SISTEMA GESTIÓN DE LA SEGURIDAD AEROPORTUARIA

MÓDULO CCTV, DESCRIPCIÓN, ANÁLISIS Y MEJORAS APLICABLES

Autor: Rogger Apolo Yauri

ESPACIO INTENCIONALMENTE EN BLANCO

Hoja de identificación del documento

Título:	Sistema de Gestión de Seguridad Aeroportuaria. Módulo CCTV, descripción, análisis y mejoras aplicables
Código:	
Fecha:	08 / 05 / 2020
Fichero:	

Autor:	Rogger Apolo Yauri
Revisor:	Fernando Gómez Comendador. Javier Pérez Castán
Aprobado:	N.A.

Versiones:			
Numero	Fecha	Autor	Comentarios
01	08 / 05 / 2020	Rogger Apolo Yauri	

Resumen ejecutivo

Debido a la necesidad de alcanzar y mantener niveles de seguridad (security) cada vez mayores, se hace cada vez más importante el apoyo tecnológico en las tareas de vigilancia, esto es especialmente importante en aeropuertos grandes, dónde pueden llegar a concentrarse varios miles de dispositivos de videovigilancia y asociados, en lo que se conoce como Circuitos Cerrados de Televisión.

El sistema Gestión de Seguridad Aeroportuaria (GSA) que realiza estas tareas tiene un desfase generacional tecnológico de algo más de un lustro, lo que en muchos casos complica las tareas de mantenimiento y operación debido a la obsolescencia de los equipos, métodos, software etc.

El objetivo de este proyecto es realizar un análisis y clasificación de nuevos sistemas de gestión de video que se puedan integrar con GSA para añadir nuevas funcionalidades y flexibilizar la gestión del sistema ante eventos o alarmas.

Para ello, el proyecto se ha desarrollado realizando:

- Una revisión de la normativa nacional, internacional y propia de Aena que aplica tanto al ámbito de la seguridad aeroportuaria como al de videovigilancia y gestión tecnológica.
- Una descripción de los procesos aeroportuarios que son el primer filtro de seguridad para alcanzar el objetivo de seguridad.
- Un estudio y descripción de la estructura y capacidades de GSA para identificar las carencias del sistema
- El desarrollo de la metodología de análisis, identificando categorías, niveles de importancia y campos dentro del sistema de CCTV para poder clasificar categóricamente todas las características que se pueden encontrar en un manual u hoja de características
- El desglose propiamente dicho de la información proporcionada por los fabricantes Siemens, Milestone, Genetec y Dallmeier, sobre sus productos.
- A partir de este desglose se hace una propuesta para la toma de decisiones futura que deberá desarrollarse a partir de este entregable, teniendo en cuenta la información disponible en el momento de su finalización.

I. Índice de contenido

I. Índice de figuras

II. Índice de tablas

III. Glosario de términos

BBDD	Bases de Datos
CA	Control de Accesos
CCTV	Circuito Cerrado de Televisión
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FPS	*Frames Per Second*
GSA	Gestión de la Seguridad Aeroportuaria
HTTPS	*Hypertext Transfer Protocol Secure*
ONVIF	*Open Network Video Interface Forum*
PE	Protocolo Estándar
PNS	Plan Nacional de Seguridad
PTZ	*Pan Tilt Zoom*
ROP	*Request Of Proposal*
SDK	*Software Development Kit*
UPnP	*Universal Plug and Play*
VMS	*Video Management System*

1 INTRODUCCIÓN

1.1 Objetivo del informe

El objetivo principal del proyecto es sentar la base para comprobar la viabilidad de ampliar la capacidad del subsistema de videovigilancia (CCTV) del sistema de Gestión de la Seguridad Aeroportuaria de Aena, mediante la comparación de varios sistemas de gestión de video, para ello, se ha llevado a cabo un estudio de mercado que analiza las características de productos de cuatro fabricantes seleccionados por su experiencia en el campo de la videovigilancia, Siemens, Milestone, Genetec y Dallmeier para que, a partir de la información recogida en las hojas de características de cada producto seleccionado, desarrollar una tabla con las características desglosadas, que permita compararlos.

El objetivo secundario es sentar la base para que, en un proyecto a futuro, a partir de la metodología propuesta para la clasificación y los resultados recogidos en el desglose, se pueda elegir uno de los productos atendiendo a las funcionalidades que podrían mejorar las capacidades del sistema GSA. Para la clasificación se ha tenido en cuenta todos los componentes del sistema, como son las cámaras, unidades de almacenamiento, cabinas de grabación o gestores de video.

1.2 Alcance

Para el control y la gestión de los dispositivos de seguridad dentro de la red de aeropuertos en España, Aena ha desarrollado una aplicación software con la intención de estandarizar los procesos, las interfaces, la normativa aplicable y en definitiva el desarrollo de la actividad de vigilancia y control en todas las áreas sensibles del aeropuerto. Esta aplicación denominada GSA (Gestión de Seguridad Aeroportuaria) distingue dos grandes campos según la funcionalidad de los dispositivos y procesos asociados, por un lado, Control de Accesos (CA) y por otro, Circuitos Cerrados de Televisión (CCTV) en lo relativo a la videovigilancia.

Este proyecto se centrará en la segunda parte que comprende, fundamentalmente, los dispositivos de cámaras (fijas y móviles) y dispositivos de grabación, así como los sistemas de gestión de video que permiten controlar y gestionar las capacidades de estas dos categorías de dispositivos.

Dado que la filosofía de GSA es poder definir una serie de funcionalidades para los dispositivos que se conecten al sistema sin importar el fabricante ni el dispositivo, es necesario definir una serie de estándares que recojan los requisitos que deberán cumplir dispositivos y sistemas, en lo referente a este proyecto se tiene el Protocolo Estándar de comunicaciones (para CCTV) y la normativa de requisitos técnicos para dispositivos de CCTV, de forma colateral se ha analizado también la normativa DTIC de Aena referente a microinformática y servidores de red.

Para poder implementar mejoras en el sistema, añadiendo nuevas funcionalidades, o dispositivos con mejores prestaciones, se ha elegido cuatro fabricantes, Siemens, Milestone, Genetec y Dallmeier, y un producto[1] de cada uno de ellos, habiendo tenido en cuenta toda la documentación anterior y los catálogos de los distintos productos se ha realizado una clasificación que permita realizar una comparación entre todos ellos para ver cual se ajusta mejor a las necesidades actuales y futuras del sistema, habiendo tenido en cuenta distintas problemáticas de los aeropuertos.

En primer lugar, se ha llevado a cabo una revisión de la normativa aplicable en lo referente a seguridad aeroportuaria a nivel nacional e internacional, por otro lado, la normativa propia de Aena, si bien se ha tenido en cuenta y se cita en los puntos donde es relevante, no se muestra debido a las restricciones bajo las que se distribuye esta información sensible.

En segundo lugar, se recoge una descripción del sistema GSA a nivel lógico y funcional de forma generalizada pues aunque GSA es único, su aplicación en cada aeropuerto en el que está desplegado es totalmente particular pues se ha adaptado para integrarse modificando lo menos posible la estructura ya existente lo cual habría provocado sobrecostes innecesarios y en muchos casos inasumibles, el objetivo de esta parte es dar a conocer los aspectos más importantes y que sientan la base para el análisis posterior.

En tercer lugar, se ha descrito la metodología descrita para realizar el desglose y clasificación, los aspectos tenidos en cuenta, características fundamentales, otras importantes, aunque negociables, características deseables, y características misceláneas. A continuación, se ha procedido a realizar una presentación de los fabricantes seleccionados, para dar una descripción general de cada sistema y para introducir los productos que se han clasificado en una tabla Excel que se ha añadido a este documento en el ANEXO D.

Por último, se presentan las conclusiones de este proyecto, puntos fuertes de cada sistema, problemáticas encontradas y sugerencias para la toma de decisiones posterior.

[1] Para Siemens, Milestone y Genetec el producto es un Sistema de Gestión de Video (VMS), para Dallmeier una cabina de grabación

2 REVISIÓN DOCUMENTAL

En este capítulo se resumen los aspectos más relevantes de la normativa aplicable a este proyecto, si bien se han revisado todos los documentos recogidos en el capítulo 7, aquí solamente se recogen aspectos clave del el Anexo 17 de la OACI y el Programa Nacional de Seguridad recogido en el BOE. La normativa interna de Aena, así como los detalles del Protocolo Estándar no se muestran explícitamente debido a las restricciones de confidencialidad de estos.

Otros aspectos importantes también, pero con menor relevancia directa, se recogen en el ANEXO A y en el ANEXO B, y sirven como complemento a las características recogidas en este capítulo.

2.1 Anexo 17 al Convenio sobre Aviación Civil Internacional

Se ha tomado la décima edición de este Anexo, titulado Protección de la aviación civil internacional contra los actos de interferencia ilícita, correspondiente a abril de 2017 y con entrada en vigor el 3 de agosto de ese mismo año [1].

En este documento se marca como objetivo primordial la seguridad de los pasajeros, las tripulaciones, el personal de tierra y el público general en cualquier asunto relacionado con la protección contra actos de interferencia ilícita, para ello, los Estados deben establecer un organismo que elabore y aplique normas, métodos y procedimientos necesarios para salvaguardar la seguridad de la aviación civil teniendo presente la regularidad y eficacia de los vuelos. Por otro lado, se establece también la necesidad de establecer una autoridad nacional de aviación civil que elabore un programa nacional de seguridad el cuál se detallará en el siguiente apartado de este capítulo, así como en el ANEXO A de este informe.

Del mismo modo, es necesario que cada Estado garantice que tanto los operadores aeroportuarios como los explotadores de aeronaves establezcan apliquen y mantengan sus propios programas internos de seguridad cumpliendo con los requisitos establecidos en su programa nacional de seguridad. Por último, se establece la necesidad de realizar controles de calidad y cualificaciones a los procedimientos y personal tanto para la realización de controles de seguridad como en las auditorías e inspecciones.

Dado el objetivo de este proyecto, el capítulo de mayor interés de este Anexo es el Capítulo 4. *Medidas preventivas de seguridad*, donde se establecen distintas necesidades que deberán traducirse en medidas para evitar la introducción de armas, explosivos u otros artefactos o sustancias potencialmente peligrosos a bordo de las aeronaves para evitar su uso en la comisión de actos de interferencia ilícita o cuyo transporte o tenencia no estén autorizados. El resumen de estas medidas se recoge en el ANEXO B de este informe.

En el capítulo final del Anexo 17 y en sus adjuntos se establecen los distintos criterios para la aplicación de medidas de actuación ante interferencias ilícitas y los procesos de notificación en todos los casos, sin embargo, dada la generalidad de los Anexos de OACI se ha decidido abordar directamente la normativa nacional, recogida en el Plan Nacional de Seguridad.

2.2 Plan Nacional de Seguridad para la Aviación Civil

Texto legal consolidado, a nivel nacional y recogido en el Boletín Oficial del Estado, para este proyecto se ha tenido en cuenta la versión correspondiente a la modificación del 1 de agosto de 2019 [2].

Se declara de uso público la parte del PNS que afecta directamente a los pasajeros y aquella que, en el ámbito interno, constituye aplicación de las medidas comunes de seguridad aérea que no tienen carácter de información clasificada de la Unión Europea.

En este apartado se rescatan los Principios Generales del Plan pues son los que sientan la base para los procesos de seguridad en los aeropuertos, dada la extensión del documento, se ha decidido recoger en el ANEXO A algunos párrafos y subpárrafos más extensos del Capítulo 1 que sirven como complemento a los Principios aquí mencionados.

2.2.1 Principios Generales

Marcan el contexto en el cual se aplican las medidas del PNS, se compone de tres artículos:

a) Artículo 1: Objetivo y alcance del programa

b) Artículo 2: Definiciones

c) Artículo 3: Referencias normativas y legislativas

A continuación, se desarrollan los puntos del artículo 1 ya que los otros dos no son tan relevantes para el objetivo de este proyecto.

2.2.1.1 Objetivo y Alcance del Programa

"El PNS tiene como finalidad establecer la organización, métodos y procedimientos necesarios para asegurar la protección y salvaguarda de los pasajeros, tripulaciones, público, personal de tierra, aeronaves, aeropuertos y uss instalaciones, frente a actos de interferencia ilícita, perpetrados tanto en tierra como en el aire, intentando preservar la regularidad y eficiencia del tránsito aéreo nacional e internacional en el Estado español y su espacio aéreo"

"La Autoridad competente para la seguridad en la aviación civil, en el ámbito de sus competencias, hará cumplir las medidas contenidas en el Programa, siendo éstas de obligada aplicación en la totalidad de los aeropuertos nacionales e instalaciones de navegación aérea, así como en los helipuertos con vuelos comerciales. Asimismo, las compañías y explotadores afectos al transporte aéreo están igualmente obligados a la aplicación de las normas contenidas en el PNS, con las responsabilidades y limitaciones de aplicación que se establecen en el documento"

2.2.1.2 Ámbito de Aplicación y Limitaciones

Las medidas y procedimientos descritos en el Programa deben aplicarse en:

a) Todos los aeropuertos nacionales, helipuertos e instalaciones de navegación aérea, tanto incluidas como no incluidas en recinto aeroportuario.

b) *Todos los operadores, incluyendo a las compañías aéreas, que presten servicios en los aeropuertos mencionados en la letra a).*

c) *Todas las entidades que aplican normas de seguridad aérea que lleven a cabo sus actividades en locales situados dentro o fuera de las instalaciones del aeropuerto y suministren bienes y/o servicios a los aeropuertos mencionados en la letra a) o a través de ellos.*

"Quedarán fuera del ámbito de aplicación del Programa Nacional de Seguridad las Bases Aéreas y los aeródromos militares que reciban eventualmente tráfico civil. No obstante, llegado el caso, se aplicarán aquellas medidas que, consensuadas entre la Autoridad competente de Seguridad de la Aviación Civil y el Ministerio de Defensa garanticen un adecuado nivel de protección. De igual manera, quedarán fuera del ámbito de aplicación del Programa Nacional de Seguridad las aeronaves de Estado.

Cuando no sea posible la aplicación de determinadas medidas en algunos aeropuertos o helipuertos, se podrán aplicar medidas alternativas que garanticen un nivel adecuado de seguridad conforme a lo dispuesto en disposiciones adicionales de carácter restringido aprobadas por la Autoridad competente."

En cualquier caso, estos aeropuertos y/o helipuertos presentarán un Programa de Seguridad para aprobación por la Autoridad competente."

2.2.1.3 Otros Programas de Seguridad para la Aviación Civil

El PNS marca las líneas generales de cumplimiento de normas básicas en materia de seguridad y protección de la seguridad de la aviación civil en el Estado español. Se complementa con la adopción e implementación de procedimientos para:

- Control del cumplimiento de normas y métodos comunes: a través del Programa Nacional de Control de Calidad de la Seguridad de la Aviación Civil (PNC).
- Formación en seguridad: a través de un Programa Nacional de Formación de Seguridad de la Aviación Civil (PNF).
- Protección de aeropuertos e instalaciones de navegación aérea designados como infraestructuras críticas: los programas de seguridad se consideran como Planes de Protección Específicos.

"En cualquier caso, el Ministerio del Interior podrá proponer contenidos adicionales en conformidad con lo establecido en el artículo 25, apartado quinto del Real Decreto 704/2011"

Por otro lado, los integrantes del sistema de transporte aéreo como aeropuertos, compañías o entidades deben establecer sus propios programas de seguridad en los que se establecerán medidas del control del cumplimiento y control de calidad de la aplicación de las medidas y requisitos descritos en el PNS, se distingue así:

a) Programas de Seguridad de aeropuertos y compañías aéreas: evaluados y aprobados por la Autoridad competente para aeropuertos nacionales, helipuertos con vuelos comerciales y compañías aéreas que presten servicios desde el Estado., y

b) Programas de Seguridad de entidades

2.2.1.4 Alcance del Programa Nacional

El PNS se ha estructurado para sistematizar los procedimientos de aplicación y se ha ordenado para facilitar los procesos de auditoría e inspección del cumplimiento según lo establecido en el Reglamento (CE) 300/08

a) Principios generales.

"Establece la finalidad y ámbito general de aplicación del Programa; las definiciones aplicables en el contexto del sistema de seguridad de la aviación civil español; referencias normativas y legislativas; y finalmente las actividades de coordinación internacional inherentes al Programa Nacional, así como los procesos de comunicación en situaciones de contingencia que prevé el mismo."

El Programa Nacional de Seguridad se estructura en un total de 15 capítulos y un Anexo con 10 Adjuntos ordenados de la "A" a la "J" de la siguiente forma:

b) Capítulos del PNS

"En los Capítulos 1 y 2 se recogen los métodos y procedimientos específicos de seguridad en relación con la seguridad en los aeropuertos. En el caso del capítulo 2 se determinan los criterios establecidos para adoptar medidas de seguridad alternativas a las normas básicas comunes de seguridad en los aeropuertos o en las zonas demarcadas de los aeropuertos.

En el Capítulo 3 se recogen los métodos y procedimientos específicos de seguridad en relación con la seguridad de las aeronaves.

Los Capítulos 4 y 5 se refieren al control de pasajeros y equipajes de mano y en bodega.

El Capítulo 6 establece requisitos del control de la carga y el correo.

Los Capítulos 7 y 8 indican los controles aplicables al correo y material de las compañías aéreas, así como a las provisiones de a bordo.

El Capítulo 9 indica los controles aplicables a los suministros de aeropuerto.

El Capítulo 10 establece las medidas de seguridad que se aplicarán durante el vuelo.

El Capítulo 11 establece las competencias que debe adquirir el personal que aplica controles de seguridad.

El Capítulo 12 establece los requisitos de utilización y mantenimiento de los equipos de seguridad.

El Capítulo 13 enuncia la necesidad de establecer un Programa Nacional de Control de Calidad en materia de seguridad.

El Capítulo 14 establece las definiciones de las áreas y medidas necesarias para garantizar la protección de las instalaciones y dependencias de Navegación Aérea con independencia de su ubicación.

El Capítulo 15 establece las referencias de actuación frente a actos de interferencia ilícita, así como los medios necesarios en relación con estas contingencias.

c) *Anexo A: Instrucciones de seguridad (SA).*

Establece directrices complementarias a la aplicación de las normas básicas y procedimientos establecidos en su capitulado a través de las Instrucciones de Seguridad."

2.2.1.5 Cumplimiento del Programa y sanciones

"La Autoridad competente por su parte, velará por el cumplimiento de la norma y verificará su eficacia y correcta implantación a través del ejercicio de auditorías en todas sus formas. El carácter y procedimientos de estas evaluaciones de seguridad se recogen en el Programa Nacional de Control de Calidad de la Seguridad de la Aviación Civil. Los gestores aeroportuarios, los operadores de transporte aéreo y en general todas las compañías que desarrollen su actividad en el entorno aeroportuario tienen el deber de someterse a tales auditorías y colaborar en su desarrollo ofreciendo los medios técnicos y humanos para su correcta realización.

El incumplimiento de las normas contenidas en el presente programa, puede ser objeto de sanción según se establece en la Ley de Seguridad aérea 21/2003."

ESPACIO INTENCIONALMENTE EN BLANCO

3 PROCESOS AEROPORTUARIOS

3.1 Introducción

Dentro de un aeropuerto un pasajero puede realizar dos trayectos básicos, bien embarcar en un avión para realizar un vuelo nacional o internacional, o bien desembarcar de un avión nuevamente con un origen nacional o internacional. En algunos casos y gracias a los distintas alianzas y modelos de negocio de las compañías aéreas, es posible realizar transbordos o transferencias, respectivamente, que el pasajero haga una escala en el aeropuerto volviendo a embarcar en un avión de otra compañía o que dicho avión pertenezca a la misma compañía o alianza. En cualquier caso, estos últimos pasajeros se introducirían dentro de uno de los tramos de un flujo de llegadas, de salidas o de ambos ya que, por un lado, los pasajeros en transferencia deben esperar en el lado aire (zona restringida) del aeropuerto no pudiendo mezclarse con los pasajeros en el lado tierra y, por otro lado, los pasajeros que realicen un transbordo, en general completarán el último tramo de llegada, debiendo recoger su equipaje (realizando el paso por la aduana y control de pasaportes si fuera necesario) y volviendo a facturar y completar el control de seguridad antes de volver a embarcar en su siguiente vuelo el cual además puede producirse en un periodo bastante más prolongado que en una transferencia.

Como se ha ido indicando en la revisión normativa, todos estos flujos entorno a los cuales se definen los procesos aeroportuarios (facturación, embarque, traslado y recogida de equipajes…) deben estar protegidos y debidamente controlados para garantizar la seguridad (física) de los pasajeros, además de la continuidad en las operaciones, para ello, se aplican al menos todas las medidas descritas pormenorizadamente en la normativa nacional, en el caso de España el PNS.

Se tiene así, por ejemplo, para un pasajero en salidas:

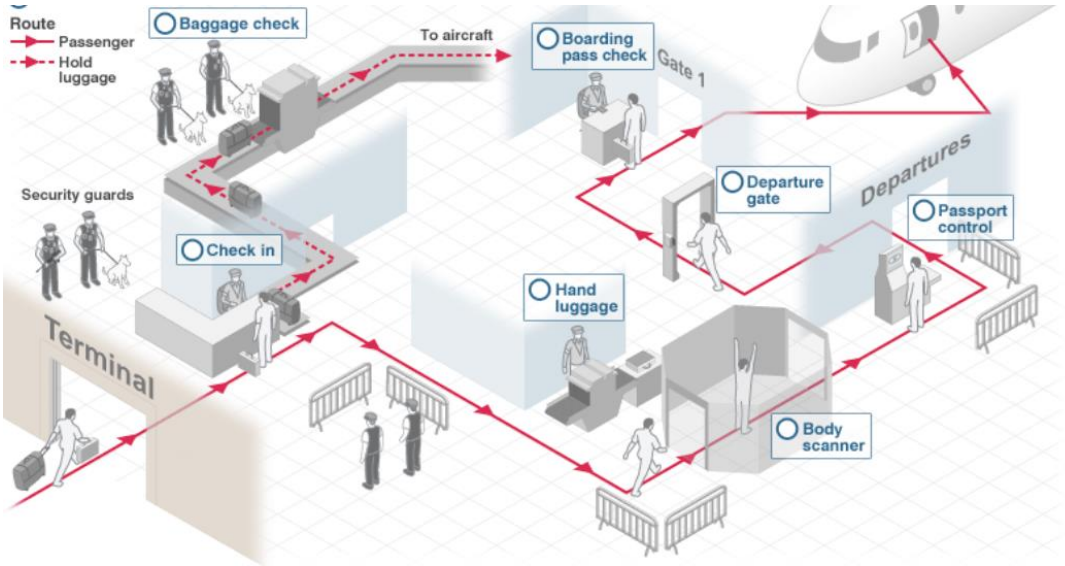

Figura 1. Diagrama de flujo de un pasajero en salidas, fuente [3]

Con el objetivo de ahorrar tiempo y dinero a los pasajeros y compañías, se intenta que todos estos procesos sean lo más cómodos y simplificados posible. De esta forma han ido automatizándose y virtualizándose, aprovechando las nuevas tecnologías móviles y las facilidades de internet, por ejemplo, con la posibilidad de realizar el check in desde la página web de la compañía, mediante un teléfono móvil o mediante terminales individuales (para pasajeros sin equipaje facturado, aunque se están probando prototipos para pasajeros que viajen con bultos facturados).

Por ejemplo, en el aeropuerto Adolfo Suárez Madrid-Barajas:

Figura 2. Mostradores de Self check in de Iberia, sin equipaje (izquierda) y con equipaje (derecha)

Hoy en día éste es el proceso más fácilmente automatizable, sin embargo, el control de seguridad y el embarque son procesos mucho más delicados y sobre todo lentos, lo cual repercute en la experiencia del pasajero, aun así, es algo que se asume como propio del transporte aéreo, de ahí que esté socialmente normalizado el llegar al aeropuerto dos o incluso tres horas antes de la hora prevista de despegue pues los propios pasajeros asumen la importancia de la seguridad.

Todos los procesos representados en la Figura 1 y algunos adicionales como el control (registro) de aduanas o controles sanitarios en caso de riesgo de contagio están definidos y pensados para controlar directamente a los pasajeros y su equipaje, para poder prevenir los actos de interferencia ilícita o terrorismo ya que es la forma más simple (y por tanto vulnerable), de acceder a las zonas restringidas de uso público de un aeropuerto. Además, es habitual que estos controles sean llevados a cabo por personal de las FCSE quedando por lo tanto la legislación pertinente fuera del alcance de este proyecto.

3.2 Seguridad perimetral y control de accesos

Como se ha mencionado en el capítulo 1, este proyecto se centrará en tipo de vigilancia y control para el mantenimiento de la seguridad física global, es decir, mediante el análisis no tanto de personas sino de zonas en los aeropuertos, distinguiendo principalmente dos grandes campos [3]:

- **Seguridad perimetral**

Relacionado directamente con la vigilancia llevada a cabo mediante dispositivos de CCTV y sensores asociados, que permiten obtener un estatus en tiempo real de todo lo que sucede en el aeropuerto al menos durante las horas en las que se encuentre en funcionamiento.

- **Control de accesos**

Relacionado con la separación de zonas de acceso al público (público general y pasajeros) frente a las de acceso restringido al personal aeroportuario como pueden ser los patios de carrillos, la torre de control o las zonas de mantenimiento, para lo cual se requiere tener una acreditación.

3.2.1 Distribución de zonas y tipos de terminal

Con este nuevo enfoque, es necesario recuperar la clasificación de zonas dentro del aeropuerto definida en el PNS: públicas, restringidas y críticas. Como se muestra en la Figura 3 y, en concordancia con lo estipulado en la normativa, para una terminal aeroportuaria genérica es posible definir estas zonas agrupando funcionalmente elementos de los distintos procesos aeroportuarios.

