. Las funciones de análisis inteligente de vídeo, como la clasificación de objetivos, la detección perimetral o la captura facial, permitirán una gestión eficiente de eventos de seguridad y reducirán las falsas alarmas. Su construcción resistente, alimentación redundante y cumplimiento normativo garantizan su adecuación en instalaciones críticas, industriales o institucionales, cumpliendo con los requisitos técnicos y de seguridad exigidos por normativas europeas.

2.2.2.6 UNIDAD DE LICENCIAMIENTO DE TODO EL SISTEMA DE VIDEOVIGILANCIA (VER PLATAFORMA VMS)

VVIP-06	Unidad de Licenciamiento de todo el sistema de videovigilancia
Descripción general	Suministro de todas las licencias necesarias para el correcto funcionamiento, gestión, visualización, grabación, configuración, análisis y explotación del sistema de videovigilancia IP descrito en el presente pliego, incluyendo videograbadores, cámaras, software cliente/servidor, módulos de analítica y cualquier otro componente software necesario para que el sistema funcione de forma completa, legal y operativa, conforme a las capacidades técnicas ofertadas. La forma de licenciamiento puede variar

	entre fabricantes, pero en todo caso deberán cubrir todo el equipamiento ofertado.
Especificaciones mínimas	● Licencias de canal VMS ○ El adjudicatario suministrará una licencia de canal por cada cámara del sistema (134 en total), pudiendo agruparlas en bundles (packs de 64 canales) para optimizar costes. ○ Las licencias deberán ser compatibles con resolución mínima de 4 MP, flujos múltiples y códecs H.265+/H.264+. ● Licencias de NVR ○ Se incluirán o activarán, según fabricante, licencias de grabación interna en cada NVR de 64 canales. ○ Deberán garantizar grabación continua de todos los canales, reproducción multicanal y gestión avanzada de vídeo. ● Licencias de cliente concurrente ○ El adjudicatario deberá incluir un mínimo de 4 licencias de puesto cliente simultáneo en el VMS. ● Integración/API ○ Se aportará una licencia de integración que permita el intercambio de eventos y vídeo con el sistema anti-intrusión. ● Compatibilidad y escalabilidad ○ Todas las licencias serán perpetuas, transferibles entre dispositivos de la misma red y ampliables con nuevos bundles. ○ Se garantizará compatibilidad ONVIF Profile S/G y con protocolos abiertos, así como interoperabilidad con cámaras IP de terceros. ● Cumplimiento legal ○ Las licencias deberán estar completamente adquiridas (no versiones de prueba), con entrega de claves, seriales y documentaciones al cliente. ○ La solución deberá cumplir la normativa de videovigilancia, protección de datos (RGPD/LOPDGDD) y las normas UNE/ISO aplicables.
Resumen funcional	Esta unidad de partida comprende todos los componentes de software y licencias necesarias para garantizar la puesta en marcha completa del sistema de videovigilancia IP, sin limitaciones por parte del fabricante ni costes ocultos a futuro. Deberá contemplar todos los elementos necesarios para que las cámaras, grabadores, sistemas cliente/servidor y analítica de vídeo funcionen de manera integrada, estable y segura. El licenciamiento deberá ser adecuado al sistema físico suministrado, incluyendo cámaras de alta resolución, videograbadores de hasta 64 canales, y todos los elementos lógicos que permitan la explotación profesional del sistema de acuerdo a lo exigido en este pliego.

Basque Culinary Center Fundazioa
Paseo Juan Avelino Barriola 101
20009 DONOSTIA-SAN SEBASTIÁN - Gipuzkoa
Tel. 943 574 500 info@bculinary.com
www.bculinary.com

2.2.2.7 CANALIZACIONES Y CABLEADO HASTA CADA CÁMARA

VVIP-07	Canalizaciones y cableado hasta cada cámara
Descripción general	Las canalizaciones y el cableado de red necesario hasta cada cámara ya han sido objeto de instalación durante la ejecución del proyecto de telecomunicaciones.

2.2.2.8 CONFIGURACIÓN Y PUESTA EN MARCHA DE TODO EL SISTEMA DE VIDEOVIGILANCIA

VVIP-08	Configuración y puesta en marcha de todo el sistema de videovigilancia
Descripción general	Esta unidad contempla la configuración, parametrización, comprobación y puesta en marcha de todos los elementos que componen el sistema de videovigilancia IP descrito en el presente pliego, incluyendo cámaras, videograbadores, software, red de comunicaciones, almacenamiento, licencias, analítica inteligente y clientes de acceso, garantizando su correcto funcionamiento y operatividad integral conforme al diseño y objetivos de seguridad definidos.