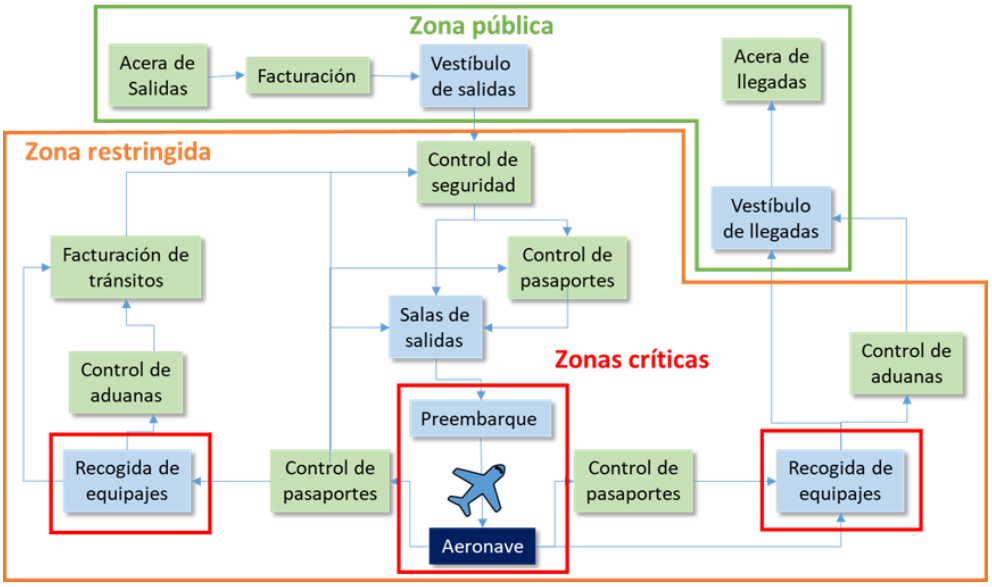

Figura 3. Distribución de zonas en una terminal aeroportuaria, fuente [4]

Como ya se ha mencionado en la introducción de este capítulo, los flujos de pasajeros, llegadas y salidas no pueden mezclarse entre sí para no comprometer la seguridad de los procesos aeroportuarios, por ello, todas las conexiones entre bloques de la Figura 3 pueden considerarse como separaciones físicas propiamente dichas con la excepción en la zona pública.

Estas separaciones deben estar optimizadas para no ralentizar innecesariamente los flujos, lo cual conlleva a no tener un modelo estándar de terminal, pues la separación física de las zonas puede realizarse tanto en horizontal como en vertical, dando lugar a infinidad de posibles construcciones

completamente funcionales, a modo de ejemplo se puede citar la terminal 4 de Barajas, la cual separa verticalmente los flujos de llegadas y de salidas, llegando al punto de poder acceder con un vehículo propio hasta la misma puerta de la terminal de llegadas o la de salidas.

En cualquier caso, la forma más habitual de separar las zonas públicas de las restringidas es mediante el uso de corredores de no retorno consistentes en un pasillo de dos puertas automáticas que solamente se abren desde un lado para garantizar el movimiento de personas en un único sentido.

4 SISTEMA GSA

En este capítulo se realizará una descripción GSA a nivel funcional y a nivel estructural, citando las funcionalidades a nivel usuario del sistema y describiendo las características internas a nivel lógico y técnico siempre que sea posible, con el fin de dar una visión general de cómo funciona el sistema para así poder identificar sus carencias, problemas y posibilidades de mejora.

4.1 Interfaz y funcionalidades

En la Figura 4 se muestra la interfaz de inicio de la aplicación a la que un usuario cualquiera tendría acceso, en este caso se observa desde un perfil de administrador con lo cual todos los iconos estarían disponibles y con todas sus opciones completamente disponibles, por lo que está es la interfaz más genérica que un usuario podría encontrares, pues para perfiles con menos derechos, algunos accesos podrían estar restringidos o vetadas algunas opciones de personalización o configuración.

Figura 4. Menú principal de GSA, fuente [5]

Los distintos iconos permiten acceder a diferentes aplicaciones dentro del sistema, de izquierda a derecha:

1) Configuración de tarjetas de acceso (acreditaciones)
2) Gestión de visitas.
3) Acreditaciones de vehículos
4) Rondas
5) Centro de control sinóptico
6) Centro de control CCTV
7) Reproducción CCTV
8) Editor de sinóptico
9) Informes

10) Administración y configuración

En los capítulos siguientes se recogen las características principales del Protocolo Estándar de comunicaciones y el módulo de CCTV., el detalle de cada una de las funcionalidades de GSA mencionadas se recoge en el ANEXO C.

4.2 Protocolo estándar

Se denomina Protocolo Estándar [6] a una serie de protocolos de comunicación estandarizados, para comunicar el sistema con los distintos dispositivos de campo directamente relacionados con la seguridad aeroportuaria, a dos niveles:

- Tecnológico: especificando qué tecnologías son válidas para realizar la interacción con los dispositivos.
- Funcional: definiendo las funcionalidades máximas y mínimas requeridas para cada que cada tipo de dispositivo pueda realizar una misión dentro del sistema.

La necesidad de definir un protocolo común surge de la dificultad de compatibilizar dispositivos de distintos fabricantes, lo que obliga en muchas ocasiones a depender total o parcialmente de la evolución del producto de un único fabricante a la hora de introducir mejoras o ampliar funcionalidades dentro del sistema, lo que deriva en pérdidas de oportunidades económicas y dificultades a la hora de evaluar (comparar) la compatibilidad de productos de terceros fabricantes con respecto a otros.

De esta forma, aceptando solamente productos calificados con el cumplimiento de un protocolo estándar, se garantizar la integración completa de cualquier dispositivo con el sistema GSA y además se simplifica el proceso de certificación de las capacidades requeridas por el sistema.

Dado que estos protocolos están sujetos a cambios relacionados con las mejoras tecnológicas que se van incorporando al mercado de dispositivos, es necesario definir una serie de requisitos que se deben tener en cuenta a la hora de definir nuevos protocolos o modificar los ya existentes, principalmente atendiendo a:

- Viabilidad del cumplimiento por parte de los fabricantes y/o integradores, adoptando para ello restricciones o requisitos cuya implementación entre dentro de lo razonable.
- Flexibilidad para los fabricantes en la implementación, de forma que no se limite la utilización de múltiples herramientas o plataformas (especialmente en el desarrollo del software).
- Mantenibilidad y extensibilidad de las funciones y la vida útil de los dispositivos, de forma que la integración de modificaciones o mejoras se realice de la forma más sencilla posible.
- Estandarización, de forma que la comunicación entre sistemas esté lo más unificada posible, intentando en la medida de lo posible, evitar diferenciar entre dispositivos de distintos fabricantes.

Es por ello por lo que el desarrollo del sistema GSA atiende a una arquitectura orientada a servicios (SOA) y no a dispositivos, lo que se busca es cubrir una serie de necesidades en forma de funciones dentro del sistema, para lo cual no es necesario definir un dispositivo concreto. Entendido un servicio como una unidad de trabajo realizada por un proveedor de servicios para conseguir unos resultados finales entregables a un consumidor de servicios.

En una red de tipo SOA, los nodos comparten sus recursos con cualquier participante dentro de dicha red como servicios independientes a los que se accede siempre de la misma forma, mediante interfaces predefinidos. Estos servicios están débilmente acoplados entre sí para garantizar una alta interoperabilidad haciendo que las comunicaciones sean independientes de la plataforma subyacente (hardware) y el lenguaje de programación (software), encapsulando para ello la interfaz de comunicaciones, ocultando así cualquier particularidad durante la implementación, con ello, se garantiza que los componentes de software desarrollados sean reutilizables.

Gracias al compromiso de la industria y organizaciones internacionales de estandarización, se han desarrollado una serie de definiciones/especificaciones comúnmente aceptadas por la industria a las que se ha denominado perfiles, el más útil en este campo se denomina ONVIF y ha sido adoptado por la práctica totalidad de los fabricantes de cámaras, software y equipos de comunicación.

El tipo de servicios elegidos para operar con esta arquitectura son los servicios web ya que permiten combinar dos tecnologías de amplio uso en la actualidad, el lenguaje XML para descripción de datos y el protocolo de transporte HTTP, soportado por la práctica totalidad de navegadores y servidores web. Debido a esto, este tipo de servicios son autocontenidos y autodescriptivos ya que ni el cliente ni el servidor necesitan conocer los detalles del servicio pues solamente deben conocer el formato y el contenido de los mensajes asociados a la petición y a la respuesta de la comunicación realizada.

De esta forma, la estructura de comunicaciones de GSA se puede resumir con un diagrama de flujo como el de la Figura 5, dónde cada flecha doble se corresponde con un protocolo estándar de comunicaciones diferente y único para cada tipo de dispositivo, incluyendo además un elemento denominado “interfaz de campo compatible” que es básicamente un traductor entre el protocolo estándar de GSA y el protocolo del fabricante para con el dispositivo de campo.

Los servicios web utilizados deben contar con una serie de esquemas o componentes que caractericen los mensajes intercambiados, por un lado, un archivo descriptor del servicio en lenguaje WSDL, que defina los requisitos del protocolo y el formato de los mensajes, necesarios para interactuar con los servicios guardados en su catálogo. Por otro lado, un esquema XML donde se detallen los diferentes tipos de datos utilizados en el archivo WSDL.

Esta pareja de archivos, WSDL y XSD debe permanecer inalterados en todo momento ya que se utilizarán como patrón de implementación (tabla de traducción) para garantizar que el interfaz de comunicación es correcto.

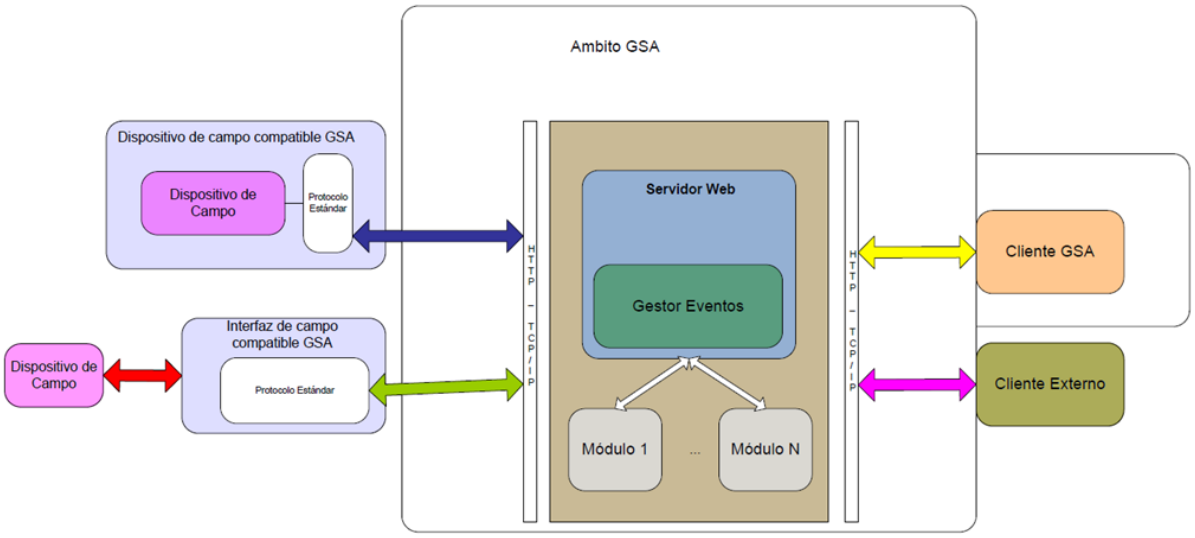

Figura 5. Estructura funcional de GSA, fuente [6]

Este protocolo se describe de forma detallada en el documento Protocolo estándar para CCTV de GSA de Aena [6], incluyendo la estructura de los mensajes y las funcionalidades de cada uno de los dispositivos de campo dentro del sistema GSA. Debido a la extensión y sensibilidad de esta información, en este informe no se profundizará mucho más en el contenido del documento, en su lugar, se procederá a describir la arquitectura del sistema en la rama de CCTV.

4.3 Arquitectura de la red CCTV

Dentro del sistema GSA, se distinguen dos redes, principales, la primera de Control de Accesos y la segunda y objeto de análisis de este documento, la red de CCTV, la cual cuenta con dos tipos principales de estructura lógica, la primera se muestra en la Figura 6, que muestra una arquitectura centralizada con el uso de un elemento denominado conector por el cual pasan todas las comunicaciones de los dispositivos de CCTV (principalmente cámaras IP, aunque también codificadores y decodificadores y cabinas de almacenamiento) que garantiza que las comunicaciones se realizan siguiendo el Protocolo Estándar.

Una de las principales características del sistema GSA es que el sistema se apoya en el software propio de los fabricantes de cámaras y grabadores, y se almacena (reside) en lo que en el esquema de la Figura 6 se ha denominado Servidor de CCTV [7]. Estos servidores se encargan de gestionar las grabaciones realizadas por cada cámara y almacenar dichas grabaciones en el Sistema de Almacenamiento, el cual se compone de cabinas de almacenamiento con discos duros en configuración de particiones tipo RAID-5 o similar.

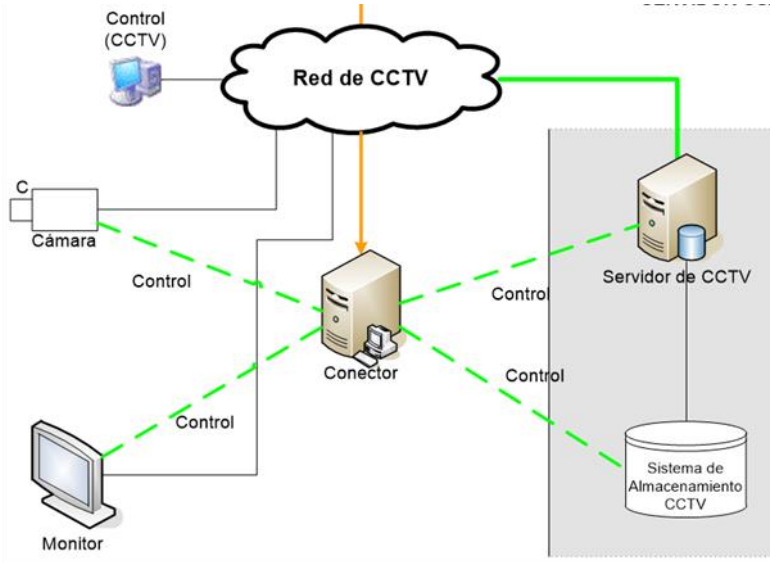

Figura 6. Arquitectura CCTV con conector, fuente [7]

Para permitir la interacción entre el software propio de GSA y el software de los fabricantes, se emplea el conector, el cual es básicamente un traductor de Protocolo a estándar a protocolo de fabricante y viceversa, siguiendo el diagrama de flujo:

Puesto de control (cliente) de CCTV → Servidor GSA → Conector → Dispositivo CCTV

Dónde los dispositivos de CCTV son los periféricos hardware soportados son [7]:

- Cámaras: dispositivos que captan y transportan señales de video en forma de flujos (streams) de video, con una compresión tipo MPEG4 o H.264, pueden ser de dos tipos atendiendo a su capacidad de movimiento, estáticas o móviles (con función de telemetría) en cuyo caso deben poder moverse, manual y automáticamente.
- Decodificadores: Transforman los flujos de video codificados y comprimidos en los formatos anteriormente mencionados a señales de video visualizables en una pantalla tipo LCD o similar, denominando como "monitor" dentro de GSA a cada representación de la imagen de una cámara y layout a cada distribución de monitores.
- Servidores CCTV: actúan como gestores de grabaciones, monitorizando y gestionando la configuración de las grabaciones de las cámaras en el Sistema de Almacenamiento, son el punto de unión con los dispositivos de grabación (grabadores).

Con cada uno de estos dispositivos se construyen diferentes funcionalidades dentro de GSA, cada una de las cuales es lo que se denomina Dispositivo de Campo propiamente dicho, distinguiendo hasta la fecha, tres tipos:

- Cámaras: Dispositivos que permiten visualizar video, en caso de que tenga función de telemetría además permitirá mover el objetivo de la cámara. Aparte de las visualizaciones, tienen asociados flujos de grabación de tres tipos, continuo, que se almacena automática y constantemente en los grabadores, bajo demanda a petición de un usuario, y grabaciones por evento donde además se incluyen buffers de memoria pre y post de longitud modificable.
- Monitores: Dispositivo que permite la recepción de flujo de video proveniente de **una** sola cámara, siendo posible agrupar en un mismo descodificador varios Monitores para visualizar varias cámaras en una sola pantalla, formando una distribución concreta o layout.
- Grabador: Dispositivo que permite gestionar los flujos de grabación de las cámaras, de cualquiera de los tres tipos mencionados, este dispositivo recibe las órdenes de GSA vía el conector para iniciar o parar las grabaciones.

El segundo tipo de arquitectura utiliza tecnología de tipo Onvif, y se muestra en la Figura 7, con esta arquitectura se distinguen dos configuraciones, Dispositivos Onvif y Grabadores externos o Dispositivos y Grabadores Onvif. Este estándar ha sido adoptado por la gran mayoría de fabricantes como ya se mencionó en el capítulo 4.2, permitiendo así simplificar mucho la estructura del sistema.

En esta configuración, los Dispositivos de Campo de tipo cámara son manejados directamente por GSA aunque se mantiene el elemento conector para la búsqueda, visualización y exportación de grabaciones, del mismo modo, las cámaras siguen almacenando el video en el Sistema de Almacenamiento mediante el Servidor de CCTV.

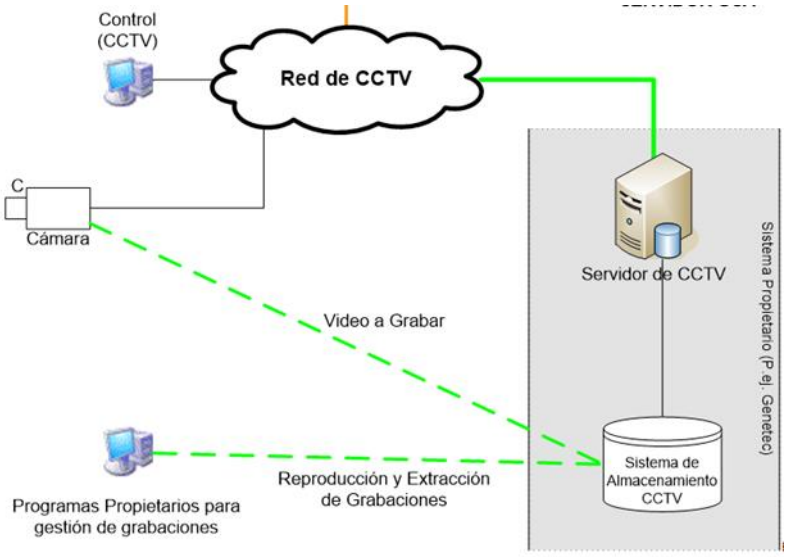

Figura 7. Arquitectura CCTV con tecnología Onvif, fuente [7]

En caso de que tanto los dispositivos como los grabadores cuenten con tecnología Onvif, el conector desaparece y es el sistema GSA el que gestiona completamente todos los dispositivos, debiendo realizar la configuración de las grabaciones específicamente en cada uno de los grabadores.

4.3.1 Especificaciones hardware

Para el caso del Conector, el Sistema de gestión de CCTV y el servidor de transcodificación, se dedican servidores dedicados para el software de cada uno, siendo además virtualizados en el entorno de virtualización Windows de cada uno de los aeropuertos, siendo además gestionados por la normativa DTIC de Aena.

El resto de casos se describen a continuación [7]:

- Sistema de almacenamiento CCTV gestionado externamente: el dimensionamiento dependerá del número de cámaras de las que conste el sistema, considerando que para cada cámara se debe almacenar como máximo el periodo definido por la LOPD. A modo de ejemplo se citan las características más destacables:
    - Protocolo de red: iSCSI.
    - Almacenamiento: RAID-5
    - Capacidad máxima: mayor de 8 TB si se montan todos los discos
    - Discos duros: capacidad de intercambio caliente (hot stand-by)
- Sistema de almacenamiento CCTV con tecnología Onvif: nuevamente, el dimensionamiento dependerá del número de cámaras Onvif manejadas por el sistema, considerando como periodo máximo el definido por la LOPD, las características más destacables son:
    - Protocolo de red: Ethernet
    - Almacenamiento: RADI-5
    - Capacidad máxima: mayor de 8 TB si se montan todos los discos
    - Discos duros: capacidad de intercambio caliente (hot stand-by)
- Cámaras: deben ser de tipo IP, esto es, que envíen la imagen por una red de datos codificada en un formato estándar, si bien aún se mantienen en funcionamiento cámaras analógicas en algunos aeropuertos. Para estos dispositivos, se definen requisitos en:
    - Óptica: resoluciones y sensibilidad lumínica, también los requisitos de la analítica de video y detección de movimiento.
    - Telemetría (PTZ): capacidad de movimiento 360º y con hasta 99 preposicionamientos.
    - Codificador IP: dos flujos de video configurables independientemente, uno para la grabación y otro para la visualización, en formatos MPEG-2/4 y H.264, codificación RTP-IP, limitación a 10 Mbps de ancho de banda, con resoluciones desde CIF hasta 1920p y una tasa de muestreo de hasta 30 fps.

- Alimentación
- Carcasa envolvente

- Descodificadores: se distinguen dos tipos, el descodificador IP simple para cámaras de baja o media definición y el descodificador IP avanzado para cámaras de alta definición. Este elemento puede ser un equipo diseñado propiamente para decodificar los datos de video o un PC con ese propósito general con un software capaz de comunicarse con GSA mediante Protocolo Estándar, en este caso se definen requisitos de:
  - Flujos de entrada: debe admitir hasta 25 flujos para presentar la salida en cuadrícula de 5x5, pudiendo seleccionar individualmente cada uno de los flujos, en formato MPEG-4 y H.264 y Onvif, y en general los mismos requisitos que el codificador de la cámara.
  - Capacidad de proceso: de dos a doce flujos en compresión H.264, en calidad decreciente, a 30 fps y con limitación del ancho de banda para cada uno.
  - Salidas de video digital
  - Estándares soportados: Gigabit Ethernet, compatibilidad multicast (IGMP versiones 2 y 3) y compatibilidad Onvif
  - Sincronización horaria: por protocolo NTP o SNTP

4.3.2 Especificaciones funcionales

Dentro de las especificaciones funcionales cabe destacar las fases de funcionamiento de los Dispositivos de Campo, estas fases se describen de forma detallada en el Protocolo Estándar, y consisten básicamente en un bucle de comunicaciones entre los dispositivos y el sistema, mediante el cual los dispositivos solicitan el alta (para empezar a funcionar) en el sistema y una vez GSA los ha reconocido, envía un mensaje denominado *Keep Alive* de forma periódica, manteniéndose en un bucle de N tiempos *Keep Alive* hasta que falle la comunicación o GSA quiera desconectar el dispositivo.

Es importante tener en cuenta también la necesidad de sincronización horaria, la cual será obligatoria para todos los servidores (conector, gestión CCTV y almacenamiento), las cámaras y codificadores y monitores y descodificadores.

Esta sincronización se realiza por protocolo NTP, mediante el envío de paquetes NTP hacían un servidor de hora de referencia, cuya designación depende de cada aeropuerto, con una periodicidad no superior a 60 minutos. Por otro lado, los cambios de hora propios del horario de invierno y de verano, deben realizarse localmente incluso si no hay comunicación con un servidor NTP o similar. También se acepta que las cámaras y monitores realicen esta sincronización mediante los servidores de Conector o de Gestión CCTV siempre y cuando estos servidores la obtengan mediante un servidor NTP.

En cuanto a los requisitos funcionales propios de cada elemento de CCTV, se tiene [7]:

- Conector: como ya se mencionado a lo largo de estos capítulos, el conector actúa como traductor entre el Protocolo Estándar de GSA y el formato de mensajería propio de cada fabricante, por ese motivo, la práctica totalidad de las acciones disponibles desde GSA sobre sus dispositivos se llevan a cabo pasando por este dispositivo, exceptuando:
    - Visualización del flujo de video desde una cámara Onvif.
    - Solicitud de una sesión de reproducción desde el cliente GSA al Reproductor (Servidor de CCTV), cabe destacar que esta comunicación no se realiza por Protocolo Estándar sino a nivel de video SDK, aún así se mantiene el diagrama de flujo habitual del conector.
    - Visualización de flujo de video grabado

Por otro lado, desde el Conector deben poder realizarse las siguientes funciones:

- Habilitar y deshabilitar Dispositivos de Campo individualmente.
- Modificación del GUID y del Alias de cada Dispositivo de Campo, priorizando la modificación del Alias frente al GUID.

En cuanto a las configuraciones de red de los dispositivos, se establecen tres tipos en el Protocolo Estándar, distinguiendo entre la configuración de red propia del conector (con su máscara, su puerto y su dirección IP), del equipo o de telemetría, si la cámara dispone de esta función.

- Cámaras: como ya se ha mencionado, las cámaras deben devolver al menos dos flujos, uno de grabación y otro de visualización, sea mediante conector o mediante tecnología Onvif, en cualquier caso, se establecen restricciones:
    - Modificación manual de las características de flujo, solamente para el stream de visualización se podrá modificar la tasa de muestreo, la resolución o la calidad del video mediante mensajes de Protocolo Estándar, en caso de que no sea posible modificar el flujo de visualización sin afectar a los parámetros del de grabación, la orden de modificación será ignorada por el sistema.
    - Configuración multicast, debe ser posible para todas las cámaras conectadas a GSA, al igual que para el funcionamiento en unicast, las direcciones IP y los puertos no se asignan desde GSA sino en la configuración previa de la cámara. La conmutación unicast-multicast debe ser posible mediante Protocolo Estándar y además excluyente en el caso de flujo de video, manteniendo para el resto de comunicaciones la dirección IP, la máscara y el puerto unicast.
    - Pérdidas de conexión, deben ser gestionadas por el Conector, el cual deberá notificar la ocurrencia de dicho fallo y cancelar los mensajes *Keep Alive* mientras dure, realizar nuevamente la solicitud de alta una vez solucionado (si se requiere) y recuperar las conexiones cámara monitor previos al fallo.

- Onvif, las cámaras deben ser compatibles con el perfil S de Onvif de acuerdo con la documentación accesible desde el portal oficial de Onvif:

  (http://www.onvif.org/Documents/Specifications.aspx)

- Grabadores: como ya se ha mencionado, las cámaras pueden manejar tres tipos de grabaciones, de forma continua, manual y por evento (pre-post), con las siguientes características:
  - Continua, de carácter permanente y con calidad baja para minimizar el gasto de espacio de almacenamiento. Cuando se busquen grabaciones deberá aparecer una grabación continua por cada cámara con hora de finalización la hora actual.
  - Bajo demanda, de carácter esporádico a petición de un usuario y con calidad superior, la duración de estas grabaciones queda a decisión del usuario y no está limitada por GSA, las órdenes de inicio y parada se realizarán por Protocolo Estándar y se deberá registrar de forma precisa la hora de inicio y de finalización, de ahí la importancia de la sincronización horaria.
  - Por evento (pre-post), estas grabaciones se activan de forma programada ante la ocurrencia de un evento en el sistema, por ejemplo una alarma aunque no exclusivamente, y se guardan con una calidad superior. Se llevan a cabo mediante el envío de una única orden, la de inicio de grabación, por parte de GSA, en estas grabaciones la duración viene marcada por dos tiempos, uno el de la grabación de un buffer (tiempo pre) y otro tiempo fijo sumado al de la orden de inicio (tiempo post).

    Ambos tiempos son de una longitud fija y preconfigurada, no inferior a un minuto para el caso del tiempo post, para el caso del tiempo pre se admite una longitud nula. Para la obtención de datos de video en alta calidad de la grabación correspondiente al tiempo pre, es necesario disponer de un buffer de memoria temporal gestionado desde el Servidor de gestión CCTV.

El término calidad hace referencia a la combinación de parámetros de resolución, tasa de muestreo (fps) y ancho de banda del flujo de video. Debe ser posible configurar tres calidades distintas para cada uno de los tipos de grabación, modificando los parámetros que la cámara permita, por ejemplo, en el caso de compresión H.264 solamente es posible cambiar la tasa de muestreo, pero no la resolución.

Todas estas características se ilustran en la Figura 8:

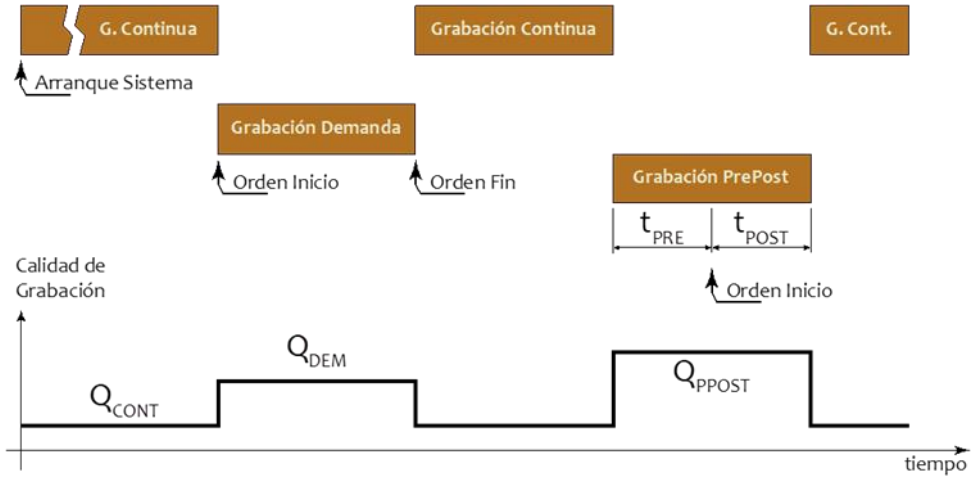

Figura 8. Tipos de grabación, tiempos y calidades asociados, fuente [7]

- Búsqueda de grabaciones, de forma acorde a lo estipulado en el Protocolo Estándar para esta acción, con opción a buscar por cámara y tiempo de inicio y fin de la grabación, en caso de que no se especifique una cámara en concreto la búsqueda deberá devolver todas las grabaciones realizadas entre los dos tiempos especificados. Por último, el conector ordenará los resultados por orden cronológico en sentido ascendente y presentarlos así al cliente.
- Prioridad de las grabaciones, necesaria para distinguir grabaciones que se inician de forma simultánea, la calidad prioritaria en caso de coincidencia es siempre la mayor, como se muestra en la Figura 8, esta se corresponde con las grabaciones pre-post, en caso de que se inicie una grabación bajo demanda mientras se lleva a cabo una pre-post o viceversa, primará esta calidad, si bien se realizarán las dos grabaciones en paralelo.

En caso de que se intente iniciar una grabación bajo demanda cuando ya se está realizando una, el sistema lo notificará al usuario e ignorará la acción.

- Monitores: como ya se ha mencionado, este dispositivo puede ser manejado mediante Conector o directamente a través del descodificador via Protocolo Estándar, en este caso se definen:
  - Codificación de los colores
  - Disposición en layouts, siempre y cuando el descodificador acepte la recepción de múltiples flujos de video y requiera una presentación simultánea de hasta NxM vistas, entendiendo NxM como las dimensiones de una matriz, las vistas se enumeran de izquierda a derecha y de arriba hacia abajo, debiendo asignar un código GUID a cada vista o monitor, añadiendo una numeración (1,2,3…) a un GUID de referencia.

- Recepción multicast, siempre que una cámara esté configurada en este modo, el monitor deberá ser capaz de suscribirse al grupo multicast de emisión mediante protocolo IGMP, en ningún caso será aceptable el establecimiento de comunicación unicast entre cámara y monitor.
- Pérdidas de conexión, al igual que en el resto de casos, será notificada y gestionada por el Conector acorde al Protocolo Estándar.

- Reproductor, en versiones actuales de GSA este Dispositivo de Campo ya no se define, aunque se mantienen el flujo de eventos para realizar una sesión de reproducción via Conector.

4.3.3 Seguridad del sistema CCTV

Como ya se intuye, es necesario evitar el acceso al sistema o a determinados dispositivos del sistema por parte de usuarios no autorizados, dado que la configuración de los componentes dentro del sistema de CCTV recae sobre el Conector, el software de este elemento debe adaptarse al fortalecimiento de la seguridad sin mostrar cambios apreciables para un usuario o cliente GSA.

Generalmente las medidas de seguridad se centran en la autenticación correcta de usuarios via distintos perfiles de usuario y contraseña, para los siguientes casos se establecen medidas más detalladas [7]:

- Cabinas de almacenamiento iSCSI: dos tipos de acceso
  - Acceso al espacio de almacenamiento en lectura y escritura, no controlado por contraseña puesto que perjudicaría la funcionalidad de grabación y reproducción.
  - Acceso a la configuración global de la cabina, controlado por contraseña tanto en la propia cabina como en el gestor de video.
- Cámaras/codificadores: se configuran tres usuarios con contraseñas independientes.
  - Service, permite el acceso a la configuración y al cambio del resto de contraseñas, es el primero en asignarse.
  - User, permite el movimiento PTZ y la activación de salidas, es el segundo en asignarse.
  - Live, permite la visualización de video en vivo, es el último en asignarse.

Las contraseñas para cada usuario se configurarán de acuerdo con la política de seguridad de cada aeropuerto, por otro lado, debe existir un procedimiento en el Conector que se encargue de asignar o actualizar las tres contraseñas, para lo cual será necesaria la contraseña del usuario Service.

Este mismo procedimiento debe encargarse de actualizar la contraseña Service de cada cámara en el Gestor de Video, de tal manera que el sistema siempre tenga acceso a nivel Service de cada una de sus cámaras, para lo cual será necesario disponer de las credenciales a nivel Admin.

Este procedimiento se basará en un fichero de contraseñas limitado adecuadamente por controles de acceso en el servidor del Conector.

- Monitores: funcionan de forma similar a las cámaras o codificadores exceptuando por la no existencia del usuario Live.
- Sistema de Gestión de Video (VRM): Deben tener una contraseña asignada a cada uno de los usuarios preconfigurados y aquellos definidos con posterioridad a la instalación, diferenciados por los privilegios concedidos, siendo los usuarios principales:
    - Admin, grupo de usuarios con todos los privilegios que pueden concederse, incluyendo el de crear nuevos grupos y usuarios, este tipo de usuarios se reservan exclusivamente para tareas administrativas del sistema de CCTV y el Conector estando totalmente prohibido el uso de estos perfiles para comunicarse con el Sistema de Gestión de Video.
    - Administrado, siguiente grupo por privilegios, no pudiendo crear nuevos grupos ni usuarios. El Conector maneja las credenciales de este grupo de usuarios para conectarse con el Sistema de Gestión de Video y para comunicarle al servidor de GSA las credenciales del VRM.
    - Observer, grupo de usuarios que no permite el acceso al Sistema de Gestión de Video para fines relacionados con el Conector.

Al igual que en el resto de casos, las contraseñas se gestionarán mediante un fichero ubicado en los respectivos controles de acceso en el servidor del Conector, nunca en el propio código del Conector.

- Ficheros de contraseñas: estarán ubicados en el disco duro y permitiendo su acceso de lectura y escritura al administrador local de la máquina, no siendo posible acceder a él sin estas credenciales, como ya se ha mencionado contendrán las credenciales de los usuarios mencionados en esta sección.

4.4 Limitaciones del sistema GSA

Una vez descrito el sistema de CCTV en conjunto, es necesario destacar las limitaciones y carencias del mismo, pues son esas limitaciones el principal motivo de la realización de este proyecto, la primera y más importante debido a sus implicaciones es la dependencia casi total de un único fabricante, en este caso Bosch, el cual ha puesto a disposición de Aena los servidores tipo utilizados como Servidores de CCTV o Servidores de transcodificación (ver Figura 6), lo cual limita en gran medida la adaptabilidad de GSA a lo que el fabricante ofrezca y al precio que considere, lo que prácticamente resulta en una situación de monopolio virtual en la que Aena no tiene ningún tipo de libertad de decisión.

Por ello se ha decidido hacer la prospección en el mercado para comprobar la viabilidad de introducir nuevos productos de otros fabricantes, los cuales añadan funcionalidades a GSA y permitan flexibilizar el servicio acorde a las necesidades de cada aeropuerto con una solución más económicamente rentable.

Aparte de la **dependencia casi exclusiva de un solo fabricante** o proveedor, hay que añadir el desfase entre la tecnología utilizada en los servidores y formatos con respecto al actual mercado, de forma generalista se puede estimar en un salto generacional de unos cinco años en el mejor de los casos. Esto viene motivado nuevamente por una razón económica ya que los equipos (no solo los dispositivos periféricos) no son especialmente baratos y requieren de una certificación y puesta en marcha con un coste no solo en dinero sino también en tiempo.

Por otro lado, los distintos formatos tanto de imagen como de compresión en los flujos de video, por ejemplo, GSA utiliza **H.264 como formato de compresión** frente al formato H.265 mucho más eficiente en el uso de ancho de banda y mejora de la calidad de los flujos de video, aprovechando información redundante entre fotogramas.

Sin embargo, el paso de H.264 a H.265 requiere de mucha más potencia de cálculo pues si bien el algoritmo de codificación H.265 optimiza los parámetros de video, requiere de una capacidad de cálculo unas 10 veces superior a su predecesor, con lo cual la utilización de este formato en muchos de los servidores actuales sería contraproducente ya que se ralentizarían los procesos. Por ello es necesario disponer de nuevos sistemas de Gestión de Video ya que esa transición es inevitable.

Por último, y nuevamente relacionado con el desfase generacional de GSA, **el sistema no permite la federación o interconexión de sistemas**, esto es, la gestión remota de un sistema GSA a partir de otro sistema externo, por ejemplo, desde un aeropuerto grande como Madrid-Barajas poder gestionar la videovigilancia de los aeropuertos pequeños de la región como Cuatro Vientos o Torrejón.

Esta posibilidad, muy presente hoy en día en los sistemas de videovigilancia, permiten muchas nuevas funcionalidades, como el **acceso al sistema desde dispositivos móviles** como smartphones, tabletas u ordenadores portátiles simplemente, además del acceso desde otros clientes de un sistema GSA central.

Por supuesto, existen muchas más carencias menores y particulares pues cada aeropuerto es prácticamente un mundo, sin embargo, las aquí citadas son las más importantes y su solución aliviaría mucho tanto la carga de trabajo para los operarios como la flexibilidad y robustez del sistema.

4.5 Requisitos esenciales de GSA

Dado que el objetivo de este proyecto es analizar soluciones de mercado para su posible implementación en el subsistema de CCTV dentro de GSA, es necesario recalcar qué requisitos deben cumplir esas soluciones para efectivamente ser integrados dentro del sistema, esto es, que condiciones te arquitectura, integración con equipos o sistemas de terceros, formatos y protocolos de comunicaciones deben manejar para poder ser aceptados como una solución factible.

Estos requisitos más tarde se conocerán como características esenciales, las cuales servirían para descartar directamente un candidato a producto en el análisis posterior y son los siguientes [7]:

- **Soporte Onvif**: cualquier dispositivo, componente o sistema que se elija como solución debe ser compatible con el perfil de Onvif correspondiente, en este caso se manejarán principalmente dos (con todos los perfiles asociados), el perfil S y el perfil G, tal y como se mencionó en el capítulo 4.3.2.
- **Soporte multicast**: como ya se ha mencionado, en algunas ocasiones las cámaras pueden conmutar a transmisión de datos con metodología multicast para enviar el flujo de video a múltiples destinatarios de forma selectiva, especialmente importante en la sucesión de alarmas, incidentes o eventos. También es importante recalcar que en ningún momento se admitirá conexión unicast de una cámara a un monitor, si bien GSA ya cuenta con mecanismos para impedirlo.
- **Formatos de compresión/codificación de video**: se debe soportar formato de compresión H.264 como mínimo, si bien como ya se mencionado, será preferible y deseable que una solución de mercado admita formato H.265 e incluso H.263, en cualquier caso, cuantos más formatos se soporte, más adaptabilidad ganará el sistema.
- **Integración con terceros**: los sistemas contemplados deben evitar en la medida de lo posible trabajar con formatos, protocolos y comunicaciones propias, ya que esto impediría o dificultaría en exceso el trabajo en el entorno actual de GSA, pues el sistema se sirve de una amalgama de dispositivos de múltiples fabricantes, aunque la arquitectura lógica esté soportada por Bosch principalmente.
- **Actuación ante fallo en los servidores**: en caso de fallo catastrófico o necesidad de desconexión por mantenimiento, el sistema debe soportar cambios o conmutaciones "en caliente". Este requisito cobra especial importancia en los servidores y cabinas de grabación, donde un fallo supondría una pérdida de hasta un 20% de datos de grabación con una configuración RAID 5.
- **Protección de las grabaciones**: como ya se mencionó en el capítulo 4.3.3 las grabaciones deben estar protegidas por distintos perfiles con sus respectivas contraseñas, aunque esto ya está contemplado en los servidores actuales de GSA, las soluciones de mercado deberán cumplir el mismo requisito por su cuenta, aportando nuevas funcionalidades si las hubiera.
- **Exportación de grabaciones**: las soluciones de mercado deberán garantizar la no modificación de los datos exportados, mediante marcas de agua o firmas digitales, soportando además formatos estándar de codificación como JPEG o MPEG, del mismo modo, deberán garantizar la adecuada encriptación de estas para evitar el acceso a las mismas por usuarios no autorizados, en concordancia con lo estipulado en la LOPD.

Adicionalmente, en un análisis posterior derivado de este documento deberán comprobarse los requisitos de compatibilidad con el Conector y la gestión de las visualizaciones mediante el SDK de cada fabricante, este proceso sin embargo, deberá realizarse una vez se haya aceptado como válida una solución de mercado y se disponga de una maqueta.

ESPACIO INTENCIONALMENTE EN BLANCO

5 ANÁLISIS DE PRODUCTOS

El análisis que se ha llevado a cabo como producto final para el proyecto, se ha centrado en intentar identificar las características más propensas a cubrir las carencias descritas en el capítulo 4.4, garantizando de forma simultánea el cumplimiento de los requisitos citados en el capítulo 4.5.

En este capítulo se describe la metodología empleada para clasificarlos, así como los productos que se han seleccionado como posibles candidatos, por último, se recogen las características más favorables de cada uno y las conclusiones extraíbles del desglose y recomendaciones para los futuros trabajos que puedan derivar de este análisis.

5.1 Metodología de análisis

El primer paso, necesario para desglosar las características de cada producto es acotar las variables que se pretende analizar, para ello se han definido dos puntos principales de clasificación, que se detallan a continuación.

- Nivel de importancia: cómo de importante es la característica atendiendo al criterio de cumplimiento o no cumplimiento de los requisitos esenciales y cómo de relacionado esté con una o varias de las carencias principales, se han definido cuatro niveles:
    - **Esencial:** Indispensable para la correcta implementación con GSA, prima el cumplimiento de algún requisito más que la mejora de alguna carencia.
    - **Alto:** Afecta de forma directa a la operativa, su pérdida o degradación afectaría gravemente al sistema, de forma similar al caso anterior, prima el cumplimiento de requisitos que no siendo esenciales pueden comprometer el correcto funcionamiento de GSA.
    - **Medio:** Puede afectar de forma directa a la operativa, sin embargo, su pérdida o degradación no imposibilita el funcionamiento del sistema, engloba a las características de que siendo interesantes como posibles mejoras o complementos, no comprometen el correcto funcionamiento de GSA.
    - **Bajo:** Poco relevante, se incluyen también posibles mejoras misceláneas, engloba a todas las características adicionales, generalmente se reservan para las funcionalidades de usuario como la personalización de la interfaz o el manejo mediante teclado, ratón, joysticks etcétera.
- Categoría: se ha definido este punto de clasificación para separar las características en función del campo al que afecten principalmente, se tiene así:
    - **Almacenamiento:** Incluye todo lo referente a servidores de almacenamiento, archivos, exportaciones, salvado de datos etc.

- **Arquitectura:** Incluye todo lo referente a estructura lógica o física del sistema, conexiones y características generales.
- **Datos:** Incluye todo lo referente a formatos de datos, de exportación, transmisión etc.
- **Dispositivos:** Incluye todo lo referente a características, configuración y gestión de dispositivos en el sistema.
- **Evento/fallo:** Incluye todo lo referente a la gestión de eventos, acciones programadas ante incidentes, alarmas y su gestión etc.
- **Gestión:** Incluye todo lo referente a gestión externa o general del sistema, principalmente gestión de documentos o gestión de datos (de usuario, de licencias etc.).
- **Integración:** Incluye todas las características referentes de forma explícita a la integración de sistemas propios y de terceros.
- **Usuarios:** Incluye todo lo referente a usuarios de forma directa, derechos de usuario, perfiles etc.

Como es lógico, estas categorías son artificiales y no son cerradas, por lo tanto, las características desglosadas se han incluido dentro de alguna de estas categorías a criterio del autor, pudiendo cualquier lector adoptar un criterio distinto en aquellas características que afecten a varios campos del sistema, un ejemplo de ello es la gestión de los sistemas de almacenamiento en arquitecturas federadas.

El segundo paso, es ordenar la clasificación, esta tarea es mucho más sencilla si se realiza a priori, por lo tanto, este paso se ha llevado a cabo diseñando una tabla que permita clasificar de forma visual todas las características desglosadas, para ello se ha recurrido a la herramienta Excel de Microsoft, la cual es muy cómoda además para filtrar datos, lo cual la hace ideal habiendo definido los dos puntos anteriores.

Atendiendo a esto, un esquema de la tabla se muestra a continuación:

Tabla 1. Ejemplo genérico de desglose, fuente propia

NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN de CARACTERÍSTICAS	FABRICANTE/DISPOSITIVO	
			FABRICANTE 1	FABRICANTE 2
			Producto 1	Producto 2
Nivel de importancia C1	Categoría C1	Característica 1 (C1)	Cumpliento particular de C1	Cumpliento particular de C1
Nivel de importancia C2	Categoría C2	Característica 2 (C2)	Cumpliento particular de C2	Cumpliento particular de C2
Nivel de importancia C3	Categoría C3	Característica 3 (C3)	Cumpliento particular de C3	Cumpliento particular de C3

El tercer paso es el de definir una serie de características, correspondiente con la columna “Descripción” de la tabla, lo más genéricas posible para que las casillas de cumplimiento de cada fabricante resulten útiles para la decisión que se pretende tomar que es la de implementar alguno de estos sistemas para mejorar el funcionamiento de GSA.

Ligado a este tercer paso y el que se podría definir como último paso en la metodología posterior al análisis pormenorizado de características a partir de los manuales y hojas de características o *datasheets,* ha sido ajustar la redacción de cada una de las características de cada fabricante para que resulten comparables entre sí, para ello, se ha procurado evitar el uso innecesario de palabras y conectores para facilitar la lectura horizontal de la tabla ya que el número de características desglosadas es considerablemente alto.

Los resultados de este informe, la tabla Excel con el desglose de características se recoge en el ANEXO D de este entregable.

5.2 Productos y fabricantes

En este capítulo se recogen descripciones generales de todos los sistemas. Inicialmente se realizó el desglose para tres productos, dos sistemas de gestión de video, uno de Siemens y otro de Genetec y una cabina de grabación de Dallmeier, de forma adicional se ha incluido otro sistema de gestión de video de la empresa Milestone.

La finalidad de estas descripciones es contextualizar el análisis más allá de GSA de forma que el lector pueda tener una idea general de las características de cada producto sin necesidad de leer toda la tabla de resultados.

A continuación de cada una de las descripciones se recogen las características más destacables atendiendo a las limitaciones y carencias mencionadas en el capítulo 4.4 y los requisitos del capítulo 4.5 los cuales, es posible afirmar que se cumplen en todos los casos con la información disponible.

5.2.1 Siveillance VMS 300 R2, Siemens

Es un sistema diseñado con una filosofía orientada a utilizar estructuras de sistema de gestión centralizada con arquitecturas federadas o interconectadas, ofreciendo acceso y control completo a dispositivos, usuarios y servidores desde cualquier nodo padre o nodo central, las características más destacables en lo referente al objetivo de seguridad son las mejoras en ciberseguridad, mediante el uso de certificados propios o de terceros entre los servidores de gestión y de grabación, el control de cualquier dispositivo mediante bloqueo por contraseña [8].

Ofrece también servicios de analíticas de video aceleradas por hardware, verificación en dos pasos y control de acceso vía aplicación móvil. Permite exportar evidencias (fragmentos de video y audio) de forma inmediata en tres pasos y protegida, desde cualquiera de los clientes, así como enviar estas evidencias a distintos usuarios prioritarios por email o para que accedan desde el cliente web o móvil mediante el servidor móvil.

La filosofía del sistema es aumentar la automatización al máximo posible para facilitar centralización de la gestión por parte de los usuarios, por ello cuenta con un sistema de reglas muy versátil, que permite definir acciones automáticas para prácticamente cualquier campo dentro del sistema, control y movimiento de cámaras, generación, tratamiento y transmisión de mensajes ante eventos o alarmas y definición de perfiles temporales para llevar a cabo acciones automáticas en horarios establecidos.

Por último, cuenta con la capacidad de retransmitir audio y video vivo hacia los clientes móvil y web mediante transcodificación de datos en los propios servidores del sistema y en los dispositivos de recepción.

5.2.1.1 Resultados del análisis

La documentación proporcionada por Siemens es la que se ha utilizado como patrón inicial en las primeras versiones del desglose pues se describe de forma generalista y ya desglosada prácticamente todos los elementos de interés de un sistema de este tipo.

Las características más destacables acorde a las carencias y requisitos presentados, son [8]:

- **Formatos de compresión:** H.264 y H.265.
- **Federación e interconexión:** Estructura orientada a centralización con un nodo central o principal del que dependen todos los nodos secundarios, compatible con todas las subversiones del sistema.
    - Autonomía de los sistemas federados: Se concede autonomía ante fallos en la red que produzcan desconexiones con el nodo principal, guardando para ello configuraciones locales y reglas automáticas configuradas para ello.
    - Acceso a los flujos de video: desde el nodo central, un administrador puede acceder a los datos de grabación o video vivo de las cámaras en sistemas interconectados o federados como si fuera una extensión del nodo central, pudiendo enviar dichos flujos a monitores en el nodo padre.
    - Listado de alarmas/eventos: es común para todos los sistemas interconectados, desde el nodo central se puede acceder a la información (informes, logs, configuracioens, perfiles…) de cualquier nodo secundario, en el caso de las alarmas o eventos, se pueden consultar de forma global y filtrar mediante filtros básicos o personalizados, por ejemplo, fecha/hora, dispositivos implicados, o categoría de alarma.
    - Requisitos adicionales de licencia: ninguno, la licencia para el uso de arquitectura federada es libre y se incluye con la licencia base, en el caso de los dispositivos conectados en nodos federados, el tratamiento es similar a los del nodo central, una licencia por dispositivo conectado al sistema.

- **Cliente web:** disponible para el acceso remoto, pensado para perfiles de administrador o supervisor que necesiten conectarse al sistema sin necesidad de acceder a una consola o cliente local.
    - Adquisición: Incluido con la licencia del servidor móvil.
    - Acceso y puesta en marcha: desde el propio navegador web, no hay requisitos de setup ni instalación de aplicaciones adicionales, el acceso se concede con las mismas credenciales que en el acceso local, aunque pueden aumentarse los filtros de acceso para garantizar que la persona que se conecta es quien dice ser.
    - Funcionalidades disponibles: control PTZ en las tres dimensiones y llamada a preposicionamientos, creación de archivos .AVI o imágenes JPEG (capturas de pantalla), decodificación de video mediante un flujo MJPEG dedicado sin necesidad de plugins adicionales.
    - Exportaciones, creación y edición pudiendo posponer la descarga (se almacena en el servidor) en caso de que se disponga de poco ancho de banda o así se requiera.
    - Protocolo de seguridad de la conexión: HTTPS
    - Audio: Admite transmisión de audio hacia los altavoces desplegados y recepción del mismo por parte de los sensores o comunicaciones dúplex con los operadores, también se concede acceso a las grabaciones disponibles.
    - Vistas compartidas entre usuarios: es posible configurar desde el cliente de gestión una serie de vistas de cámaras o layouts privadas (restringidas) para usuarios particulares y comunes para grupos, por ejemplo, para un conjunto de administradores.
    - Sincronización de eventos: se notifica la sucesión de eventos o alarmas y se siguen las mismas reglas que en los clientes de video locales, pudiendo mostrar una distribución de layouts concreta o el video vivo de la cámara asociada a la alarma o evento.