Especificaciones mínimas	• Alcance de la configuración técnica:
	  ○ Parametrización individual de todas las cámaras IP (direcciones IP, nombres, resolución, codificación, flujo, detección de eventos, horarios, analítica, zonas de privacidad, etc.)
	  ○ Configuración de videograbadores (NVR): estructura de grabación, almacenamiento RAID, grabación por eventos, programación horaria, alertas
	  ○ Configuración del software de gestión VMS: estructura jerárquica, usuarios, privilegios, escenas de visualización, exportación de vídeos, búsquedas inteligentes
	  ○ Integración del sistema en la red de datos del edificio, según topología prevista y VLAN si aplica.
	• Configuración de seguridad lógica:
	  ○ Definición de perfiles de usuario con permisos diferenciados
	  ○ Establecimiento de contraseñas seguras, cifrado de comunicaciones, configuración de protocolos HTTPS y autenticación
	  ○ Control de acceso lógico por dirección IP, rango de red o cliente autorizado
	• Configuración de eventos inteligentes y analítica (si aplica):
	  ○ Definición de reglas de análisis: cruce de línea, intrusión, conteo de personas, capturas faciales, etc.
	  ○ Enlaces a grabación, notificaciones, activación de salidas, o seguimiento PTZ

	○ Comprobación funcional de cada regla en cámaras que lo permitan • Pruebas de funcionamiento: ○ Comprobación de conectividad de todos los dispositivos IP ○ Verificación de la correcta visualización, grabación, reproducción y exportación de vídeos ○ Validación del almacenamiento, RAID, alertas y notificaciones ○ Prueba de grabación por evento y por detección inteligente • Formación básica a usuario final: ○ Sesión presencial o remota de formación operativa sobre visualización, búsqueda, exportación de evidencias, acceso multiusuario y mantenimiento básico ○ Entrega de manual de usuario del sistema en castellano • Documentación final exigida: ○ Plano final as-built con codificación de cámaras y puntos ○ Informe de configuración completa del sistema ○ Manual de operación y administración básica ○ Documentación de usuarios, contraseñas iniciales, licencias activadas ○ Certificado de puesta en marcha y conformidad del sistema completo
Resumen funcional	La presente unidad incluye todas las tareas necesarias para dejar el sistema de videovigilancia plenamente configurado, operativo y validado, asegurando la correcta integración entre cámaras, grabadores, red IP y software, así como la activación de funcionalidades inteligentes, seguridad lógica y almacenamiento conforme a los criterios técnicos del proyecto. El adjudicatario será responsable de dejar cada elemento ajustado, probado y documentado, y de realizar una puesta en marcha completa y satisfactoria ante la dirección facultativa y la propiedad, incluyendo una formación básica al personal designado. La instalación no se considerará finalizada hasta que se entreguen los informes, documentación técnica y certificados asociados a esta unidad.

2.2.3 SISTEMA DE VMS

El adjudicatario deberá suministrar, instalar y licenciar una plataforma VMS independiente y abierta que actuará como capa corporativa de integración para:

- El sistema de videovigilancia IP definido en este proyecto.
- El sistema anti-intrusión especificado en el capítulo 2.2.1.
- Cualesquiera otros subsistemas de seguridad electrónica (control de accesos, detección técnica, CRA, etc.) que BCCF incorpore en el futuro.
- Las sedes adicionales del BCCF, posibilitando una administración centralizada multi-sitio.

Esta VMS no sustituye al software de visualización propietario entregado con los NVR, sino que lo complementa y garantiza que la solución resultante sea escalable, interoperable y preparada para la expansión corporativa de BCCF.

2.2.3.1 PLATAFORMA VMS

VMS-01	Plataforma VMS
Descripción general	El adjudicatario realizará el suministro, instalación, configuración, puesta en marcha y licencia de un **Sistema de Gestión de Vídeo (VMS)** profesional, de arquitectura abierta, diseñado específicamente para integrar, gestionar, monitorizar, grabar y administrar los sistemas de **videovigilancia IP y anti-intrusión** del edificio objeto del presente contrato. El VMS proporcionará una plataforma unificada que permita centralizar todos los elementos del sistema de seguridad electrónica en un entorno gráfico intuitivo y seguro, facilitando la gestión diaria de la seguridad por parte del personal autorizado. Deberá soportar plenamente la integración con cámaras IP mediante protocolos abiertos (ONVIF mínimo Perfil S y G), así como integrar alarmas y eventos generados por sistemas anti-intrusión mediante protocolos estándar (Contact-ID, SIA, API abierta o equivalentes).