Todas estas características aplican tanto al nodo principal como a los nodos federados, pudiendo un usuario acceder a estos nodos secundarios con las mismas restricciones que tendría si lo hiciera desde una consola local en el nodo central.

- **Cliente móvil:** sigue la misma filosofía que el cliente web, con la salvedad de que se requiere de una aplicación propia en un dispositivo tipo smartphone o tableta, con sistemas operativos tipo Android 5.0 o superior o iOS 9.3 o superior. Las funcionalidades son básicamente las mismas, a continuación se recogen las más relevantes:
    - Transcodificación de video: se realiza en el servidor móvil convirtiendo los flujos H.264 o H.265 a flujos MJPEG, pudiendo ajustar los parámetros de resolución y ancho de banda para limitar la necesidad de decodificación en el dispositivo móvil.
    - Acceso a los sistemas interconectados: se concede mediante la configuración particular de las credenciales de cada usuario.

- Exportaciones de video: similar al cliente web
- Creación de datos de video: es posible utilizar la cámara del dispositivo móvil como si fuera una cámara más del sistema, pudiendo realizar grabaciones con los metadatos de posición GPS asociados.
- Creación y activación manual de eventos: para marcar fragmentos de video que se consideren relevantes.
- Audio: Se admite transmisión y recepción mediante Video Push, de forma similar al cliente web.
- Acceso a flujos de video: tanto en vivo como grabado, mediante filtros de búsqueda de cámaras o grabaciones, es posible también sincronizar la lista de cámaras asociadas al usuario para facilitar el acceso.
- Imagen en pantalla: es posible utilizar la aplicación móvil en pantalla completa y utilizar la función de zoom digital en las cámaras que dispongan de telemetría.

Como carencia destacable de este sistema se pueden citar las limitaciones en algunas funciones, reservadas solamente para formatos propios como la encriptación de video o la federación con sistemas de gestión de terceros, en cualquier caso, ofrece posibilidades interesantes que deberán ser tenidas en cuenta en la toma de decisiones.

5.2.2 XProtect Corporate, Milestone

Software de gestión de video con una plataforma abierta con hasta 8000 dispositivos diferentes de videovigilancia soportados, servidores nativos de 64 bits, soportando una velocidad de grabación de hasta 3.1 Gb/s. Este producto permite una alta escalabilidad ya que está orientado a estructuras centralizadas con sistemas interconectados a un nodo central, mediante mapas interactivos y menús optimizados de navegación en las interfaces de video, dispositivos, alarmas etc [9].

En lo referente a ciberseguridad, emplea protocolos de encriptación tipo HTPPS para los clientes web y móvil, separando física y lógicamente la red de cámaras de la red de clientes (estaciones de trabajo), también se realiza un control de permisos en los accesos múltiples por parte de los usuarios.

Cuenta con diversas licencias en función del tamaño de la instalación para permitir flexibilidad y libertad de elección al usuario, soportando desde 8 cámaras por servidor de grabación hasta un número ilimitado de dispositivos, en cualquier caso, se dispone de decodificación acelerada por hardware e integración de dispositivos de terceros.

5.2.2.1 Resultados del análisis

Es un sistema con funcionalidades en primera instancia bastante similares a las del Siveillance de Siemens, pues cuenta con una estructura orientada a la federación y centralización jerarquizada, admitiendo una retrocompatibilidad total entre las distintas versiones del software, con cinco en total, Essential, Express, Professional, Expert y Corporate [9].

Nuevamente, la posibilidad de acogerse a estas versiones ofrece flexibilidad a los centros de pequeño y medio tamaño para que puedan federarse a un nodo principal que los gestione de forma remota permitiendo así ahorrar costes a largo plazo y aumentar el nivel de seguridad a medio y largo plazo.

Dado que la información proporcionada por el fabricante estaba orientada a las capacidades y limitaciones del sistema más que a las funcionalidades a nivel usuario, se ha podido extraer información suficiente para completar entorno al 80% del desglose total, por ello al igual que con el producto de Siemens, se recogen de forma resumida las características más destacables.

La principal fortaleza de este sistema es la capacidad de convivir con software de terceros en los servidores, lo que lo hace un muy buen candidato para su integración con GSA pues no hay que olvidar que el objetivo no es sustituir el software actual sino mejorarlo con las capacidades del nuevo.

- **Formatos de compresión:** H.264 y H.265
- **Federación e interconexión:** Jerarquizada de forma piramidal de manera que el acceso se limita desde los nodos con mayor jerarquía a los de menor jerarquía.
    - Autonomía de los sistemas federados: se concede autonomía total pero se deben definir unos supervisores comunes que controlen la actividad dentro de los nodos secundarios.
    - Acceso a los flujos de video: desde el nodo central, un usuario con los permisos adecuados puede acceder a los datos de grabación o video vivo de las cámaras en sistemas interconectados o federados de la jerarquía inferior.
    - Listado de alarmas/eventos: es común para todos los sistemas interconectados, desde el nodo central se puede acceder a la información (informes, logs, configuraciones, perfiles…) de cualquier nodo secundario, en el caso de las alarmas o eventos, se pueden consultar de forma global.
    - Credenciales de acceso: se configuran en los propios nodos federados, para conceder acceso remoto a los usuarios de jerarquías superiores.
    - Requisitos adicionales de licencia: ninguno, la licencia para el uso de arquitectura federada es libre y se incluye con la licencia base, en el caso de los dispositivos conectados en nodos federados, el tratamiento es similar a los del nodo central, una licencia por dispositivo conectado al sistema padre.
- **Cliente web:** disponible para el acceso remoto, mediante un ordenador particular.
    - Acceso: directamente desde el navegador, sin necesidad de plugins o extensiones adicionales, protegido mediante HTTPS.
    - Funcionalidades disponibles: control PTZ, llamada a preposicionamientos y acciones previamente programadas en la cámara, creación de archivos .AVI, imágenes JPEG (capturas de pantalla) o MKV para audio. La decodificación de video está disponible también, aunque no se especifica cómo.

- Exportaciones, creación y edición pudiendo posponer la descarga (se almacena en el servidor) pudiendo previsualizarlas sin necesidad de descargarlas.
- Audio: Admite transmisión de audio de dos vías, tanto para emisión como para recepción.
- Vistas compartidas entre usuarios: los usuarios pueden crear vistas privadas y compartirlas con usuarios con los mismos derechos
- Gestión de eventos: se tiene acceso al listado y búsqueda de alarmas, imagen de la cámara asociada y audio, las capacidades de gestión remota son las mismas que en un cliente local, destacando la posibilidad de modificar la prioridad en las alarmas y realizar escalados y reenvíos de notificaciones a otros usuarios.

- **Cliente móvil:** sigue la misma filosofía que el cliente web, con la salvedad de que se requiere de una aplicación propia en un dispositivo tipo smartphone o tableta, con sistemas operativos tipo Android o iOS. Las funcionalidades son básicamente las mismas, a continuación, se recogen las más relevantes:
  - Acceso a los sistemas interconectados: se concede mediante la configuración particular de las credenciales de cada usuario.
  - Exportaciones de video: se admiten al menos las que ya se hayan creado en el cliente web.
  - Creación de datos de video: es posible utilizar la cámara del dispositivo móvil como si fuera una cámara más del sistema, pudiendo generar metadatos si los derechos de usuario lo permiten.
  - Acceso a flujos de video: tanto en vivo como grabado, esto conllevaría a priori la necesidad de transcodificar video en el servidor móvil, sin embargo, no se especifica explícitamente en la documentación por lo que habrá que esperar a la respuesta de la ROP.
  - Imagen en pantalla: es posible utilizar la aplicación móvil en pantalla completa y utilizar la función de zoom digital en las cámaras que dispongan de telemetría.
  - Gestión de eventos: similar al cliente web.

Aunque se recogen menos características que en el caso de Siemens, en este caso la *Request Of Proposal* no se ha realizado todavía, con lo que no se dispone de información contrastada con el proveedor que permita completar y corregir los campos que faltan.

Por lo tanto, se recalca la necesidad de completar la tabla previamente a la toma de decisiones.

5.2.3 Security Center 5.8 - Omnicast, Genetec

El sistema de Genetec se sirve de una plataforma basada en la gestión mediante una red IP que actúa como nodo central de control de todos los dispositivos y servidores conectados a ella, el sistema Security Center cuenta con varios módulos diferenciados para las dos categorías principales de vigilancia perimetral, el control de accesos y la videovigilancia, el producto de análisis para este proyecto es este último módulo denominado Omnicast [10], [11].

El módulo Omnicast permite configurar todos los parámetros de control de las cámaras conectadas al sistema pues Genetec utiliza plataformas abiertas que tratan de desligar los dispositivos de los fabricantes, contando con más de 240 dispositivos compatibles declarados.

Es compatible con los perfiles S y G de Onvif, admite video vivo con hasta 60 frames por segundo y utiliza formato estándar de video, CIF, QCIF y 4CIF para la visualización y grabación de video procedente de los codificadores. Permite también rastrear individuos u objetos en movimiento de forma automática a través de distintas cámaras gracias a la analítica de video.

En lo referente a ciberseguridad, cuenta con distintas funcionalidades de garantía, certificados y firmas digitales para garantizar a los usuarios que los servidores con los que comunica son auténticos, autenticación de terceros para evitar los inicios de sesión múltiples, autenticaciones basadas en comprobaciones mediante tokens de seguridad para identificar de forma segura a usuarios externos que intenten iniciar sesión en el sistema. Encriptación de principio a fin, para garantizar protección en la transmisión de datos entre aplicaciones cliente, servidores y periféricos.

Por último, cuenta con una función de puntuación de la seguridad que permite a los administradores monitorizar el correcto cumplimiento de cada subsistema con las pautas y reglas definidas, esta función mide y verifica que los procesos de seguridad individuales se llevan a cabo para minimizar así los posibles riesgos en la red.

5.2.3.1 Comentarios post análisis

En el caso del Omnicast de Genetek la información suministrada inicialmente fue la de los manuales de usuario y administrador en los cuales se detallaba la forma de trabajar en las distintas interfaces del sistema, debido a ello, y a la extensión de dichos manuales, la extracción de características para la comparación resultó excesivamente farragosa y en la mayoría de los casos imposible, pues muchas de ellas ni siquiera aparecían explícitamente en los documentos.

Por ello, la columna correspondiente a este producto no debería tenerse en cuenta de momento para realizar la comparación al menos hasta haber recibido la respuesta de la ROP por parte del proveedor.

En cualquier caso, sí se puede destacar la función de analítica de video, máscara de privacidad y seguimiento de personas y objetos de movimiento a través de las distintas cámaras como elementos a tener en cuenta como posibles mejoras para GSA.

5.2.4 Cabina IPS 10000 SMAVIA, Dallmeier

Cabina de grabación que permite grabar simultáneamente hasta 100 flujos de video de alta resolución con una tasa de muestreo de hasta 30 fps, el método de granularidad de los datos es RAID 6. Para instalaciones grandes es posible ampliar la capacidad de almacenamiento con cabinas JBOD también en configuración RAID 6 [12].

Cada cabina dispone de ocho bahías con cerradura para discos duros de 3.5" en su parte frontal, los cuales son utilizados exclusivamente para la grabación de video, el sistema operativo (Linux) y el software Smavia están instalados en un módulo flash separado, admite una capacidad máxima de 72 TB con discos duros de 12 TB.

Se dispone de licencia SeMSy Flat con lo que es posible integrar estas cabinas en un sistema de gestión de video de ese tipo, cada cabina cuenta también con un cliente de video propio para examinar las grabaciones de forma independiente en estaciones de trabajo Windows.

El software SMAVIA cuenta con una función opcional PRemote-HD que permite transcodificar flujos de video en alta resolución tanto para grabaciones como video vivo para la transmisión en redes con bajo ancho de banda de forma independiente de los ajustes de la grabación, se dispone además de una licencia para acceder a la función DMVC Server para acceder de forma remota, con una aplicación móvil al centro de video de Dallmeier.

Las bases de datos permiten analizar en tiempo real los flujos de video de las cámaras IP conectadas, almacenando los eventos, objetos y clases casi en tiempo real, para la evaluación de estos datos se dispone de una función SmartFinder desde el cliente de visualización.

Para la integración con hardware de terceros, el software de los servidores está diseñado como plataforma abierta, mediante la adquisición de licencias adicionales permite grabar cámaras de red de terceros, con detección de movimiento y configurarlas mediante protocolo Onvif.

5.2.4.1 Comentarios post análisis

Como ya se ha mencionado, este producto es una cabina de grabación con un software integrado para la gestión de datos de video, por ese motivo, la información proporcionada por el fabricante estaba orientada a las capacidades de la cabina más que a la del software SMAVIA, que es el que realmente interesa para el objetivo de este proyecto.

Al tratarse de un elemento de hardware más que de software, la información recogida en la documentación proporcionada se centra en las características físicas del producto más que en las capacidades lógicas, por ello se ha definido una categoría propia en el desglose, denominada "Servidores", que recoge estas características.

Como funcionalidad destacable se recoge la capacidad de grabar hasta 100 flujos de video en HD si bien la licencia base solamente ofrece 32 y es necesario adquirir una por cada flujo adicional hasta el máximo. Es muy destacable también la función PRemote que entre otras cosas, permite acceder mediante un cliente móvil a los datos de video para su reproducción con el cliente de video SMAVIA de forma remota y asegurada mediante certificados [12].

6 CONCLUSIONES Y COMENTARIOS FINALES

Dadas las particularidades de este proyecto y la disparidad de la información proporcionada inicialmente por los fabricantes, solamente se ha podido establecer un desglose que resulte útil para dos de los cuatro productos considerados, el de Siemens y el de Milestone, para el primero además se ha completado la información extraída de las hojas de características con la respuesta a la ROP, lo que ha permitido completar tanto las características a tener en cuenta como la columna de este fabricante.

En el caso de Milestone, no se ha llevado a cabo la ROP ya que ha sido el último fabricante en añadirse a la tabla de resultados, sin embargo la información proporcionada por el fabricante estaba centrada en las capacidades del sistema con lo que se ha podido completar la gran mayoría de características tenidas en cuenta, una vez realizada la ROP y obtenida una respuesta, sería una tarea sencilla completar las casillas que faltan y corregir las características que puedan estar mal interpretadas.

En el caso del producto de Genetec es necesario requerir la información correcta pues de los manuales de usuario no se pueden extraer la gran mayoría de características del análisis, en este caso aún no se ha recibido respuesta a la ROP, una vez obtenida se podrá realizar el desglose prácticamente desde el principio y con la garantía de que la información disponible es correcta al haber sido revisada por el proveedor.

En el caso de Dallmeier el problema es similar, ya que la información se centraba en la cabina más que en el software SMAVIA que es el que se podría añadir como complemento de GSA, por lo que una vez obtenida la respuesta a la ROP o si se obtiene una hoja de características de SMAVIA, realizar el desglose para completar la columna correspondiente a este producto, será una tarea sencilla pues la separación por categorías y subcategorías permite realizar una búsqueda directa de las funcionalidades tenidas en cuenta.

Para completar el análisis aquí propuesto, será necesario completar las columnas de estos dos productos teniendo en cuenta ya solamente el tercer paso de la metodología propuesta en el apartado 5.1 de este entregable.

Una vez completado el desglose, la comparación entre sistemas es directa, al menos para los tres sistemas de gestión de video, con lo que, seleccionando un número manejable de características, por ejemplo entre 10 y 15 (de distintas categorías) de las 353 en total, sería posible descartar alguno de los fabricantes y tomar una primera decisión para elegir finalmente a uno de los productos candidatos.

Una vez completado todo ese proceso, el siguiente paso será, como marca la normativa, solicitar una maqueta del producto para poder certificar el sistema en el Centro de Integración de Sistemas y en caso de que se produzca alguna incompatibilidad, se pueda bien llegar a un acuerdo con el fabricante para solucionarlo o bien se recurra a alguno de los otros productos del desglose.

ESPACIO INTENCIONALMENTE EN BLANCO

7 BIBLIOGRAFÍA

[1] D. E. Aviaci and C. Internacional, *Anexo 17 Seguridad*. 2017.

[2] M. De Fomento, "Resolución de 1 de febrero de 2019 , de la Secretaría General de Transporte , por la que se aprueba la actualización de la parte pública del Programa Nacional de Seguridad para la Aviación Civil . TEXTO CONSOLIDADO," pp. 1–97, 2019.

[3] Á. P. Loreiro, "Gestión de Centros Aeroportuarios," pp. 1–132, 2019.

[4] G. MIDAS, "Caso de Estudio 1: análisis de flujos de pasajeros."

[5] D.- GSA, "Manual de formación, Administración Y Configuración," pp. 1–30.

[6] D.- GSA, "Gestión de Seguridad Aeroportuaria Protocolo estándar para CCTV de GSA," 2012.

[7] S. Norma, S. Gsa, A. Aeropuertos, and A. Aeropuertos, "Norma de Equipamiento de Campo del Sistema," pp. 1–94, 2018.

[8] S. S. Ltd, "Siveillance™ VMS 300 2019," pp. 1–24, 2019.

[9] M. & L. Systems and Software, "Especificación XProtect Corporate," pp. 1–59, 2020.

[10] G. Inc, "Guía del Usuario de Security Center 5.8," p. 650, 2019.

[11] G. Inc, "Security Center Administrator Guide 5 . 8 Legal notices," pp. 1–1244, 2019.

[12] D. E. Inc, "SMAVIA, Ips 10 000," pp. 1–7, 2019.

[13] D.- GSA, "2. Especificaciones de Uso 2.1 Acreditaciones Personales," pp. 13–79.

[14] D.- GSA, "Pantallas gestión de visitas, acreditaciones Acceso y Vista Principal."

[15] D.- GSA, "Manual de formación, Rondas."

[16] D.- GSA, "Manual de formación, Centro De Control sinóptico," no. 11, pp. 1–8, 2014.

[17] D.- GSA, "Manual de formación, Editor de Sinóptico."

[18] D.- GSA, "Manual de formación, Centro De Control CCTV," no. 11, pp. 1–8, 2014.

[19] D.- GSA, "Manual de formación, Reproduccion cctv."

ESPACIO INTENCIONALMENTE EN BLANCO

ANEXO A PLAN NACIONAL DE SEGURIDAD, CAPÍTULO 1

En este capítulo se establecen las directrices y medidas generales, necesarias para garantizar un nivel adecuado de seguridad en los recintos aeroportuarios. Se establecen las medidas y requisitos de planificación aeroportuaria, de verificación e identificación del personal de aeropuerto, Compañías Aéreas y Fuerzas y Cuerpos de Seguridad del Estado; las medidas necesarias para establecer y realizar controles de seguridad, revisión de pasajeros y equipajes, y vigilancia perimetral [2].

Se ha decidido citar los fragmentos de interés directamente pues resultan relevantes para entender la motivación del proyecto y el funcionamiento del sistema GSA.

En primer lugar, definición de los elementos básicos de control para garantizar el mínimo nivel de seguridad:

"1.1 Requisitos de Planificación Aeroportuaria.

El diseño, la configuración o remodelación de los aeropuertos, terminales de pasajeros y de carga y otros edificios que tengan acceso directo a la zona de operaciones deberán tener en cuenta, entre otros, los siguientes requisitos:

a) *Controles para acceso de personal.*
b) *Controles de seguridad aplicados a las personas, el equipaje de mano y facturado, la carga y el correo, así como, provisiones y productos de restauración de las compañías aéreas.*
c) *Protección y acceso controlado a las zonas restringidas de seguridad.*
d) *Uso eficaz de los equipos de seguridad."*

- Definición de las distintas zonas en las que se puede dividir un aeropuerto:

"Se deberán crear las siguientes zonas en los aeropuertos:

a) *Lado tierra; la zona de los aeropuertos, terrenos y edificios adyacentes o partes de ellos que no es una zona de operaciones;*
b) *Lado aire o zona de operaciones; la zona de circulación de los aeropuertos, terrenos y edificios adyacentes o partes de ellos en la que está restringido el acceso por motivos de seguridad aeroportuaria.*

b.1) Zonas de acceso controlado.

b.2) Zonas restringidas de seguridad, y

b.3) Zonas críticas de las zonas restringidas de seguridad.

"1.1.1 Límites.

1.1.1.1 Los límites entre el lado tierra, la zona de operaciones, las zonas restringidas de seguridad, las partes críticas y, cuando proceda, las zonas demarcadas, serán claramente reconocibles en todo aeropuerto a fin de facilitar la adopción de las medidas de seguridad oportunas en todas esas zonas.

1.1.1.2 El límite entre el lado tierra y la zona de operaciones constituirá un obstáculo físico claramente visible para el público en general que impida el acceso a personas no autorizadas."

- Medidas mínimas de seguridad en las zonas controladas:

"1.1.1.3 Se establecerán límites entre las distintas zonas de los aeropuertos a fin de facilitar la adopción de las medidas de seguridad oportunas, mediante:

a) Barreras de Seguridad:"

"Las zonas restringidas estarán separadas de las zonas públicas o no restringidas por medio de barreras físicas que deberán someterse periódicamente a inspección.

Dentro de esta categoría se contemplan las persianas o cancelas que comunican los hipódromos con el patio de carrillos, las cuales deberán permanecer cerradas cuando la cinta del hipódromo se encuentre parada. Además, estarán dotadas de un sistema que impida su apertura por persona no autorizada o de un sistema de alarma que detecte su apertura no permitida.

b) Accesos a Zona Restringida de Seguridad:

El número de accesos será siempre el mínimo necesario que garantice la plena eficacia de las operaciones.

c) Carteles:

Se mostrarán carteles anunciadores de zonas restringidas de seguridad en los puntos adecuados del edificio terminal, en todos los accesos y en el vallado perimetral.

1.1.2 Zonas restringidas de seguridad.

1.1.2.1 Las zonas restringidas de seguridad incluirán, al menos:

a) La zona del aeropuerto a la que tengan acceso los pasajeros en espera de embarcar que hayan pasado el control de seguridad,

b) La zona del aeropuerto por la que pueda circular o en la que se pueda guardar el equipaje facturado pendiente de embarque ya inspeccionado, salvo en lo que concierne al equipaje seguro, y

c) La zona del aeropuerto utilizada para el estacionamiento de toda aeronave sujeta a operaciones de carga o embarque."

Las zonas restringidas de seguridad se definirán al menos durante los periodos en los que se realicen cualquiera de las actividades mencionadas en el apartado 1.1.2.1.

"1.1.3 Zonas críticas de las zonas restringidas de seguridad.

1.1.3.1 Se establecerán zonas críticas en los aeropuertos en los que más de 60 miembros del personal esté en posesión de acreditaciones aeroportuarias que permitan el acceso a las zonas restringidas de seguridad.

1.1.3.2 Las zonas críticas de seguridad incluirán, al menos:

a) Todas las zonas del aeropuerto a las que tengan acceso los pasajeros en espera de embarcar que hayan pasado el control, y

b) Todas aquellas zonas de un aeropuerto por las que pueda circular o en las que se pueda guardar el equipaje facturado pendiente de embarque ya controlado, salvo si se trata de equipaje seguro.

Un área del aeropuerto se considerará zona crítica, al menos durante el período en que se estén llevando a cabo las actividades mencionadas en los apartados anteriores.

1.1.3.3 Una vez establecida una zona restringida o crítica de seguridad, se efectuará un registro de seguridad inmediatamente antes del establecimiento de dicha zona de todas aquellas partes que hubiesen podido contaminarse inmediatamente antes del establecimiento de dicha zona, con objeto de cerciorarse de que no existen artículos prohibidos. Esta disposición se considerará cumplida por toda aeronave sometida a un registro de seguridad.

1.1.3.4 Se efectuará rápidamente un registro de seguridad de todas aquellas partes que hubiesen podido contaminarse a fin de garantizar razonablemente que no contienen artículos prohibidos"

"1.2 Control de Acceso.

1.2.1 Acceso a las zonas de operaciones.

1.2.1.1 Sólo se autorizará el acceso a las zonas de operaciones a las personas o vehículos que tengan que acceder por una necesidad justificada. Las visitas guiadas del aeropuerto acompañadas por personas autorizadas se considerarán que tienen una necesidad justificada.

1.2.1.2 Tan solo tendrán acceso a las zonas de operaciones aquellas personas que estén acreditadas.

1.2.1.3 Tan solo tendrán acceso a las zonas de operaciones aquellos vehículos con una autorización válida.

1.2.1.4 Las personas que se encuentren en las zonas de operaciones deberán mostrar, cuando así se les solicite, las acreditaciones pertinentes a efectos de control.

1.2.2 Acceso a zonas restringidas de seguridad.

Se controlará en todo momento el acceso a las zonas restringidas de seguridad para garantizar que no entre en ellas ninguna persona sin autorización, y que no puedan introducirse artículos prohibidos ni en las zonas restringidas de seguridad ni en las aeronaves"

"1.2.2.2 El acceso autorizado a las zonas restringidas se limitará a:

a) Pasajeros provistos de tarjetas de embarque o documento equivalente aceptados para viajes con un transportista aéreo."

Se establecen excepciones para acompañantes de menores de 14 años para acceder a la sala de embarque o de recogida de equipajes en vuelos de llegada, así como para el acompañante (que no vaya a volar) de un pasajero PMR, siempre y cuando dispongan de una tarjeta de acompañante válida.

b) "Personas y vehículos provistos de acreditación y/o autorización aprobada para el acceso a zonas restringidas de seguridad.

También podrá autorizarse el acceso previa identificación positiva mediante la verificación de los datos biométricos.

c) Tripulaciones.

d) Personal con competencias de inspección aeronáutica de aviación civil provisto del correspondiente carné y orden de actuación.

1.2.2.3 Tan solo podrán acceder a las zonas restringidas de seguridad aquellos vehículos con una autorización válida.

1.2.2.4 Se controlará la tarjeta de embarque o equivalente a que se refiere el punto 1.2.2.2, letra a), a fin de garantizar razonablemente su validez, antes de autorizar a su portador el acceso a las zonas restringidas de seguridad.

Se controlarán las tarjetas mencionadas en el punto 1.2.2.2, letras b) a d), a fin de garantizar razonablemente que son válidas y corresponden a quien las porta antes de autorizar el acceso a las zonas restringidas de seguridad.

Cuando se utilice la identificación biométrica, la verificación garantizará que la persona que solicite acceder a las zonas restringidas de seguridad posee una de las acreditaciones indicadas en el punto 1.2.2.2, y que tal acreditación es válida y no ha sido cancelada.

1.2.2.5 Para impedir el acceso sin autorización a las zonas restringidas de seguridad, se instalarán puntos de control en los accesos consistentes en:

a) Un sistema electrónico que restrinja el acceso a una persona cada vez, o

b) Personas autorizadas encargadas de supervisar y efectuar el pertinente control de los accesos.

Las acreditaciones que permiten el acceso a las zonas restringidas de seguridad serán comprobadas electrónica o visualmente para asegurar que son válidas y se corresponden con la identidad del titular.

La restricción de acceso a una persona cada vez no será aplicable en los puntos de acceso utilizados exclusivamente por las Fuerzas y Cuerpos de Seguridad que desarrollen su actividad en el aeropuerto, aunque esto no exime del control de acceso para cada persona.

1.2.2.6 Toda autorización para vehículo se controlará oportunamente antes de permitir el acceso a las zonas restringidas de seguridad a fin de garantizar que es válida y corresponde al vehículo en cuestión."

- Definición de las características de acreditaciones para cada tipo de personal:

"1.2.3 Requisitos aplicables a las acreditaciones del personal del aeropuerto y las tarjetas de identificación de miembros de tripulación de la Unión.

1.2.3.1 Tan solo se podrán expedir tarjetas de identificación como miembros de tripulación empleados en una compañía aérea de la Unión y acreditaciones como personal de aeropuerto a las personas con necesidades operativas que hayan superado una verificación de antecedentes con arreglo al Adjunto H. A partir del 31 de diciembre de 2020 se realizará una verificación de antecedentes reforzada.

1.2.3.2 Las tarjetas de identificación de los miembros de tripulación y las acreditaciones del personal de aeropuerto tendrán una validez no superior a cinco años.

1.2.3.3 La tarjeta de identificación y la acreditación de toda persona que no supere la verificación de antecedentes realizada conforme al Adjunto H será inmediatamente desactivada o retirada, según proceda, y devuelta a la autoridad competente, el gestor o entidad, según corresponda.

1.2.3.4 La tarjeta de identificación y la acreditación deberá llevar la tarjeta de identificación o la acreditación en un lugar visible, al menos mientras el titular se halle en zonas restringidas de seguridad."

"En caso de detectarse alguna irregularidad en la acreditación o en la tarjeta de identificación, se pondrá en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado. El personal de seguridad del aeropuerto deberá retener dicha acreditación de forma preventiva y entregarla a la Oficina de Seguridad."

"1.2.3.5 La tarjeta de identificación o acreditación será devuelta de inmediato a la entidad emisora:

a) Previa solicitud de la autoridad competente, el gestor o la entidad emisora, según corresponda;

b) Por extinción del contrato;

c) Ante un cambio de empleador;

d) Ante un cambio en la necesidad de acceder a zonas para las que se ha concedido la acreditación;

e) Por expiración de la tarjeta; o

f) Por suspensión.

1.2.3.6 La entidad emisora deberá ser informada inmediatamente en caso de pérdida, robo o no devolución de la tarjeta de identificación o acreditación.

1.2.3.7 La tarjeta o acreditación electrónica será desactivada inmediatamente tras su devolución, expiración, suspensión o una vez recibida la notificación de pérdida, robo o no devolución de la misma."

"1.2.4.1 La tarjeta de identificación de los miembros de tripulación empleados en una compañía aérea de la Unión deberá mostrar:

a) El nombre y la fotografía del titular;

b) El nombre de la compañía aérea;

c) El término inglés «crew», y

d) la fecha de expiración.

1.2.5 Requisitos adicionales aplicables a las acreditaciones del personal de aeropuerto.

Las condiciones de concesión de acreditaciones y correcto uso de las mismas se encuentran recogidas en la instrucción SA-7 y son de obligado cumplimiento tanto para la Autoridad aeroportuaria como para el personal que las solicita.

1.2.5.1 La acreditación personal deberá mostrar:

a) Nombre, apellidos, DNI/NIE/pasaporte y fotografía del titular.

En las acreditaciones de los miembros de las Fuerzas y Cuerpos de Seguridad y de los Funcionarios de Aduanas se podrá poner su número de tarjeta de identificación profesional en lugar del nombre y/o DNI.

En las acreditaciones de los vigilantes de seguridad que desarrollen su actividad en el aeropuerto, se podrá sustituir el DNI por el TIP. La oficina local de seguridad pondrá a disposición de las FFCCS del aeropuerto la información que permita vincular el DNI al TIP.

b) Nombre de la empresa, si procede.

c) Nombre del aeropuerto.

d) Las zonas para cuyo acceso se ha autorizado al titular, y

e) La fecha de expiración, salvo haberse programado de forma electrónica.

Las acreditaciones permitirán el acceso del personal sólo a las áreas designadas por las necesidades operativas.

1.2.5.2 A fin de evitar toda utilización indebida de las tarjetas de identificación de personal de aeropuerto, se activará un sistema que garantice razonablemente la detección de todo intento de utilización de tarjetas perdidas, robadas o no devueltas. Se adoptarán las medidas oportunas apenas se detecte un intento de uso indebido.

1.2.6 Requisitos aplicables a las autorizaciones de vehículos.

a) La autorización es exclusiva para el acceso y permanencia en la zona de seguridad en que la empresa para la que presta el servicio desarrolla su actividad, estando prohibido el acceso y permanencia en zonas distintas de las autorizadas.

b) La autorización se asignará a cada vehículo en concreto, irá colocado en un lugar que sea fácilmente visible de su parte frontal e indicará:

- *Las zonas a cuyo acceso se haya autorizado, y*
- *La fecha de caducidad.*

c) Toda autorización electrónica para vehículos deberá:

- Colocarse en el vehículo de forma que quede garantizada su intransferibilidad; o
- Estar vinculada a la empresa usuaria o al usuario del vehículo registrado a través de una base de datos de registro de vehículos segura.

La autorización electrónica para vehículos no es necesario que muestre las zonas a las que tiene acceso el vehículo en cuestión ni la fecha de caducidad, siempre que esta información sea legible en formato electrónico y se controle antes de autorizar el acceso a las zonas restringidas de seguridad. Las autorizaciones electrónicas para vehículos también deberán ser legibles electrónicamente en la zona de operaciones.

d) La autorización para vehículos deberá exhibirse en un lugar suficientemente visible cuando el vehículo circule por las zonas de operaciones.

e) Dicha autorización deberá ser devuelta de inmediato a la entidad emisora:

- *A instancia de la propia entidad emisora;*
- *Cuando deje de utilizarse el vehículo para acceder a las zonas de operaciones, o*
- *Cuando expire dicha autorización, salvo que esta quede invalidada de forma automática.*

f) La entidad emisora deberá ser informada inmediatamente en caso de pérdida, robo o no devolución de una autorización para vehículos.

g) La autorización electrónica será inmediatamente desactivada tras su devolución, expiración o una vez recibida la notificación de pérdida, robo o no devolución de la misma.

h) A fin de evitar toda utilización indebida de las autorizaciones para vehículos, se activará un sistema que garantice razonablemente la detección de todo intento de utilización de autorizaciones perdidas, robadas o no devueltas. Se adoptarán las medidas oportunas apenas se detecte un intento de uso indebido.

i) Los vehículos que se utilicen exclusivamente en las zonas de operaciones y no dispongan de permiso para circular por vías públicas estarán exentos de llevar la autorización visible a condición de que estén claramente identificados en el exterior como vehículos operativos para uso en dicho aeropuerto (vehículos sin matrícula).

1.2.7 Acceso con acompañante autorizado.

1.2.7.1 El personal de compañías aéreas perteneciente a las categorías de tripulación que no tenga acreditación aeroportuaria deberá ser acompañado por un acompañante autorizado siempre que se encuentre en zona restringida de seguridad y no esté en:

a) Áreas donde los pasajeros pueden estar presentes,

b) Áreas inmediatamente próximas a la aeronave en la cual acaban de llegar o van a salir,

c) Áreas designadas para tripulaciones, y

d) *Recorrido entre el terminal o punto de acceso y la aeronave en la que los miembros de la tripulación hayan llegado o vayan a salir."*

"1.2.7.3 Las personas que vayan constantemente acompañadas mientras se encuentren en zonas restringidas de seguridad llevarán una acreditación acorde a lo establecido en el presente capítulo.

Los acompañantes deberán:

a) *Disponer de una acreditación aeroportuaria, definitiva o provisional, válida,*

b) *Estar autorizados por la Autoridad aeroportuaria para las funciones de acompañante en las zonas restringidas de seguridad,*

c) *Acompañar en todo momento y sin perder de vista a la persona o personas que acompaña, y*

d) *Garantizar razonablemente el cumplimiento de las medidas de seguridad por parte de la persona acompañada."*

"1.2.9 Otros accesos situados en zona restringida de seguridad.

Las compañías aéreas y/o los agentes de asistencia en tierra que las representan en el aeropuerto garantizarán que:

a) *Las puertas de acceso que conducen a las pasarelas, al lado aire y a las rampas estén cerradas y aseguradas cuando no se estén utilizando, teniendo en cuenta las correspondientes normas de emergencia, evacuación y seguridad.*

b) *Las puertas de acceso utilizadas únicamente para el desembarque, que permitan acceso a rampas o zonas restringidas de seguridad, permanecerán abiertas solo durante este proceso.*

1.3 Inspección de personas que no sean pasajeros y de los objetos transportados.

1.3.1 Inspección de personas que no sean pasajeros y de los objetos transportados.

1.3.1.1 Las personas que no sean pasajeros serán inspeccionadas por uno de los siguientes medios:

a) *Inspección manual;*

b) *Arco detector de metales (WTMD);*

c) *Perros detectores de explosivos (EDD);*

d) *Equipo de detección de trazas de explosivos (ETD);*

e) *Escáner de seguridad que no utilice radiaciones ionizantes;*

f) *Equipo de detección de trazas de explosivos (ETD) combinado con un detector de metales portátil (HHMD);*

g) *Equipos de detección de metales para calzado (SMD);*

h) *Equipos de detección de explosivos para calzado (SED)."*

Estos medios se aplicarán en los controles de seguridad correspondientes en salidas o en las aduanas en llegadas o transferencias.

"1.4 Registro de los vehículos.

Se examinará a los vehículos antes de autorizar su acceso a las zonas restringidas de seguridad.

1.4.1 Vehículos que accedan a zonas críticas.

1.4.1.1 Se examinará el 100% de los vehículos que accedan a zona crítica de seguridad.

Una vez finalizada la inspección, deberá protegerse de toda interferencia ilícita hasta acceder a las zonas críticas."

"1.4.3 Métodos de inspección.

1.4.3.1 El registro manual tendrá por objeto efectuar un control manual de las zonas y áreas seleccionadas, incluido su contenido, para garantizar suficientemente que no haya en ellas artículos prohibidos."

"1.5 Seguridad Física y Patrullas.

1.5.1 Con el fin de detectar comportamientos sospechosos, descubrir puntos vulnerables que puedan ser aprovechados para cometer actos de interferencia ilícita y disuadir a las personas de cometerlos, se efectuarán servicios de vigilancia y patrullas con objeto de controlar:

- *Los límites entre el lado tierra (incluyendo el vallado perimetral), la zona de operaciones, las zonas restringidas de seguridad, las zonas críticas de seguridad, y, cuando proceda, las zonas demarcadas;*
- *Las áreas del terminal y adyacentes de acceso público, incluido el parking y las vías de acceso;*
- *Mediante controles aleatorios, que toda persona lleva su acreditación visible en las zonas restringidas de seguridad en las que no haya pasajeros presentes y la validez de las mismas;*
- *Que las autorizaciones de vehículos se llevan en un lugar visible en las zonas de operaciones, y la validez de las mismas, y*
- *El equipaje facturado, la carga, el correo, las provisiones de a bordo y el correo y material de la compañía aérea en espera de embarque en las zonas críticas de seguridad.*

1.5.2 Los servicios de vigilancia y patrulla se efectuarán en virtud de un análisis de riesgos."

"1.7 Requisitos para el vallado perimetral.

Para la protección perimetral de la zona de operaciones, se deberá disponer de un cerramiento de seguridad de altura y consistencia suficientes para evitar los accesos no autorizados. Los requisitos del vallado perimetral se regirán por disposiciones adicionales de carácter restringido aprobadas por la Autoridad competente."

ANEXO B ANEXO 17 OACI, CAPÍTULO 4

En este capítulo se recogen las medidas generales propuestas por OACI a partir de las cuales se sientan las bases para desarrollar los planes de seguridad de cada uno de los Estados contratantes [1].

- **Medidas relativas al control de acceso:** Cada Estado debe asegurar el control del acceso al lado aire de los aeropuertos de personas no autorizadas, para ello se deben definir zonas de seguridad restringidas basándose en la evaluación de riesgos que realicen las autoridades nacionales competentes.

Del mismo modo, cada Estado debe asegurar el establecimiento de medidas de identificación de personas y vehículos para evitar el acceso no autorizado al lado aire o zonas restringidas, para ello se deben definir puntos de inspección en los accesos a estas zonas.

Se debe también realizar una comprobación de antecedentes de las personas que no sean pasajeros, así como de cualquier pertenencia que puedan llevar consigo antes de acceder a una zona restringida. Relacionado con esto, los documentos de identidad de las tripulaciones deben seguir un formato internacional para facilitar el paso por los controles de seguridad.

Por último, se establece la necesidad de realizar la supervisión de la circulación de personas y vehículos hacia y desde las zonas restringidas de los aeropuertos debiendo inspeccionar los artículos contenidos en estos últimos.

- **Medidas relativas a los pasajeros y a su equipaje de mano:** Cada Estado debe establecer medidas para asegurar que se inspeccione a los pasajeros en origen de las operaciones, así como su equipaje de mano antes de embarcar en una aeronave que salga de una zona de seguridad restringida.

Del mismo modo, cada Estado debe asegurar que los pasajeros ya inspeccionados estén protegidos contra interferencias no autorizadas desde el punto de inspección hasta su embarque en la aeronave correspondiente, debiendo repetir el control si estos pasajeros o su equipaje de mano se mezclan o entran en contacto con otros.

Queda a criterio de cada Estado el establecimiento de las medidas de protección contra interferencia ilícita de pasajeros y su equipaje, es posible también que en caso de que se produzca un transbordo, dos Estados establezcan acuerdos para establecer procesos de validación y procedimientos permanentes para garantizar la inspección en origen y la protección en tránsito hasta el embarque en la aeronave de salida en el aeropuerto de transbordo.

- **Medidas relativas al equipaje de bodega:** Al igual que con el equipaje de mano, cada Estado debe adoptar medidas para la inspección antes del embarque y la protección ante interferencias ilícitas desde el punto en que se inspeccione o el transportista acepte su custodia, lo que suceda antes, debiendo repetir la inspección en caso de que se comprometa la integridad del equipaje.

Es posible también, establecer acuerdos bilaterales que armonicen las inspecciones para equipajes en transbordo garantizando la protección durante todo el trayecto.

Cada Estado debe asegurar que los explotadores del transporte aéreo, transporten únicamente artículos del equipaje de bodega identificados individualmente como equipaje acompañado o no acompañado inspeccionados y cuyo transporte haya sido aceptado por el transportista aéreo, debiendo dejar constancia del cumplimiento de dichos criterios.

- **Medidas relativas a la carga, el correo y otros artículos:** Cada Estado debe establecer controles de seguridad apropiados siempre que sea factible en origen, antes de embarcarlos en una aeronave, así como un proceso de seguridad en la cadena de suministro incluyendo la aprobación de agentes acreditados o expedidores reconocidos si estos participan en la aplicación de inspecciones o controles de seguridad.

Se deben establecer medidas particulares específicas para correo y carga de alto riesgo para evitar las amenazas conexas, así como para las piezas de repuesto y aprovisionamientos.

Cada Estado debe asegurar que los explotadores no acepten transportar carga o correo en una aeronave a menos que un agente acreditado o una entidad aprobada por la autoridad competente confirme y demuestre la aplicación de las medidas de inspección o controles de seguridad.

Al igual que para el resto de cargas, cada Estado debe asegurar que la carga y el correo disponen de un estatus de seguridad en formato electrónico o por escrito a lo largo de toda la cadena de suministro segura.

- **Medidas relativas a categorías especiales de pasajeros:** Cada Estado, debe definir requisitos para los transportistas aéreos, relativos al transporte de pasajeros que viajen bajo coacción por haber sido sometidos a procedimientos judiciales o administrativos, ante las posibles perturbaciones que puedan ocasionar. Del mismo modo, se deberá garantizar el establecimiento de medidas y procedimientos específicos para estos pasajeros en los programas de seguridad.

Cada Estado debe asegurar que tanto explotadores como pilotos estén informados de la presencia de estos pasajeros para que se apliquen los controles de seguridad apropiados, pudiendo ser necesario que agentes de mantenimiento del orden público u otras personas autorizadas porten armas a bordo o acompañen a estos pasajeros en el trayecto.

En el caso de porte armas a bordo, se deberá asegurar que están descargadas y, aun así, que se colocan en un lugar inaccesible a cualquier persona durante el tiempo de vuelo. Del mismo modo, en caso de que un Estado emplee oficiales de seguridad a bordo, éstos deberán ser funcionarios gubernamentales especialmente seleccionados y entrenados

- **Medidas relativas a la parte pública:** Cada Estado deberá identificar las áreas definidas como parte pública, debiendo establecer las medidas de seguridad apropiadas para mitigar el riesgo de posibles actos de interferencia ilícita, coordinando estas medidas entre los distintos departamentos, agencias y otros órganos del Estado y demás entidades intervinientes.
- **Medidas relativas al ciberterrorismo:** Se establecen una serie de recomendaciones para que cada Estado se asegure y en la medida de lo posible establezca medidas para proteger la confidencialidad, integridad y disponibilidad de sistemas críticos de tecnología de la información y comunicaciones y de los datos críticos para fines de la aviación civil

En el capítulo final de este Anexo y en sus adjuntos se establecen los distintos criterios para la aplicación de medidas de actuación ante interferencias ilícitas y los procesos de notificación en todos los casos.

ANEXO C INTERFACES DE GSA

En este capítulo se recogen los detalles de las interfaces presentadas en la Figura 4 del capítulo 4.1.

C.1. Configuración de tarjetas de acceso (acreditaciones)

Desde esta aplicación se configuran todas las tarjetas de acceso o acreditaciones que el sistema reconocerá como válidas para que bien los vigilantes o bien los controles de acceso automáticos, puedan reconocer a la persona o vehículo que porta una acreditación siempre que esté en vigor y tenga los permisos de acceso adecuados [13].

Se distinguen principalmente tres tipos de acreditaciones:

- Acreditaciones personales: Conceden unas credenciales de acceso a una persona en concreto durante un tiempo prolongado, entendiendo como prolongado, un tiempo superior a una semana e inferior a tres años, en el caso de que la vigencia sea inferior a seis meses, la acreditación se considerará provisional y se distinguirá por la presencia de una letra “P” sobre la misma.
- Acreditaciones de visitante: Conceden unas credenciales de acceso a una persona o grupo de personas con una vigencia entre un día y una semana, el personal con este tipo de acreditaciones necesita de una acompañante con una acreditación personal de la cual además heredarán los derechos de acceso, el sistema limita la renovación de una misma tarjeta de visita a 8 veces en un año.
- Acreditaciones de vehículos: Conceden unas credenciales de acceso a un vehículo teniendo en cuenta su matrícula y conductor principalmente. Nuevamente, los controles automáticos de acceso (lectores de matrícula en este caso) deberán reconocer la matrícula dentro de su base de datos, en el caso de acceso con vigilante habría que comprobar además la acreditación del conductor.

La ventana principal de este módulo se muestra en la Figura 9. Esta pantalla corresponde con el primer tipo de tarjetas, acreditaciones personales, en los cuadros de texto se pueden introducir todos los datos de la persona acreditada, incluyendo la pertenencia a las FCSE, la fecha de caducidad, empresa o grupo de empresas a las que pertenece, los permisos de acceso concedidos (que limitan el acceso a franjas horarias determinadas) y las zonas a las que se conceden estos permisos incluyendo por supuesto el aeropuerto donde aplican estas credenciales.

Todos los datos directamente relacionados con los permisos y la vigencia se plasman sobre la tarjeta en una vista previa siguiendo unos modelos definidos en el menú Administración y Configuración (Anexo C.8.)

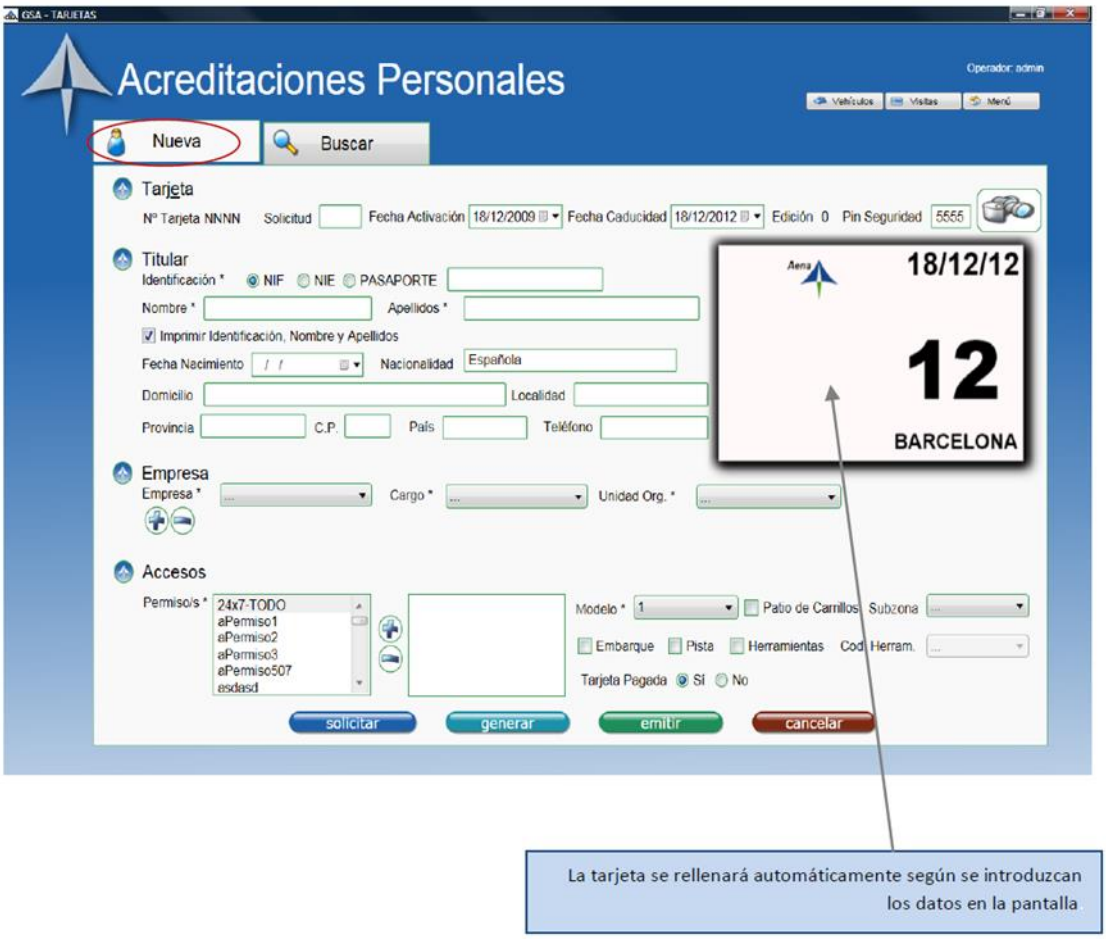

Figura 9. Pantalla principal menú Tarjetas de Acceso (Acreditaciones), fuente [13]

En la parte inferior de la ventana, se aprecian cuatro cuadros de texto que permiten llevar a cabo distintas acciones, empezando por la izquierda:

- Solicitar: Una vez cumplimentados todos los datos de la persona, la empresa, permisos, zonas y vigencia, permite emitir una solicitud de acreditación. Esta solicitud queda pendiente de su aprobación o rechazo por un usuario con permiso para llevar a cabo esta acción. En cuanto a la fecha de vigencia, se tomará como día de inicio el momento de su activación una vez se confirme la solicitud.
- Generar: Permite generar directamente una acreditación en el sistema sin necesidad de que un administrador verifique la solicitud, los pasos para ello son los mismos que en el caso anterior. Una vez generada la tarjeta, esta se queda en estado “no emitida”. Es posible definir una lista negra, si se intenta generar una acreditación para una persona incluida en esta lista, el sistema enviará un aviso al operario denegando la acción y le permitirá continuar con la generación.