Especificaciones mínimas	• Características Generales del Sistema VMS:
	  ○ Plataforma abierta y escalable capaz de gestionar un mínimo de 134 canales IP simultáneos con resolución mínima de 4 MP por canal, ampliable según necesidades futuras.
	  ○ Compatibilidad nativa con cámaras IP mediante estándares abiertos tipo ONVIF (Perfiles S/G).
	  ○ Grabación continua o por evento, con funciones avanzadas de búsqueda inteligente, reproducción sincronizada multipantalla y exportación segura de grabaciones.
	  ○ Gestión integral de usuarios, con definición de perfiles de acceso diferenciados por roles y privilegios.
	• Integración de Sistemas Anti-Intrusión:
	  ○ Capacidad para integrar alarmas y eventos procedentes del sistema anti-intrusión mediante protocolos estándar del mercado (SIA, Contact-ID, SDK, API abierta u otros).
	  ○ Visualización y gestión en tiempo real de eventos de intrusión: alarma, sabotaje, fallo de equipos o zonas.
	  ○ Vinculación automática de grabaciones con eventos específicos de intrusión y activación automática de visualización en pantalla ante alarmas críticas.

	○ Posibilidad de reconocimiento, validación o cancelación de alarmas desde el propio entorno del VMS. ● Analítica Inteligente Incorporada: ○ Integración nativa de eventos analíticos provenientes de las cámaras IP (detección de cruce de línea, intrusión, objetos abandonados o retirados, detección facial, conteo de personas). ○ Alertas automáticas y gestión centralizada de eventos analíticos en tiempo real. ● Funciones Avanzadas de Gestión Operativa: ○ Interfaz gráfica intuitiva y personalizable en castellano. ○ Visualización simultánea multipantalla en tiempo real y reproducción sincronizada de varias cámaras. ○ Búsqueda avanzada de grabaciones por fecha, hora, cámara, evento inteligente, zona o alarma específica. ○ Posibilidad de exportar grabaciones en formatos estándar seguros y válidos como evidencias legales (AVI, MP4), con marcas digitales para integridad probatoria. ● Ciberseguridad y Protección Lógica: ○ Cifrado HTTPS/TLS para acceso remoto y gestión segura del sistema. ○ Gestión avanzada de contraseñas y perfiles según requisitos del Esquema Nacional de Seguridad (ENS), RGPD y LOPDGDD. ○ Registros de auditoría de acciones relevantes del sistema, accesibles solo por personal autorizado. ● Interoperabilidad y Apertura del Sistema: ○ API o SDK documentado y abierto para integración con sistemas externos (control de accesos, sistemas VMS, SCADA, CRA externa, etc.). ○ Capacidad para emitir notificaciones externas por correo electrónico, SNMP, HTTP(S) o mediante protocolos estándar tipo REST API. ● Licenciamiento y Soporte: ○ Se admitirán licencias perpetuas o licencias por suscripción con una vigencia inicial mínima de 36 meses, siempre que comprendan, sin restricciones, todos los canales, módulos y analíticas requeridos en el presente pliego. ○ El adjudicatario garantizará, sin coste adicional, el acceso a actualizaciones de seguridad, parches correctivos y soporte del fabricante durante al menos 24 meses a partir del acta de recepción, o durante toda la vigencia de la suscripción cuando ésta sea superior.
Resumen funcional	El sistema VMS solicitado constituirá la plataforma tecnológica unificada para la gestión integral del sistema de seguridad electrónica (videovigilancia IP y anti-intrusión), proporcionando una gestión

	centralizada, intuitiva y segura para la vigilancia, control y supervisión continua de las instalaciones del edificio. Permitirá gestionar de forma unificada y en tiempo real todas las cámaras IP instaladas, así como los eventos, alarmas e incidencias generadas por el sistema anti-intrusión, facilitando una respuesta inmediata y efectiva por parte del personal de seguridad. Además, ofrecerá avanzadas capacidades de análisis inteligente, gestión robusta de eventos, exportación segura de evidencias y altos estándares en seguridad lógica y ciberseguridad.

2.2.3.2 WORKSTATION

VMS-02	Workstation
Descripción general	La empresa adjudicataria deberá suministrar una estación de trabajo profesional destinada a la explotación diaria del VMS, capaz de decodificar, visualizar y gestionar en tiempo real los 129 flujos IP y las alarmas de intrusión integradas. La Workstation deberá combinar rendimiento gráfico y de proceso de gama media-alta con fiabilidad 24/7, manteniendo un coste contenido y garantizando ampliaciones futuras sin sustitución completa del equipo.
Especificaciones mínimas	• CPU: Intel Core i7 12.ª gen (≥ 12 núcleos lógicos, PassMark ≥ 25 000) o AMD Ryzen 7 5700G equivalente. • GPU: Tarjeta dedicada con decodificación H.265/H.264 por hardware (p. ej. NVIDIA T600 4 GB GDDR6 o AMD Radeon Pro W6400) con ≥ 2 salidas DisplayPort/HDMI 2.0 aptas para 2 monitores FHD/4K. • Memoria: 16 GB DDR4/DDR5 3200 MHz, ampliable a 32 GB (mínimo dos zócalos libres o no ocupados). • Almacenamiento: 1 TB SSD NVMe M.2 (≥ 3000 MB/s lectura) + bahía libre para segundo disco. • Conectividad de red: Doble puerto Gigabit Ethernet (chipset Intel o Realtek RTL8125), opción Wi-Fi 6 (deshabilitable). • Puertos E/S ≥ 4 × USB 3.2 Gen1, 2 × USB-C, audio HD, RJ-45 independientes. • Chasis y PSU: Torre/mini-tower silenciosa, filtro antipolvo, PSU 80+ Gold ≥ 500 W; preparada para funcionamiento continuo 24/7 (MTBF ≥ 50 000 h). • Sistema operativo: Windows 11 Pro 64 bit OEM (o distribución Linux LTS si el VMS lo permite). Sistema preinstalado y activado. • Accesorios: Cableado de vídeo y alimentación, teclado y ratón óptico USB con disposición en castellano.
Resumen funcional	La Workstation suministrada proporcionará la potencia de cálculo y capacidad gráfica necesarias para decodificar y mostrar simultáneamente múltiples cámaras en tiempo real, gestionar alarmas de intrusión desde el cliente VMS y ejecutar análisis de vídeo sin latencias perceptibles. Su arquitectura de procesador multinúcleo y GPU profesional con decodificación

	por hardware garantiza fluidez y estabilidad en entornos 24/7, mientras que el SSD NVMe acelera tiempos de arranque y búsqueda de grabaciones. La doble interfaz de red dota al puesto de redundancia y reserva de ancho de banda; la memoria y almacenamiento ampliables permiten escalabilidad futura sin renovación completa. La garantía NBD asegura continuidad operativa y minimiza tiempos de parada, cumpliéndose así las exigencias de un centro de control de seguridad profesional.

2.2.3.3 INSTALACIÓN Y PUESTA EN MARCHA DEL VMS

VMS-04	Instalación y puesta en marcha del VMS

Alcance	• **Instalación, configuración, integración completa y puesta en marcha** de una plataforma profesional de gestión de vídeo (VMS), diseñada específicamente para la gestión integral del sistema de seguridad dimensionado, compuesto por:
	  ○ 129 cámaras IP gestionadas a través de 3 NVR de hasta 64 canales cada uno.
	  ○ 1 central de seguridad anti-intrusión.
	  ○ 33 contactos magnéticos.
	  ○ 52 detectores PIR.
	  ○ 1 sirena exterior.
	  ○ 14 módulos expansores.
	  ○ 1 teclado de control.
	• **Integración completa y bidireccional de alarmas y eventos** procedentes del sistema anti-intrusión con la plataforma VMS, garantizando:
	  ○ Visualización inmediata, clara y en tiempo real de alarmas e incidencias.
	  ○ Categorización, priorización y reconocimiento directo desde el entorno gráfico del VMS.
	  ○ Vinculación automática de grabaciones de vídeo asociadas a alarmas críticas de intrusión (intrusión confirmada, sabotajes, fallos técnicos).
	• Implementación de un entorno gráfico personalizado y basado en planos interactivos actualizados del edificio, que deberá:
	  ○ Representar visualmente todos los dispositivos instalados (cámaras, contactos magnéticos, detectores PIR, sirena y expansores).
	  ○ Reflejar claramente el estado en tiempo real de cada elemento (funcionamiento normal, alarma activada, fallo técnico, sabotaje).
	  ○ Permitir gestión operativa inmediata y directa desde los planos interactivos del sistema (validación, reconocimiento y resolución de alarmas).

	• Realización obligatoria de pruebas funcionales exhaustivas por parte del adjudicatario, asegurando:
	  ○ Comprobación individual y conjunta de cámaras IP, NVR y dispositivos de intrusión.
	  ○ Validación completa y demostrable de la integración de alarmas y gestión gráfica en planos interactivos.
	  ○ Documentación detallada del proceso y resultados de las pruebas funcionales y de integración.
	• Entrega final completa, incluyendo:
	  ○ Documentación técnica integral, licencias permanentes definitivas activadas, y manuales detallados en castellano para usuario final.
	  ○ Certificado firmado de puesta en marcha que garantice la operatividad completa del sistema.
	  ○ Garantía de escalabilidad, apertura e interoperabilidad mediante protocolos abiertos reconocidos (ONVIF, SIA, Contact-ID, APIs estándar).
	• **Cumplimiento pleno y documentado** de las normativas técnicas aplicables vigentes (RGPD, LOPDGDD, ENS, UNE-EN 62676 y UNE-EN 50131).