- Emitir: Permite emitir (imprimir) y validar directamente una acreditación, lo habitual y recomendable es elegir una tarjeta generada o la solicitud de una mediante el buscador del módulo, el cual permite filtrar por nombre de la personal, fecha de la solicitud o generación y el resto de los campos mostrados en la Figura 9. En cualquier caso, se puede realizar la acción desde cero cumplimentando manualmente los campos y emitiendo la acreditación, una vez seleccionada esta opción se abrirá un cuadro de diálogo con las impresoras disponibles para llevar a cabo la impresión, una vez seleccionada la acreditación pasará a estar en estado "emitida" y a todos los efectos será funcional con las características con las que haya sido configurada.

En cuanto al número de acreditación, es un número único que permite distinguir unas de otras incluso cuando se hayan renovado, este número se concede a las tarjetas una vez se haya llevado a cabo al menos una de las acciones anteriores, durante la introducción de datos este número no se encuentra disponible.

Como ya se ha mencionado, una acreditación no solo sirve para el reconocimiento visual del acreditado, sino también para conceder acceso mediante controladores automáticos generalmente acoplados a interfonos, estos controladores tienen principalmente tres métodos de verificación:

- Código pin: código numérico asociado a la tarjeta de longitud variable, aunque habitualmente contiene entre 4 y 6 caracteres, se introduce mediante un panel acoplado al lector.
- Lectura de banda magnética: mediante un sensor adecuado acoplado al controlador.
- Lectura de proximidad: mediante un sensor de proximidad acoplado al controlador.

Para garantizar la seguridad y el buen uso de las acreditaciones, la lectura de sensor, bien por banda o bien por proximidad, deberá complementarse siempre con la introducción del código pin de la tarjeta para así inutilizar los robos o las suplantaciones.

Puesto que es habitual que las tarjetas sufran perturbaciones y puedan desmagnetizarse o perder la calibración, es posible realizar recalibraciones de las tarjetas en el propio sistema, esta opción se activa en la misma ventana de Tarjetas para las acreditaciones emitidas y en vigor y solamente deberá ser llevada a cabo por un operario autorizado.

Por último, con el fin de aumentar la seguridad asociada a las acreditaciones, se está estudiando la implementación de métodos de verificación que incluyan lecturas biométricas de la persona acreditada, principalmente lectura de huella dactilar y reconocimiento facial, aunque estos métodos aún no están certificados por Aena y no están en funcionamiento actualmente.

En la Figura 10 se muestra un ejemplo de cómo quedaría una acreditación siguiendo el modelo definido en el PNS para una persona autorizada para acceder con herramientas a las zonas públicas y lado aire del aeropuerto excluyendo el área de maniobras y concretamente a la central eléctrica.

Figura 10. Ejemplo de acreditación personal definitiva, fuente [13]

C.2. Gestión de visitas

La ventana de este submenú se muestra en la Figura 11, como puede comprobarse, los datos a cumplimentar son mucho menores en comparación a una acreditación personal al uso pues este tipo de acreditaciones están pensadas para tener una vigencia mucho menor y en general para no ser renovadas [14].

De este menú es necesario destacar que la visita para la que se genera la acreditación debe tener asociada tanto una persona a la que va dirigida la visita como una persona acreditada que acompañe a esta visita, es decir, las visitas de ocio no están contempladas y deben estar controladas en todo momento para no vulnerar los niveles de seguridad y desfavorecer malos usos de las acreditaciones personales.

Tanto este menú como el de acreditaciones de vehículos son accesibles desde el menú de Tarjetas mostrado en el capítulo anterior, por lo que se está planteando suprimir estos dos iconos en versiones posteriores del software de GSA para así simplificar la interfaz general, limitando su acceso y configuración al menú de Tarjetas.

Cabe resaltar que este tipo de acreditaciones sí puede renovarse, sin embargo el sistema lo limita a 10 renovaciones en un periodo de tres meses.

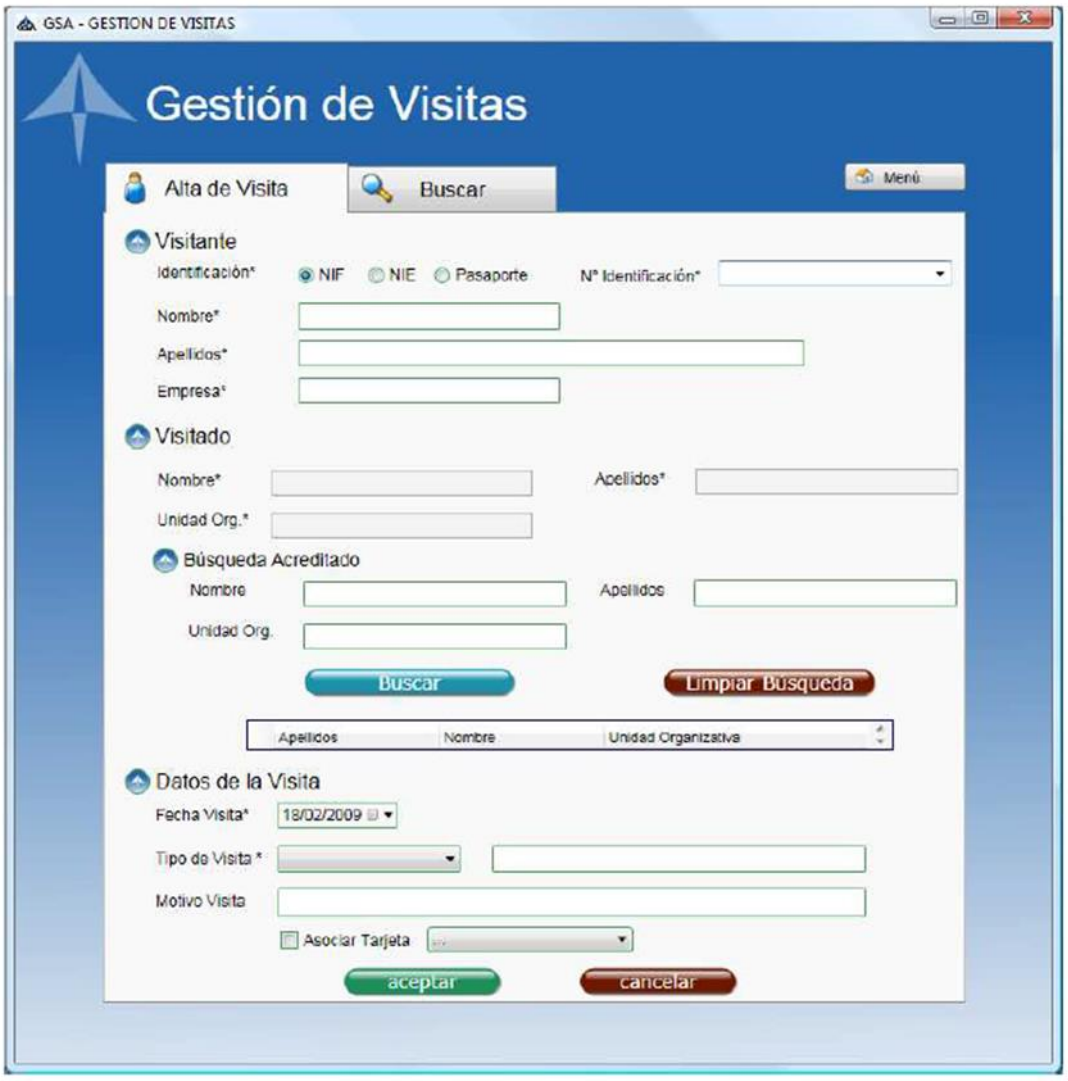

Figura 11. Pantalla principal menú Gestión de visitas, fuente [14]

C.3. Rondas

En este menú es posible inicializar las rondas de patrulla que deberá completar un vigilante, para caracterizar una ronda es necesario especificar cuatro campos como mínimo [15]:

- Nombre y descripción de la ronda: Simplemente para poder ser identificada de forma rápida y sencilla por cualquier operador.
- Acreditación: al igual que con los visitantes, es necesario asignar una ronda a una acreditación personal concreta para que así el sistema pueda confirmar en base de datos que la persona realizando la ronda es la correcta.

- Puntos de control: son los puntos de definen físicamente a la ronda, están ordenados y todos ellos deberán ser recorridos por el vigilante para considerar que la ronda se ha completado de forma exitosa.
- Tiempo de paso: asociados a los puntos de control, se define como el tiempo máximo que se le concede al vigilante para llegar de un punto de control al siguiente, si el tiempo real excede el tiempo de paso el sistema lo notificará con un icono con una cruz roja y un cuadro de texto en la columna observaciones.

Con todos estos elementos se asegura que tanto el sistema GSA como la persona que monitoriza las patrullas monitorizan todo lo que sucede durante las rondas ya que gracias a los puntos de control es mucho más sencillo hacer un seguimiento del personal de seguridad con las cámaras desplegadas y sobre el mapa virtual.

En la Figura 12 se muestra un ejemplo de ronda completada con cuatro puntos de control.

Figura 12. Menú sección Rondas, ronda completada, fuente [15]

C.4. Centro de control sinóptico

Este menú permite acceder al mapa virtual de la zona de control, sobre este mapa virtual se despliegan iconos correspondientes a los distintos dispositivos de campo, sensores y puertas automáticas (corredores) que estén registrados y funcionando en el sistema [16].

El mapa que simula la zona de control debe estar en un formato de imagen típico (PNG o JPEG) y actúa sencillamente como un fondo, los dispositivos se agrupan en distintas categorías con un icono asociado:

- Lector de acceso: Controlador asociado a una puerta con cierre electrónico que notifica y/o permite el intento de acceso con una acreditación personal, pueden configurarse para que los accesos se realicen de forma individual con un proceso de lectura, apertura y cierre o aceptar lecturas adicionales entre apertura y cierre para conceder acceso a múltiples personas (con su acreditación correspondiente) de forma continuada.

- Lector de embarque o facturación: Controladores conectados a los correspondientes puestos de embarque o facturación que manejan las compañías, en el caso de Aena previo acceso y validación de la facturación o embarque desde los servidores UCA, si están desactivados, apagados o en estado de alarma no permitirán realizar ninguna de las dos funciones.
- Sensor: Categoría generalista que agrupa cualquier tipo de sensor que sirva como señal de control para activar una alarma o notificar de un evento, por ejemplo, un sensor de movimiento (volumétrico) sensor térmico, micrófonos etc. Que permitan detectar accesos no autorizados o vulneraciones del perímetro del aeropuerto.
- Corredor: Se definen como corredores a los pasillos con puertas automáticas asociadas que actúan como filtro de acceso del lado aire al lado tierra del aeropuerto, o viceversa. En definitiva son los accesos físicos que separan la zona pública de la zona restringida, es importante que estos accesos solamente permitan el flujo de personas en un solo sentido, de ahí que se definan en una categoría propia.
- Interfono: Categoría que incluye a los elementos periféricos de interfonía, aunque generalmente se encuentran combinados con un lector de acceso se definen en categorías diferentes ya que sus funciones están bien diferenciadas, permiten recibir o realizar llamadas hacia y desde el dispositivo.
- Actuador: Categoría generalista que incluye a los dispositivos de actuación ante eventos (de activación manual o automática), por ejemplo, un flash que actúe como fogonazo ante la apertura forzada de una puerta, una alarma visual y/o sonora etc.
- Cámaras: Categoría que define a todas las cámaras de videovigilancia, excluyendo los lectores de matrícula o las cámaras de biometría, desde este menú solamente es posible previsualizar las cámaras, para realizar más acciones es necesario cambiar al submenú Centro de control CCTV, en el Anexo C.6.

Un ejemplo de mapa sinóptico se muestra en la Figura 13.

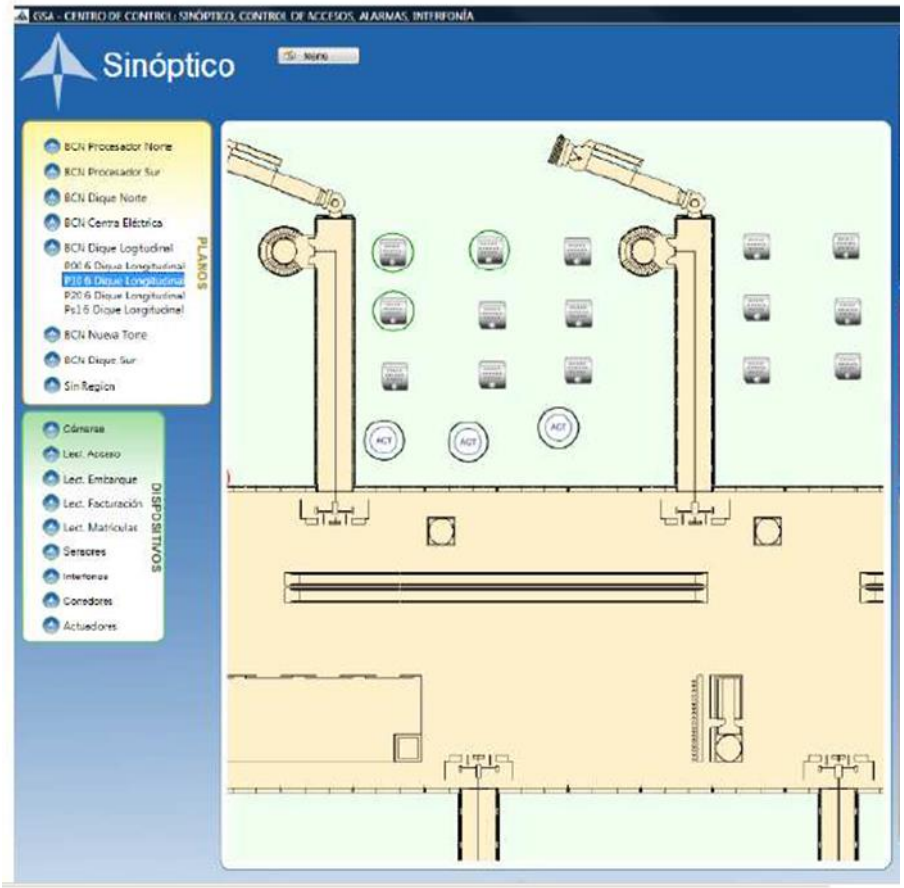

Figura 13. Ejemplo de mapa de control, menú sinóptico, fuente [16]

Rodeando a cualquiera de los iconos de dispositivo se incluye un contorno con código de color que permite identificar de forma visual distintas situaciones habituales en los dispositivos, como se muestra de forma más detallada en la Figura 14.

Figura 14. Leyenda de contornos sobre dispositivos, fuente [16]

Estos estados se definen de la siguiente manera [16]:

- Alarma: Se ha disparado una alarma en un dispositivo, por ejemplo, ante una detección de movimiento, repetidos intentos de acceso fallidos, identificación de sujetos sospechosos etc. Ante esta acción un operario puede notificar al sistema un "enterado" sin necesidad de rearmar (reiniciar) la alarma en caso de que así se decida.
- Sabotaje: Se ha abierto la cubierta del dispositivo de forma no autorizada, es decir, la carcasa del dispositivo ha sido o ha intentado ser retirada. Al igual que con las alarmas un operario puede notificar un "enterado" o no.
- Fallo de conexión: El tiempo de respuesta del dispositivo ha superado el tiempo de *keep alive* (ver capítulos 4.2 y 4.3.2) y el sistema no ha podido establecer una conexión con el dispositivo, esto no significa que el dispositivo en cuestión se encuentre apagado, este estatus puede deberse a fallos en la red o a sabotajes externos, de ahí la necesidad de diferenciarlo de otro tipo de fallos.
- Deshabilitado: el dispositivo se encuentra apagado.
- Fallo técnico: la controladora del dispositivo ha detectado un error en el funcionamiento de este y lo ha notificado al sistema, necesario para ejercer maniobras de mantenimiento conociendo el origen del fallo.
- Reposo: el dispositivo no se encuentra en ninguno de los otros estados.

Adicionalmente para interfonos y lectores de embarque o facturación se define un estado asociado a un contorno de color verde que indica que el dispositivo está llevando a cabo una acción continuada, en el caso de estas categorías, indicaría que se están llevando a cabo una llamada o acciones de facturación o embarque.

Por último, en la pantalla principal de este menú, se presentan también una serie de cuadros de texto que recopilan la información detectada para, estados de alarma en un dispositivo, llamadas realizadas en un interfono y accesos e intentos de acceso en un lector, como se muestra en la Figura 15.

En estas tablas de notificación se mostrarán todas las acciones registradas por los distintos sensores a los que van referidas, del mismo modo que con los iconos, los operarios podrán llevar a cabo acciones sobre los dispositivos mediante un submenú al que se accede con el click derecho del ratón.

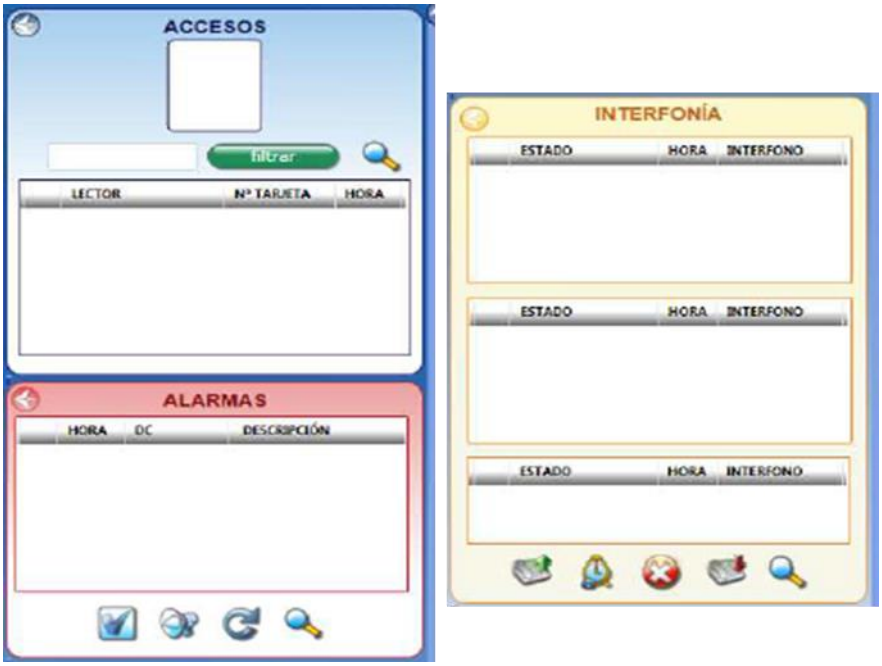

Figura 15. Tabla de notificaciones del sinóptico, fuente [16]

C.5. Editor de sinóptico

Este menú permite editar los mapas y elementos que se colocarán sobre estos, distribuir manualmente los dispositivos atendiendo a su distribución física real, crear zonas y subzonas que permitan transicionar entre mapas y modificar o eliminar dispositivos desplegados. En la Figura 16 se muestra un ejemplo de dos tipos de regiones básicas, una región rectangular (geométrica) que con un código de color definido permita diferenciar la importancia de unas zonas frente a otras, y una región tipo botón que permite transicionar entre zonas, por ejemplo, entre plantas de una terminal o entre mapas de zonas internas del aeropuerto [17].

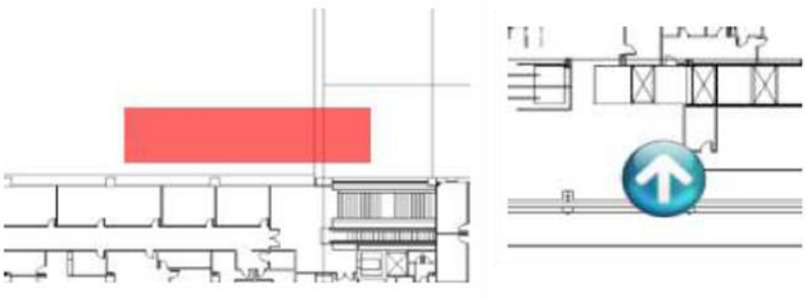

Figura 16. Ejemplo de regiones sobre un mapa, región geométrica y región botón, fuente [17]

C.6. Centro de control CCTV

Este menú permite controlar la visualización de las cámaras y la conmutación de una vista de cámara a un monitor (pantalla) físico, la pantalla principal de esta aplicación se muestra en la Figura 17:

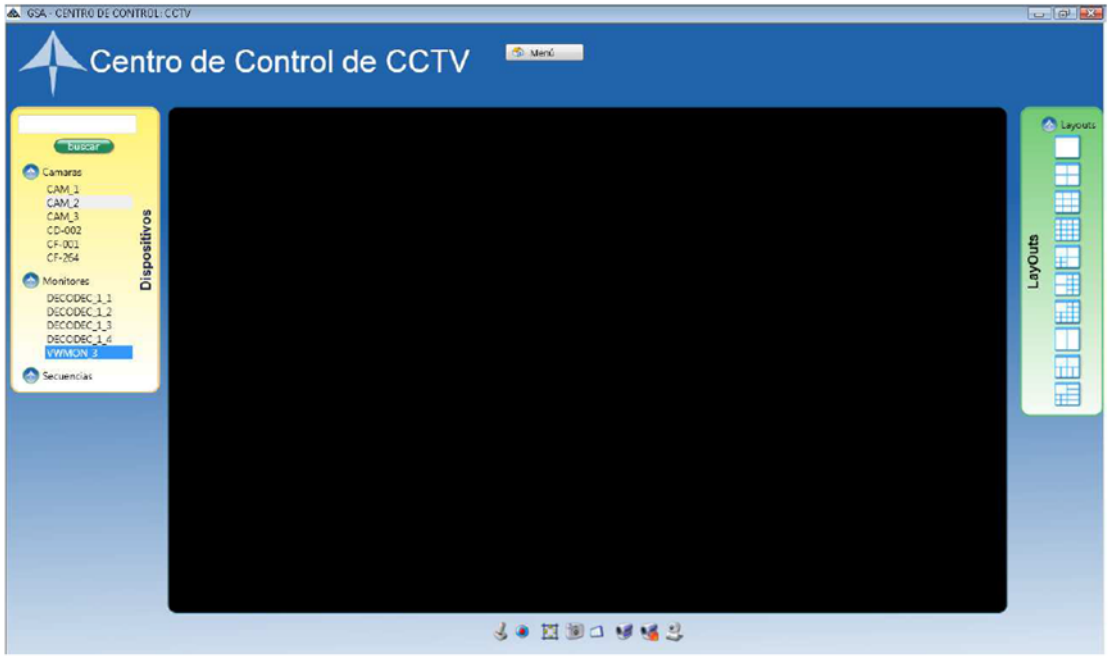

Figura 17. Pantalla principal, menú Centro de control CCTV, fuente [18]

En el centro de la ventana se muestran las vistas o layouts que el usuario haya seleccionado de todas las opciones que tenga disponibles por su perfil, estas opciones se muestran en el submenú derecho.

El submenú izquierdo permite localizar las cámaras y monitores dentro del sistema aplicando distintos filtros de búsqueda, así como secuencias de cámaras que se hayan definido en el sistema y que podrán ser seleccionadas si el usuario tiene acceso a todas las cámaras de la secuencia.

Estas secuencias no son otra cosa que sucesiones de cámaras con un tiempo determinado para la visualización de cada una, se crean y modifican en el menú de Administración y configuración (ver Anexo C.8.) y se pueden aplicar a cualquier ventana secundaria de un layout.

Los layouts o vistas, como se aprecia en la Figura 17, son la distribución de monitores virtuales que el operario encargado de la videovigilancia visualizará en la pantalla, estas distribuciones pueden ser muy variopintas dependiendo de múltiples factores como el número de cámaras desplegadas, la geometría de la zona que se vigila o ante eventos que deban visualizarse en pantalla completa. Por ello, las distribuciones de layout habituales son de 2x2, 4x4, 2x4 o similares. Estos layouts se asignan a los distintos perfiles y usuarios pudiendo estos conmutarlos manual o automáticamente ante un evento o alarma [7], [18].

Para el caso de cámaras con funciones de telemetría o PTZ como se denomina en inglés, también es posible realizar acciones de control, como mover el objetivo o alejar o acercar la vista, todo ello con el propio cursor del ratón o mediante botones digitales que aparecen al seleccionar la cámara.

Como ya se ha mencionado también, desde esta ventana es posible realizar la asignación cámara-monitor pudiendo conmutar o desconmutar una cámara en cualquier momento, desde el propio layout o seleccionando la cámara o el monitor en el submenú de dispositivos.

Por último, siempre que el usuario disponga del permiso en el sistema, es posible realizar grabaciones manuales seleccionando la cámara por cualquier método, estas grabaciones se guardan en las unidades de almacenamiento del sistema y pueden ser visualizadas para realizar la correspondiente exportación en caso de que así se requiera, desde el menú de Reproducción de video.

C.7. Centro de reproducción CCTV

Este submenú es básicamente un reproductor normal con la funcionalidad añadida de buscar las grabaciones dentro del sistema mediante filtros de fecha, dispositivo, usuario, unidad de almacenamiento o tipo (continua o bajo demanda) [19]. Las opciones de reproducción son las básicas de cualquier reproductor, play, pause, stop, salto al inicio/final, salto frame a frame, modificación de la velocidad de reproducción (x1,x2,x10…) añadiendo a estas opciones la visualización en layouts en cualquier distribución definida en el sistema con el fin de realizar exportaciones de evidencias unidas a capturas de pantalla y los correspondientes informes.

Puesto que el fin último de este menú es realizar dichas exportaciones, dentro de cada layout es posible reproducir distintos fragmentos de video sincronizado y grabarlos para su exportación. También es posible bloquear grabaciones para evitar el borrado automático al sobrepasar el tiempo máximo de retención definido en la LOPD.

Debido a la sensibilidad de la información y a la propia LOPD, el acceso a la reproducción de grabaciones está restringido a la máxima autoridad de un aeropuerto, el director de este o en su defecto un cargo delegado para tal función que asuma esa responsabilidad.

C.8. Administración y configuración

Este es el menú más importante en lo que a gestión se refiere pues modifica muchas de las acciones que se pueden llevar a cabo desde el resto de menús, en este capítulo se hará un recorrido meramente descriptivo sobre las distintas opciones disponibles pues son realmente extensas y no todas son importantes para el objetivo de este informe.

En la Figura 18 se muestra la pantalla principal de este menú.

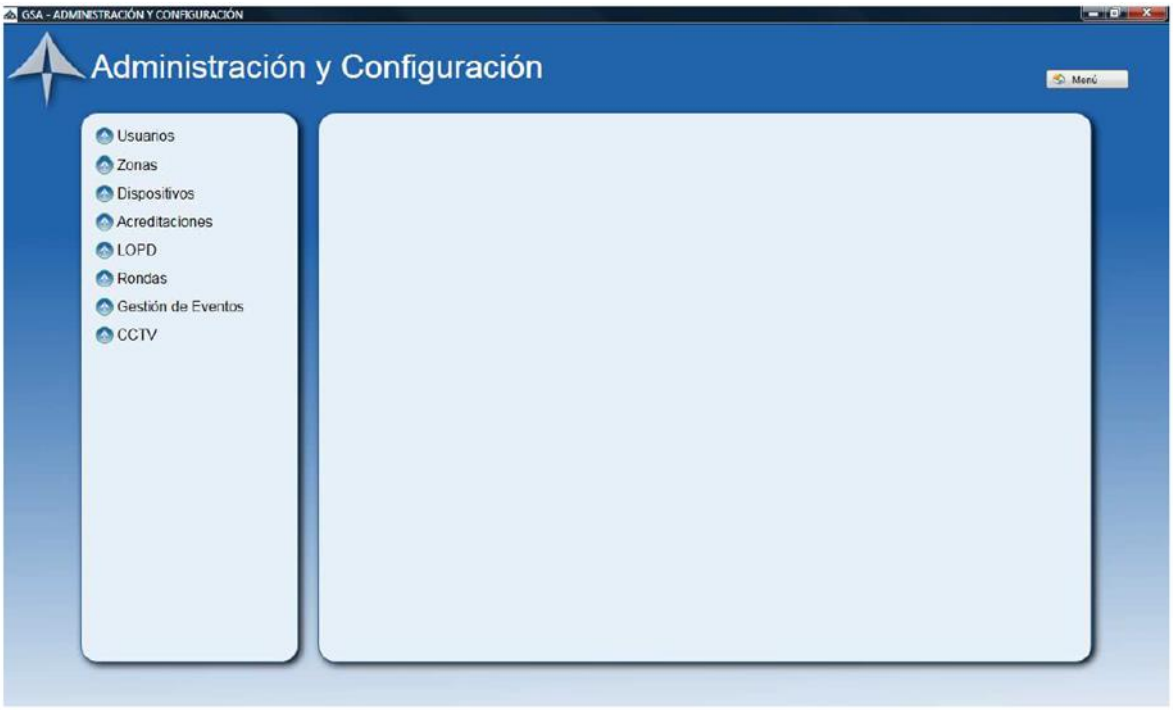

Figura 18. Pantalla principal, menú Administración y configuración, fuente [5]

En el submenú de la izquierda aparecen las distintas opciones de configuración, cada una de las cuales tiene distintas opciones, empezando por la primera se tiene [5]:

- Usuarios

Dentro de esta sección se pueden configurar tres elementos que caracterizan a un usuario:

- Perfiles, son básicamente patrones, configurados con una prioridad dentro del sistema numerada entre 1 y 1000 siendo el 1 el valor más prioritario, y con una serie de permisos, por ejemplo, generar acreditaciones, modificar mapas de sinóptico, acceso a las rondas etc.
- Cuentas de usuario, para las que se define un nombre de usuario y una contraseña, a cada cuenta se le asocian uno o más perfiles de los cuales heredará los permisos y una o más zonas a las que podrá acceder desde el sinóptico. También es necesario definir las distintas configuraciones de layouts que el usuario tendrá disponibles, desde esta ventana también es posible, para un administrador, cerrar la sesión de un usuario activo.
- Puestos, son los objetos que permiten identificar los puestos de trabajo físicos (clientes) a los que el usuario tendrá acceso, del mismo modo que para las cuentas de usuario, los puestos tienen zonas asignadas pudiendo solamente configurar los dispositivos que se encuentren dentro de esas zonas.

La prioridad dentro del sistema será la más alta (numéricamente la más baja) entre la cuenta de usuario y uno de los perfiles asignados, viéndose limitada también por los permisos asociados al puesto en el que se haya iniciado sesión.

- Zonas

Se caracterizan por ser "contenedores" de los dispositivos de campo asociados, a cada zona se le asignan unos dispositivos y son los únicos a los que permitirá acceso. Para realizar esta asignación se disponen de distintos filtros de búsqueda, por nombre o por tipo principalmente

- Dispositivos

Desde esta sección es posible dar de alta o de baja a un dispositivo dentro de la base de datos de GSA, para cada categoría de dispositivos definidas en el Anexo C.4. incluyendo además a los lectores de matrícula, monitores, y grabadores.

A cada dispositivo se le asigna una ficha con dos partes diferenciadas, una común y una específica para cada tipo, en la parte común se asigna un identificador único global (GUID) dentro del sistema básicamente un código alfanumérico, el cual se podrá reutilizar si se da de baja un dispositivo, también, un Alias que permita identificarlo de forma más sencilla para los operarios, por ejemplo, "dispositivo_01_zona00", junto a una descripción que puede ser algo más detallada.

Uno de las características más críticas para que un dispositivo sea compatible con GSA es su compatibilidad con el Protocolo Estándar (PE) de GSA, concepto que se desarrollará con más profundidad en el capítulo 4.2, este protocolo se actualiza de forma periódica y es necesario introducir en la ficha la versión del mismo que el dispositivo utiliza.

Por último, es necesario asignar a cada dispositivo un puerto, una máscara y una dirección IP dentro de la red, elementos que le permitirán interactuar y comunicar a través de la red interna, es posible también, asignar desde esta sección una zona o zonas al dispositivo en cuestión.

La parte específica de configuración de un dispositivo es única para cada tipo, con lo que se procederá a describir la correspondiente a las cámaras y grabadores ya que son los dispositivos de mayor interés para este proyecto:

  - Cámaras, cuentan con tres pestañas de configuración, la primera es la de video, dónde se le asigna un fabricante de los que estén reconocidos dentro del sistema (Sony, Bosch…), un formato de video (MPEG, JPEG, MxPEG…), la dirección y puerto IP así como el modo de trabajo (unicast o multicast), por último, resolución y tasa de frames y los parámetros de codificación del video para limitar el ancho de banda asignado.

La segunda pestaña, de telemetría, permite definir los preposicionamientos dentro del sistema, estos se pueden configurar asignándoles un número identificador entre 1 y el máximo aceptado por el sistema, una descripción y la posición que deberá adoptar la cámara al llamar a este preposicionamiento.

En la última pestaña, de grabaciones, es posible asignar el tipo de grabaciones que puede realizar la cámara, por defecto, continua, pudiendo permitir o no la grabación manual y por evento. Desde esta pestaña se asigna también un grabador al cual la cámara enviará los datos de video para ser almacenados.

  - Grabadores, al igual que para las cámaras, se les asigna una configuración de red, desde esta sección se puede comprobar el espacio total y el disponible del grabador, no siendo posible modificar estos campos.

Cuenta con dos pestañas de configuración, la primera de unidades de almacenamiento, básicamente particiones de memoria que actúan como contenedores de datos de video, esta opción no está disponible para grabadores de Bosch y VisioWave.

La segunda pestaña, de grabaciones, permite acceder a las grabaciones realizadas en cada grabador, están caracterizadas por la cámara que las ha realizado, la unidad de almacenamiento dónde está contenida y el tipo de grabación.

- Acreditaciones

En este submenú se configuran todos los campos desplegables presentados en la Figura 9, los permisos que se pueden conceder a una acreditación, los distintos modelos de tarjeta que se pueden imprimir, la lista negra de personas a las que no se puede conceder ningún tipo de acceso, los códigos de herramientas y el texto que aparecerá en el reverso de la acreditación una vez impresa.

- LOPD

En este submenú es posible consultar el tiempo máximo de retención de los datos personales, incluyendo grabaciones, generalmente limitado a 30 días naturales.

- Rondas

En este submenú se configuran los puntos de control, y tiempos de paso que conforman una ronda, las cuales pueden ejecutarse desde el menú GSA correspondiente.

- Gestión de eventos

En este submenú se configuran las acciones a llevar a cabo de forma automática por los distintos dispositivos, bien de forma programada, definiendo perfiles temporales con unas acciones determinadas dentro de ese intervalo horario, o bien ante la detección de determinados estados o eventos en los dispositivos de campo, como una alarma, un sabotaje o un acceso coaccionado.

- CCTV

En este submenú se configuran las secuencias de cámaras accesibles desde el menú Centro de control CCTV de GSA, definiendo el orden y tiempo asignado a cada cámara dentro de la secuencia.

ANEXO D DESGLOSE DE FABRICANTES

Tabla 2. Desglose completo de los productos

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
				Siveillance Video Pro 2019 R3	XProtect (Corporate)	VMS Omnicast-Security Center 5.8	SMAVIA Recording Server IPS 10000
RQ-001	Esencial	**Arquitectura**	Opciones del SDK	Completa API de desarrollo para framework .NET, gratuita	Integración de funcionalidades de sistemas propios y de terceros (**página 46**)	-	-
RQ-002	Esencial	**Arquitectura**	Otros estándares soportados	ONVIF y PSIA	ONVIF	ONVIF	ONVIF
RQ-003	Esencial	**Arquitectura**	Redundancia de servidores: características	Se dispone de servidores de conmutación dedicados y preconfigurados en modo hot spare (1-1) o cold spare (1-n)	Se dispone de redundancia de grabaciones entre sites y el nodo central con distinta calidad en funcionamiento normal y ante un evento	Se dispone de redundancia de archivos, archivos auxiliares, edge storage, almacenamiento en la nube, es necesario definir los roles que pueden conmutar	-
RQ-004	Esencial	**Arquitectura**	Redundancia de servidores: tipos de conmutación por fallo	Hot/Cold-stand by	Hot/Cold stand by. Se puede conmutar las grabaciones a los sites federados en caso de caída del nodo principal.	-	-
RQ-005	Esencial	**Arquitectura**	Soporte multicast	Sí, aunque por defecto es unicast ya que las cámaras se conectan directamente a los grabadores y estos a los clientes	Sí, (confirmación necesaria)	Sí, para reproducciones	Sí, para reproducciones y grabación
RQ-006	Esencial	**Arquitectura**	Soporte ONVIF	Perfiles S y G	Perfiles S y G (+puente ONVIF hacia sistemas públicos remotos)	Perfiles S y G	Perfil S
RQ-007	Esencial	**Datos**	Exportaciones: garantía de no modificación de los archivos exportados	Mediante firma digital	Mediante firma digital	Mediante marca de agua	-
RQ-008	Esencial	**Datos**	Formatos de almacenamiento de cámaras IP o (de)codificadores IP	MJPEG, MPEG4, MPEG-4 ASP, MxPEG, y H264	MJPEG, MPEG4, MPEG-4 ASP, MxPEG, H264 y H265	MJPEG, MPEG4, H263, H264, H265, CIF, QCIF y 4CIF	H264, H265/G.722.1
RQ-009	Esencial	**Datos**	Formatos de codificación (compresión) de video	H264 y H265	H264 y H265	H263, H264, H265	H264, H265/G.722.1
RQ-010	Esencial	**Integración**	Integración via MIP SDK (de terceros)	Se pueden añadir plug-in de terceros fabricantes para analítica de video, control de accesos, paneles de intrusión, etc.	Se pueden añadir plug-in de terceros	-	-
RQ-011	Esencial	**Integración**	Integración via MIP SDK (propios)	Integración de forma nativa SiPass, Siveillance Vantage, Site IQ, Desigo CC (**ver aclaración**)	-	-	-
RQ-012	Esencial	**Integración**	Limitaciones por hardware/software de dispositivos conectados	No	No (admite software de terceros en los servidores)	No (ofrece una lista de los fabricantes compatibles)	-
RQ-013	Alto	**Almacenamiento**	Almacenamiento de grabaciones pre-evento	Por defecto, el pre-buffer se almacena en la memoria de los propios grabadores, si no se dispone de memoria, se puede almacenar en los discos	El tamaño del pre-buffer es configurable y se puede almacenar en el disco o en la memoria del dispositivo	-	-
RQ-014	Alto	**Almacenamiento**	Ampliación de la capacidad de almacenamiento	Sí, mediante cualquier disco/carpeta de almacenamiento accesible desde Windows, reconocible como una unidad de disco (locales, iSCSI, fiber-channel…)	-	-	JBOD 12/24, MegaRAID controller Kit

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-015	Alto	**Almacenamiento**	Comportamiento ante caida de los servidores de almacenamiento	Se utiliza el almacenamiento local, conmutación por fallo, o se hace uso de los servidores en stand-by	Se utilizan servidores auxiliares de conmutación por fallo	Conmutación por fallo, es necesario mover las cámaras de una unidad de video a otra dentro del Archiver, las cámaras desplazadas se tratan como nuevos dispositivos	-
RQ-016	Alto	**Almacenamiento**	Contenedores de almacenamiento: asignación de dispositivos	Es posible asignar un dispositivo a distintos contenedores de forma simultánea		-	-
RQ-017	Alto	**Almacenamiento**	Contenedores de grabación: gestión de dispositivos	Es posible mover uno o varios dispositivos entre dos contenedores, junto a los datos grabados, o dejar los datos para que consuman el tiempo de retención	Cada dispositivo se asigna a un contenedor, mientras que los contenedores pueden compartir el contenido de uno o varios dispositivos entre sí	-	-
RQ-018	Alto	**Almacenamiento**	Control de los parámetros de flujos de video	Por cada flujo (MPEG y H265) es posible grabar sólo los i-frames y no los p-frames o b-frames, (todo el flujo o sólo frames clave)	-	-	-
RQ-019	Alto	**Almacenamiento**	Firma digital de las grabaciones (garantía de no modificación/edición de los datos)	Sí, se realizan en la base de datos del servidor de grabación	Sí, mediante cifrado AES de 256 bit para medios, modo simple y completo. Mediante SHA-2 para audio, video y metadatos grabados	Sí, mediante marca de agua	-
RQ-020	Alto	**Almacenamiento**	Frame rate soportado en grabaciones	Desde 30 fps hasta más de 60 en cámaras industriales, limitación sólo por el hardware de la cámara	Al menos 30 FPS por cámara, límitado solamente por el hardware	Hasta 60 FPS por cámara independientemente del número de cámaras conectadas al sistema	Hasta 30 FPS en UHD
RQ-021	Alto	**Almacenamiento**	Granulación/partición de los datos	Sí, los grabadores pueden asignarse a distintas unidades de almacenamiento (cabinas) para que en caso de fallo en una, el resto soporte las cámaras asignadas	RAID 5 ó 6 para las BBDD de archivo y RAID 10 para las BBDD vivas	-	Tipo RAID 6
RQ-022	Alto	**Almacenamiento**	Tasa de bits por canal	Variable o fija (y acotada) para cada flujo de video, para limitar el ancho de banda por cada cámara	-	-	Hasta 50 Mbps dependiendo de la cámara
RQ-023	Alto	**Almacenamiento**	Tiempo máximo disponible para grabaciones manuales	Sí, modificable por los administradores	Sí	-	
RQ-024	Alto	**Arquitectura**	Arquitectura federada: autonomía de los sistemas	Sí, los sistemas locales federados pueden actuar de forma totalmente autónoma ante fallos en la red, aunque siempre supeditados al sistema central	Sí, los sites pueden funcionar de forma totalmente autónoma, deben tener un supervisor o gestor común (sólo Corporate y Expert)	Sí, es posible controlar el PTZ, acceder al video en caché y mantener la conexión con una cámara ante fallos o desconexiones del sistema	-
RQ-025	Alto	**Arquitectura**	Arquitectura federada: estructura	Centralizada, con un nodo central y uno o varios nodos locales	Estructura jerarquizada piramidal, los sites individuales conceden acceso general desde los nodos superiores (con mayor prioridad/derechos)	-	-
RQ-026	Alto	**Arquitectura**	Arquitectura federada: retrocompatibilidad (propia y de terceros)	Sólo para software propio, admite la versión 2016 y 2014 del Siveillance Video y todas las subversiones (Core, Plus, Advanced y Pro)	En la federación padre/hijo, la versión Corporate es compatible con el resto de versiones, reservando para estas las autorizaciones de log in	-	-
RQ-027	Alto	**Arquitectura**	Base de datos de grabación (características)	El video MJPEG, MPEG4, MPEG-4 ASP, MPEG, H.264 o H.265 se almacena en la base de datos de video, que puede cifrarse para proteger los datos	Las BBDD admiten dos modos de cifrado de video usando cifrado AES de 256 bits, ligero (sólo para una parte de los datos de video) o fuerte (para todo)	-	-
RQ-028	Alto	**Arquitectura**	Cliente de video: acceso a cámaras de sistemas interconectados o federados	Sí	Sí	-	-
RQ-029	Alto	**Arquitectura**	Cliente de video: acceso de los usuarios a las cámaras	Los usuarios sólo acceden a las cámaras a través de los grabadores, dejando la red de cámaras restringida a video y aislada por seguridad (Hotspot global)	Los usuarios acceden a las funcionalidades de la cámara mediante Función Hotspot global y local (desde cualquier vista o desde la vista actual)	-	-
RQ-030	Alto	**Arquitectura**	Cliente de video: ajuste de la calidad de la visualización en vivo	Es posible aplicar filtros para eliminar bordes de imagen	-	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-031	Alto	**Arquitectura**	Cliente de video: número de layouts soportados	41, optimizados para displays 4:3 y 16:9	100, optimizados para displays 4:3 y 16:9. Pueden incluir imágenes, páginas web, texto…	-	-
RQ-032	Alto	**Arquitectura**	Cliente de video: opciones adicionales	Tecnología propia SVQR, para adaptar la resolución de la cámara al ancho de banda real mediante transcodificación del video (**ver explicación**)	Indicadores de estado de video, para monitorizar el estado de la cámara sin necesidad de acceder a ella	-	-
RQ-033	Alto	**Arquitectura**	Cliente de video: opciones para vistas con poco movimiento	Función motion only para descodificar o no una imagen en vistas con poco movimiento	Función de actualización de imagen en función de la VMD para descodificar o no una imagen y poder visualizarla	-	-
RQ-034	Alto	**Arquitectura**	Cliente de video: proceso de exportación de video	En tres pasos, (**ver explicación**). En formato propio se pueden exportar varias cámas simultáneamente	En un solo paso, si se hace desde el cliente web pueden almacenarse para su descarga posterior	-	-
RQ-035	Alto	**Arquitectura**	Cliente de video: reproducción múltiple	Sí (se puede reproducir simultáneamente hasta 100 cámaras)	Sí (se puede reproducir simultáneamente hasta 100 cámaras sin necesidad de que estén sincronizadas)	Sí (se pueden reproducir simultáneamente hasta 64 cámaras sincronizadas o no)	-
RQ-036	Alto	**Arquitectura**	Cliente de video: visualización de cámaras ante eventos (incidentes)	Automática, con un click para volver a la vista original	Manual o automática, incluyendo las cámaras de los sistemas federados o interconectados	-	-
RQ-037	Alto	**Arquitectura**	Cliente móvil: control PTZ	Sí, manual o mediante preposicionamientos	-	-	-
RQ-038	Alto	**Arquitectura**	Cliente móvil: creación de metadatos	Sí, mediante Video Push, permite además utilizar la cámara del dispositivo como una cámara de vigilancia más, con metadatos de la posición GPS	Sí, depende de los derechos de usuario, además se puede utilizar la cámara del dispositivo móvil para realizar grabaciones remotas como una cámara más	-	-
RQ-039	Alto	**Arquitectura**	Cliente móvil: exportaciones de video	Sí, se solicitan desde el cliente móvil y se exportan en el servidor para su descargar a posteriori	Sí, al menos de las que se hayan creado desde el cliente web	-	-
RQ-040	Alto	**Arquitectura**	Cliente móvil: gestión de eventos	Sí, es posible añadir eventos manuales de operador para marcar partes del video grabado que se consideren relevantes	Sí, similar al cliente web	-	-
RQ-041	Alto	**Arquitectura**	Cliente móvil: playback de grabaciones	Sí, simultáneamente con el video vivo de la misma cámara velocidad de reproducción ajustable	-	-	-
RQ-042	Alto	**Arquitectura**	Cliente móvil: sincronización de las vistas del usuario	Sí, se heredan las vistas del usuario directamente del VMS y se muestran como una lista de cámaras en el dispositivo	Sí, se heredan las vistas del usuario directamente del VMS tanto las privadas como las compartidas, mostrandolas como una lista	-	-
RQ-043	Alto	**Arquitectura**	Cliente móvil: visualización de las cámaras	Se muestran todas automáticamente cuando no hay un setup configurado, es posible aplicar filtros para buscar y seleccionar una	Se concede acceso al video vivo y grabado	-	-
RQ-044	Alto	**Arquitectura**	Cliente móvil: visualización en pantalla completa	Sí, se puede cambiar de cámara deslizando hacia los lados	Sí, se puede navegar por la vista de cámara deslizando hacia los lados	-	-
RQ-045	Alto	**Arquitectura**	Cliente móvil: zoom	Sí, digital	Sí, digital	-	-
RQ-046	Alto	**Arquitectura**	Cliente web: acceso	Directamente desde el buscador, no es necesario setup ni instalación en el ordenador cliente	Mediant HTTPS, directamente desde el navegador, sin necesidad de plug ins o extensiones. (**página 44)**	-	-
RQ-047	Alto	**Arquitectura**	Cliente web: control PTZ	Sí, admite movimiento PTZ incluyendo preposicionamientos y zoom	Sí, ofrece funcionalidad completa de preposicionamientos y acciones previamente asociadas a una cámara	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-048	Alto	**Arquitectura**	Cliente web: creación de archivos	AVI o imágenes JPEG	Imágenes JPEG, archivos AVI, MKV, audio. Permite reproducir grabaciones aunque se hayan borrado de las BBDD de medios	-	-
RQ-049	Alto	**Arquitectura**	Cliente web: decodificación de video	Sí, mediante un flujo MJPEG sin necesidad de plugins de decodificación en el lado cliente aunque son opcionales	Sí, se limitan la resolución y los FPS en la transmisión hacia el cliente web y móvil	-	-
RQ-050	Alto	**Arquitectura**	Cliente web: exportaciones de video	Sí, se pueden realizar en el servidor y descargarlas a posteriori con opción de previsualización sin necesidad de descarga	Sí, se pueden realizar en el servidor y descargarlas a posteriori. Se pueden previsualizar sin necesidad de descargarlas	-	-
RQ-051	Alto	**Arquitectura**	Cliente web: protocolo de seguridad de la conexión	HTTPS	HTTPS	-	-
RQ-052	Alto	**Arquitectura**	Cliente web: transmisión de audio hacia múltiples cámaras	Sí, simultáneamente a los altavoces de las cámaras	Sí, admite también la reproducción de audio entrante desde los dispositivos	-	-
RQ-053	Alto	**Arquitectura**	Cliente web: usuarios remotos	Pueden escuchar, reproducir y exportar grabaciones de audio via Internet de los dispositivos conectados	Pueden acceder al video vivo, audio, control PTZ, configuraciones guardadas, reproducción, exportación de video y audio	-	-
RQ-054	Alto	**Arquitectura**	Cliente web: vistas compartidas entre usuarios	Sí, hay vistas privadas para cada usuario y vistas públicas para grupos que se administran desde el cliente de gestión mediante derechos de usuario	Sí, los usuarios pueden crear vistas privadas y compartirlas con usuarios con los mismos derechos	-	-
RQ-055	Alto	**Arquitectura**	Cliente web: visualización de eventos	Sí, se puede acceder en vivo a la cámara que haya notificado una alarma o evento	Sí, se tiene acceso al listado y búsqueda de alarmas, imagen de la cámara asociada y audio, posibilidad de gestión remota, cambio de prioridad y escalado y reenvio	-	-
RQ-056	Alto	**Arquitectura**	Conexión físicamente remota de cámaras	Sí, es posible conectar cámaras desde cualquier ubicación con conexión a un grabador, de forma continua o bajo demanda	-	-	-
RQ-057	Alto	**Arquitectura**	Control (limitación) del ancho de banda de cámaras IP	Sí, limitación manual (fija) o dinámica (adaptable)	Sí	-	-
RQ-058	Alto	**Arquitectura**	Licencias: federación de la arquitectura	Licencia libre para el uso de la arquitectura federada	Licencia libre para el uso de la arquitectura federada	-	-
RQ-059	Alto	**Arquitectura**	Licencias: Garantía duración y extensión	Licencia perpetua y actualizaciones gratuitas para nuevos dispositivos y parches de seguridad, con un pago adicional se incluyen upgrades a nuevas versiones	-	-	36, 48, 60 meses (garantía y actualización)
RQ-060	Alto	**Arquitectura**	Licencias: gestión de licencias para cambio/reemplazo de dispositivos	Se otorga un margen del 15% (min 10 max 100) al año para reemplazos sin reactivación de licencias, si se sobrepasa hay que reactivar el producto (sin coste)	Se puede realizar los cambios o reemplazo de dispositivos sin necesidad de activar una nueva licencia	-	
RQ-061	Alto	**Arquitectura**	Licencias: licencia base	Obligatoria, incluye la licencia del monitoring wall para la creación de videowalls desde el sistema (**página 22**)	Obligatoria, otorga cantidad ilimitada de servidores de gestión, de grabación, y aplicaciones cliente de video, web y móvil	-	Dos licencias para clientes, módulo de protección de datos, licencia para grabación de 32 flujos y actualización por 24 meses, licencia para un JBOD
RQ-062	Alto	**Arquitectura**	Licencias: licencias adicionales/opcionales	Se pueden añadir licencias para otros dispositivos no CCTV, puertas de CA, sistemas anti-intrusión o video analíticas	-	-	Premote-HD, Recepción de datos de terceros, aumento de los FPS con cámaras propias, segunda interfaz de red

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-063	Alto	**Arquitectura**	Licencias: licencias hardware (dispositivos conectados)	Una por cada dirección IP conectada (cámaras, audio, decodificadores y otros) independientemente de los flujos que manejen	Una por dispositivo conectado, incluyendo aquellos de los sites federados (siempre que su gestión pase por el nodo central)	-	Ampliación del número de clientes (1,5,10+) y canales de grabación (también para terceros)
RQ-064	Alto	**Arquitectura**	Licencias: número de dispositivos hardware admitidos	Ilimitado, se solicitará el número de la licencia base para cada uno	Ilimitada, una por dirección IP para cámaras, dispositivos de audio, codificadores, y otros	-	
RQ-065	Alto	**Arquitectura**	Licencias: licenciamiento de sistemas interconectados	Sólo se requieren licencias para dispositivos conectados al sistema federado/interconectado si se puede acceder a ellos desde el sistema central	Se requiere una licencia por dispositivo en cada site interconectado, ligada al sistema padre, muestra todos los dispositivos interconectados	-	-
RQ-066	Alto	**Arquitectura**	Monitoring wall: configuración ante incidentes	Permite eliminar las cámaras secundarias del monitoring wall o poner las cámaras en alarma en monitores específicos automáticamente, función Black Screen	Admite cambio de contenido y distribución de los monitores en el Video Wall	-	-
RQ-067	Alto	**Arquitectura**	Monitoring wall: configuración de los monitores	Se puede definir múltiples monitoring walls, ajustando la posición y el tamaño de cada monitor, para formatos 4:3 o 16:9	Se puede definir múltiples monitoring walls, ajustando la posición y el tamaño de cada layout dentro de cada monitor	-	-
RQ-068	Alto	**Arquitectura**	Monitoring wall: opciones adicionales	Decodificación acelerada por hardware para tarjetas Nvidia para liberar al procesador de la carga de decodificación y codificación de video	Aceleración de hardware del Smart Client, mediante GPU NVIDIA, Intel Quick Sync y ambos combinados (**página 17**)	Decodificación acelerada por hardware GPU, permite mostrar más cámaras simultáneamente	-
RQ-069	Alto	**Arquitectura**	Número de cámaras para reproducción playback	Hasta 100, sincronizadas	Hasta 100	-	-
RQ-070	Alto	**Arquitectura**	Número de cámaras/flujos para visualización de video vivo simultáneamente	Hasta 100 (por monitor)	-	Hasta 64 por cliente	-
RQ-071	Alto	**Arquitectura**	Número de clientes soportados	Ilimitado (video, web y móvil)	Ilimitado	-	-
RQ-072	Alto	**Arquitectura**	Número de eventos soportados	Hasta 600 por segundo	-	-	-
RQ-073	Alto	**Arquitectura**	Número de monitores soportados	Ilimitado	Ilimitado	-	-
RQ-074	Alto	**Arquitectura**	Número de perfiles temporales configurables	Ilimitado, permiten definir horarios y ámbitos de actuación	Ilimitado	-	-
RQ-075	Alto	**Arquitectura**	Número de preposicionamientos por cámara	Ilimitado	-	-	-
RQ-076	Alto	**Arquitectura**	Número de servidores de gestión	Ilimitado	Ilimitado	-	-
RQ-077	Alto	**Arquitectura**	Número de servidores de grabación	Ilimitado	Ilimitado	-	-
RQ-078	Alto	**Arquitectura**	Opciones adicionales de seguridad y protección	Es posible cifrar la comunicación entre servidores, entre grabadores y clientes y entre bases de datos mediante certificados de clave pública	Inicio de sesión automático reutilizando las últimas credenciales utilizadas en el log in	Función de puntuación de la seguridad para monitorizar el cumplimiento de cada subsistema con las pautas de seguridad	-
RQ-079	Alto	**Arquitectura**	Protección del video contra borrado accidental	Sí, mediante permisos específicos de acceso a la opción	-	Sí	-
RQ-080	Alto	**Arquitectura**	Rastreo de personas u objetos en movimiento	Sí (mediante análisis de video)	Sí (mediante análisis de video)	Sí, función rastreo de informes, para video vivo y grabaciones (**página 190 MA**)	-
RQ-081	Alto	**Arquitectura**	Redundancia de servidores: funcionalidad	Se unifica la localización de las grabaciones en la BBDD de gestión de forma transparente para el usuario al conmutar la grabación debido a un fallo	-	Se dispone de una réplica exacta de los archivos de video y datos asociados en discos separados y BBDD	-
RQ-082	Alto	**Arquitectura**	Servidor móvil: certificados	Por defecto para encriptación HTTPS sobre SSL/TLS o uno propio personalizado	Utiliza certificados digitales propios o proporcionados por el cliente	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-083	Alto	**Arquitectura**	Servidor móvil: exportaciones	Sí, se pide desde el cliente, se prepara en el servidor y se descarga cuando se desee	Sí, se pide desde el cliente, se prepara en el servidor y se descarga cuando se desee	-	-
RQ-084	Alto	**Arquitectura**	Servidor móvil: instalación	En un servidor propio o junto a otros componentes. Funciona como un servicio dedicado	-	-	-
RQ-085	Alto	**Arquitectura**	Servidor móvil: opciones del plug-in	En el cliente de gestión da acceso a cambios de configuración, informes de estado y gestión y consulta de las exportaciones realizadas	-	-	-
RQ-086	Alto	**Arquitectura**	Servidor móvil: uso de ancho de banda	Dinámico, se adapta al disponible transcodificando los flujos de video de H264/5 a MJPEG	-	-	Transcodificación del video (vivo y grabado) para la transmisión en redes con menor ancho de banda Función Premote-HD
RQ-087	Alto	**Arquitectura**	Servidor móvil: validación y verificación del setup	Previo a la entrega mediante integradores del sistema para adaptarlo a la versión actual del sistema	-	-	
RQ-088	Alto	**Arquitectura**	Soporte DLNA	Sí, permite reproducir video en monitores compatibles sin necesidad de un ordenador o cliente	Sí, permite reproducir video en cualquier pantalla o TV sin necesidad de equipo adicional	-	
RQ-089	Alto	**Arquitectura**	Traspaso de cámaras entre servidores de grabación	Sí (sin interrumpir la grabación actual)	Sí (sin interrumpir la grabación actual)	-	-
RQ-090	Alto	**Datos**	Encriptación de video	Sí, solo para formato propio	-	Sí (de principio a fin incluyendo periféricos)	Sí
RQ-091	Alto	**Datos**	Exportaciones: exportación con múltiples destinatarios	Sí, pueden exportarse en los distintos formatos	Sí, pueden estar en distinto formato	-	-
RQ-092	Alto	**Datos**	Exportaciones: formato de imagen/video	MKV, archivos AVI o imágenes JPEG, además de formato propio de exportación y reproducción en Siveillance	AVI, MKV, JPEG, formato propio con el cliente asociado para permitir la visualización de instantáneas	-	-
RQ-093	Alto	**Datos**	Exportaciones: protección de las exportaciones	Mediante encriptación y contraseña, con los algoritmos de encriptación 56-bit DES 128 y 192/256-bit AES	Mediante encriptación y contraseña. Protocolo 56 bit DES y 128/192/256-AES	Mediante enciptación y contraseña de hasta 128 bits. Protocolo TLS con AES y RSA, RTSP	-
RQ-094	Alto	**Datos**	Exportaciones: re-exportaciones de una grabación	Sí, puede cambiarse el formato a cualquiera de los formatos soportados, se puede desactivar esta opción	Sí, puede desactivarse durante la primera exportación	-	-
RQ-095	Alto	**Datos**	Metadatos: Generación de por detección de movimiento (VMD)	Sí (independiente de la cámara)	Sí (independiente de la cámara)	-	
RQ-096	Alto	**Datos**	Protocolos de encriptación	HTTPS para dispositivos móviles y cliente web	HTPPS para el servidor móvil y web	HTTPS, SSL/TLS 1.2 (AES), acceso a red según IEEE 802.1X	Protocolo TLS, AES, RSA y RTSP
RQ-097	Alto	**Dispositivos**	Bloqueo y protección de los dispositivos (I)	Se puede denegar la gestión, lectura, edición y borrado de dispositivos por parte de cualquier usuario con prioridad inferior	-	Se puede restringir la visualización de video vivo o grabado a usuarios con menor prioridad en intervalos horarios concretos o permanentemente	-
RQ-098	Alto	**Dispositivos**	Bloqueo y protección de los dispositivos (II)	Se pueden generar y modificar contraseñas para uno o varios dispositivos	-	Se pueden encriptar también los dispositivos periféricos	-
RQ-099	Alto	**Dispositivos**	Configuración de los flujos por cámara	Admite varios flujos de video por cámara, cada uno con distintos parámetros de formato, FPS, resolución y calidad	Admite varios flujos de video vivo, con distinto formato o compresión, resoluciones y FPS	Admite varios flujos con distintos parámetros, video vivo, grabado y acceso remoto, puede ajustar automáticamente la calidad en función del tamaño del layout	-
RQ-100	Alto	**Dispositivos**	Definición de preposicionamientos PTZ	En el servidor, número no definido	En la cámara, se pueden importar y renombrar	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-101	Alto	**Dispositivos**	Detección, registro y puesta en marcha de dispositivos	Vía Hardware wizard, via UPnP, escaneo de la red IP o via detección manual. Todos los métodos se pueden automatizar (**ver aclaración**)	Vía UPnP de forma automática, escaneo de alcance de red IP o detección manual	Vía UPnP, creación automática de los dispositivos al conectarse las unidades de video al sistema	-
RQ-102	Alto	**Dispositivos**	Importación de preposicionamientos	Sí (desde la propia cámara)	Sí (desde la propia cámara)	-	-
RQ-103	Alto	**Dispositivos**	Máscara de privacidad: activación/desactivación	Mediante el cliente de gestión, se controlan mediante reglas de doble validación	-	Activación manual, derechos de usuario necesarios para la desactivación	-
RQ-104	Alto	**Dispositivos**	Máscara de privacidad: funcionalidades	Permite ocultar áreas en la visión de la cámara en el video vivo, grabaciones y exportaciones. Se pueden utilizar máscaras propias de la cámara o del servidor	Permite enmascaran areas definidas por un administrador, de forma permanente o semipermanente para usuarios con el derecho de acceso	Permite anonimizar el video y crea dos flujos, el privado (confindencial) y el público con la máscara (**página 173 MU**). Función Privacy Protector	-
RQ-105	Alto	**Dispositivos**	Número de cámaras soportadas	Ilimitado	Ilimitado	-	-
RQ-106	Alto	**Dispositivos**	Opciones de ajuste de los parámetros de video en cámaras	Formato, FPS, resolución y calidad de los flujos por cada cámara	Formato, FPS, resolución y calidad de los flujos por cada cámara	-	-
RQ-107	Alto	**Dispositivos**	Opciones disponibles en el reemplazo de dispositivos	Se conservan la configuración y las grabaciones (via Wizard)	Se conservan los ajustes y registros de configuración	Conservar la configuración al copiarla de uno a otro, para dispositivos federados sólo se admiten cámaras	-
RQ-108	Alto	**Evento/fallo**	Alarmas: acceso a las cámaras	Instantáneo tanto en video vivo como en playback	-	-	-
RQ-109	Alto	**Evento/fallo**	Alarmas: asociación de cámaras-alarmas	Se pueden asignar una o varias cámaras a una alarma, en la ventana de previsualización se muestran un máximo de 15 cámaras simultáneamente	Se pueden asignar una o varias cámaras a una alarma, en la ventana de previsualización se muestran un máximo de 15 cámaras simultáneamente	-	-
RQ-110	Alto	**Evento/fallo**	Alarmas: escalado y transmisión de alarmas	Sí (las alarmas se asignan automáticamente al usuario o a un grupo de usuarios, luego pueden escalarse para distribuirlas a otros usuarios	Sí, mediante asociación del propietario inicial de la alarma (usuario individual o grupo) y su prioridad.	-	-
RQ-111	Alto	**Evento/fallo**	Alarmas: información disponible para usuarios	Alarmas producidas, tipos de alarma, prioridad de las alarmas y textos descriptivos (dispositivos afectados, cámaras y mapas asociados)	Principalmente, imagen asociada, ubicación, fuente y tiempo, (**página 31**)	-	-
RQ-112	Alto	**Evento/fallo**	Alarmas: listado de eventos en los sites interconectados o federados	Sí, común para todos los sites	Sí, común para todos los sistemas de todos los sites interconectados	Sí	-
RQ-113	Alto	**Evento/fallo**	Alarmas: prioridad de las alarmas	Sí (se pueden aplicar filtros para mostrar sólo las más críticas)	Sí, prioridades personalizables, con notificaciones sonoras ajustadas a cada prioridad	-	-
RQ-114	Alto	**Evento/fallo**	Alarmas: trazabilidad de las consecuencias	El operador puede añadir mensajes sobre una alarma que sumados a los generados por el sistema pueden exportarse como PDF o para imprimir (**ver aclaración**)	-	-	-
RQ-115	Alto	**Evento/fallo**	Grabaciones bloqueadas: exportación	Directa, en un solo paso	Directa, en un solo paso	-	-
RQ-116	Alto	**Evento/fallo**	Grabaciones bloqueadas: herramienta de bloqueo	Sí, Función Evidence Lock para bloquear una parte de la grabación y prevención del borrado	Sí	Sí	-
RQ-117	Alto	**Evento/fallo**	Importación de imágenes pre-evento grabadas localmente en la cámara	Sí	Sí	-	-
RQ-118	Alto	**Evento/fallo**	Notificación de las incidencias	Via email con imágenes adjuntas y/o archivos AVI adjuntos (fotos o clips de video también)	Via email	Via email	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-119	Alto	**Evento/fallo**	Tiempo de retención de las grabaciones (I)	Se puede definir un tiempo de retención por cada grupo de cámaras y por cada almacen de video dentro de cada uno (**ver aclaración**)	Flexible, se pueden definir tiempos de retención a corto, medio y largo plazo	-	-
RQ-120	Alto	**Evento/fallo**	Tiempo de retención de las grabaciones (II)	Definición manual, es necesario seleccionar el intervalo de tiempo que se va a conservar (para una o varias cámaras a la vez)	Se puede extender manualmente el periodo de retención para video bloqueado de una o varias cámaras y sus dispositivos asociados	-	-
RQ-121	Alto	**Evento/fallo**	Tolerancia a fallos del sistema	Mejora mediante redundancias de equipos y clúster de Windows, Vmware o Hyper-V	-	Se pueden guardar las BBDD SQL que continenen la configuración de los directorios de forma remota o local para ejecutarlas en caso de fallo (**página 9 DT**)	-
RQ-122	Alto	**Gestión**	Gestión de evidencias (grabaciones)	Se puede configurar el tiempo de retención y previsualización de las secuencias bloqueadas	-	-	-
RQ-123	Alto	**Gestión**	Gestión del espacio de almacenamiento	En función del ancho de banda. Se puede combinar total o parcialmente entre remoto y centralizado	-	-	-
RQ-124	Alto	**Gestión**	Licencias: extensión para instalaciones multi-site	Sí	-	-	-
RQ-125	Alto	**Gestión**	Licencias: registro y validación	Online via internet, offline via email o web	Online via internet, offline via email o web en redes cerradas	-	-
RQ-126	Alto	**Gestión**	Sites: gestión remota	Se pueden definir sites conectados y desconectados, se gestionan desde el cliente de gestión. Pueden enviar video de forma continua, ante evento o por conexión	El sistema padre puede realizar las funciones de gestión de la información y comunicación de los sites que no puedan hacerlo	-	-
RQ-127	Alto	**Gestión**	Sites: subida (importación) de video	Se puede definir el intervalo de tiempo y el ancho de banda asignado a cada uno desde los grabadores para cada site desconectado	Se puede importar solamente el video disponible para playback	-	-
RQ-128	Alto	**Gestión**	Streaming multicast de un flujo a múltiples clientes	Sí (se necesita IGMP para redes remotas)	-	Sí (usa el ancho de banda de cada sector de red solamente una vez)	-
RQ-129	Alto	**Integración**	Dispositivos monitor (monitoring wall)	Independiente del hardware, funciona en servidores y displays estándar sin configuración necesaria	-	Deben conectarse el decodificador y el monitor y agregarse al sistema como una sola entidad de video	-
RQ-130	Alto	**Servidores**	Alimentación de los HDD	-	-	-	150W, 115/230V AC (5%), 50/60 Hz (hasta 3 módulos)
RQ-131	Alto	**Servidores**	Ampliación de almacenamiento	-	-	-	JBOD 12/24, MegaRAID controller Kit
RQ-132	Alto	**Servidores**	Batería auxiliar	-	-	-	Sí (para el reloj y las memorias de configuración)
RQ-133	Alto	**Servidores**	Cámaras IP: Almacenamientos de emergencia	-	-	-	Sí (solo para propias), EdgeStorage y SmartBackfill
RQ-134	Alto	**Servidores**	Cámaras IP: Base de datos	-	-	-	Sí (solo para propias), tipo VCA
RQ-135	Alto	**Servidores**	Cámaras IP: Bloquear la configuración	-	-	-	Sí (solo para propias)
RQ-136	Alto	**Servidores**	Cámaras IP: Configuración de la cámara	-	-	-	Sí (terceros y propias)
RQ-137	Alto	**Servidores**	Cámaras IP: Conmutación de modos por temporizador	-	-	-	Integrado en cámaras propias, no definido para terceros
RQ-138	Alto	**Servidores**	Cámaras IP: control PTZ	-	-	-	Sí (terceros y propias) con SVC
RQ-139	Alto	**Servidores**	Cámaras IP: Control remoto	-	-	-	Sí (terceros y propias) función Premote-HD
RQ-140	Alto	**Servidores**	Cámaras IP: Detección de movimiento	-	-	-	Sí (terceros y propias)

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-141	Alto	**Servidores**	Cámaras IP: Escaneo de red	-	-	-	Sí (solo para propias), IP Finder
RQ-142	Alto	**Servidores**	Cámaras IP: Función de búsqueda	-	-	-	Sí (terceros y propias) función SmartFinder
RQ-143	Alto	**Servidores**	Cámaras IP: Grabación de audio	-	-	-	Sí (terceros y propias) formato G.711
RQ-144	Alto	**Servidores**	Cámaras IP: Grabación de flujos en multicast	-	-	-	Sí (solo para propias)
RQ-145	Alto	**Servidores**	Cámaras IP: Modos integrados (para cámaras de terceros)	-	-	-	Temporizador, Permanente, Contacto, Movimiento y Movimiento/contacto
RQ-146	Alto	**Servidores**	Cámaras IP: Modos integrados (para cámaras propias)	-	-	-	Temporizador, Permanente, Contacto, Movimiento y Movimiento/contacto
RQ-147	Alto	**Servidores**	Cámaras IP: Protocolo de comunicación	-	-	-	RTSP (para terceros) DaVid (para propias)
RQ-148	Alto	**Servidores**	Cámaras IP: Protocolo de transporte	-	-	-	RPT via UDP (para terceros) TCP (para propias)
RQ-149	Alto	**Servidores**	Cámaras IP: Proxy de video	-	-	-	Sí (terceros y propias)
RQ-150	Alto	**Servidores**	Cámaras IP: Servidor DMVC	-	-	-	Sí (terceros y propias)
RQ-151	Alto	**Servidores**	Cámaras IP: Streamer multicast	-	-	-	Sí (terceros y propias) via SeMSy
RQ-152	Alto	**Servidores**	Certificados	-	-	-	CE, FCC, ACA, UL, DIN 50130-4
RQ-153	Alto	**Servidores**	Conexiones: AUX/line (1), micrófono (2) y audio (3)	-	-	-	Conector Jack 3,5mm (1,2,3), (2 y 3) por interfono con licencia
RQ-154	Alto	**Servidores**	Conexiones: Entradas de contacto	-	-	-	x4 con aislamiento galvánico, interruptor/pulsador 4 funciones por contacto
RQ-155	Alto	**Servidores**	Conexiones: Ethernet	-	-	-	RJ45 (10/100/1000 Mbps), (x2 con licencia requerida)
RQ-156	Alto	**Servidores**	Conexiones: Interfaz SATA	-	-	-	Tarjeta controladora RAID para ampliación JBOD
RQ-157	Alto	**Servidores**	Conexiones: Periféricos	-	-	-	Ratón y teclado
RQ-158	Alto	**Servidores**	Conexiones: Salida de video	-	-	-	DisplayPort dP 1.2/DVI (solo para configuración)
RQ-159	Alto	**Servidores**	Conexiones: Salidas de relé	-	-	-	x4 con aislamiento galvánico, 12V DC/ 14V AC, 0,5A, 150mOhm normalmente abierto/cerrado
RQ-160	Alto	**Servidores**	Conexiones: USB trasera (1) y frontal (2)	-	-	-	(1) 3.0 tipo A x2, 2.0 tipo A x6 (2) 2.0 tipo A
RQ-161	Alto	**Servidores**	Contactos de red	-	-	-	Ethernet I/O MOXA ioLogik E1210/E1212/E1214
RQ-162	Alto	**Servidores**	CPU, RAM, módulo flash, ventilador	-	-	-	Multi-core, 16GB, 8GB, 3 (velocidad de giro automática)
RQ-163	Alto	**Servidores**	Dimensiones y peso	-	-	-	483x133x533 mm, 20Kg (con los 8 HDD)
RQ-164	Alto	**Servidores**	Granulación (partición) de los datos	-	-	-	RAID 6
RQ-165	Alto	**Servidores**	Licencia de integración VMS	-	-	-	SeMSy
RQ-166	Alto	**Servidores**	Módulo flash separado (1), discos duros opcionales (2)	-	-	-	Sí (1), sí (2) hasta 72 TB en RAID 6
RQ-167	Alto	**Servidores**	Montaje de los HDD	-	-	-	Pruebas de función, largo plazo y final, aceptación y autorización incluidas

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-168	Alto	**Servidores**	Número de canales de grabación	-	-	-	Hasta 100 (HD y en tiempo real)
RQ-169	Alto	**Servidores**	Número de discos HDD	-	-	-	8 (8x3,5") ampliable con JBOD
RQ-170	Alto	**Servidores**	Potencia (consumo y térmica)	-	-	-	230W y 785 BTU/h (máximos)
RQ-171	Alto	**Servidores**	Protocolos de comunicaciones	-	-	-	DaVid, DaVidS, HTTP, HTTPS, DNS, DHCP, LDAP, RTSP, RTP, RTCP, SNMP (v1, v2c)
RQ-172	Alto	**Servidores**	Protocolos de Ethernet	-	-	-	IPv4, UDP y TCP En preparación: IPv6, UDPv6 y TCPv6
RQ-173	Alto	**Servidores**	Rango de humedad	-	-	-	5-70% RH, sin condensación
RQ-174	Alto	**Servidores**	Resolución soportada	-	-	-	Hasta 12 MPx (depende de la cámara)
RQ-175	Alto	**Servidores**	Rieles de montaje	-	-	-	De 19" (incluidos)
RQ-176	Alto	**Servidores**	Software de gestión (1) y configuración (2) externos	-	-	-	(1) Propio para el cliente de video, DMVC opcional (2) Pservice 3
RQ-177	Alto	**Servidores**	Tasa máxima de bits	-	-	-	Hasta 400Mbps
RQ-178	Alto	**Servidores**	Temperatura y temperatura recomendada	-	-	-	+5 hasta +40 ºC +20 hasta +25 ºC
RQ-179	Alto	**Usuarios**	Protección del acceso al servidor de grabaciones	Mediante un token de limitación de sesión y comunicaciones encriptadas con el cliente de acceso	Mediante huella de tiempo y usuario, se Limitan y el acceso y registro	-	-
RQ-180	Alto	**Usuarios**	Acceso remoto a un servidor de grabación	Sí, mediante redireccionamiento de puertos desde fuera del firewall de la NAT	Sí, desde el nodo principal a los sites federados y viceversa	-	-
RQ-181	Alto	**Usuarios**	Acceso y autenticación a los clientes	Se valida el usuario y contraseña, o la integración LDAP en el servidor de gestión	Mediante directorio Activo de Microsoft, credenciales, usuario local de Windows o verificación en dos pasos	Con certificados y firmas digitales. Se garantiza el inicio de sesión único	-
RQ-182	Alto	**Usuarios**	Autenticación y autorización	Simple, mediante usuario y contraseña o LDAP, o en dos pasos, el sistema reconoce al usuario pero sólo se inicia sesión si se confirma por un supervisor	Autenticación centralizada para los sites, todos los inicios de sesión pasan por el servidor de gestión central	Basada en comprobaciones mediante tokens, adicionalmente admite reconocimiento facial contrastando con la foto de la autorización	-
RQ-183	Alto	**Usuarios**	Auto log-in	Sí, mediante un usuario propio o el usuario de Windows, restaura automáticamente las vistas	Sí, reutilizando las últimas credenciales utilizadas en el inicio de sesión	Sí, para conectar los Archiver a las unidades de video	-
RQ-184	Alto	**Usuarios**	Colaboración entre usuarios	Compartición de alarmas, imágenes, marcadores, mapas, secuencias… Y entre centros de control	-	-	-
RQ-185	Alto	**Usuarios**	Comunicaciones internas	Se pueden compartir mensajes de texto con el centro de control, de forma manual o automática por eventos o programados (**ver aclaración**)	-	-	-
RQ-186	Alto	**Usuarios**	Derechos de usuario: derechos de administrador	Acceso a configuración general, cámaras, micrófonos, alarmas, grabaciones, sistemas federados, (**páginas 11 y 12**)	Administración de la configuración de los sites en la jerarquía de la arquitectura federada	-	-
RQ-187	Alto	**Usuarios**	Derechos de usuario: gestión y asignación	Se pueden heredar y asignar derechos parcialmente, la gestión es centralizada para todos los usuarios	Se pueden heredar y asignar parcialmente, se definen funciones que se pueden asociar a perfiles, usuarios o grupos	-	-
RQ-188	Alto	**Usuarios**	Derechos de usuario: perfiles de administrador	Se pueden personalizar los derechos de cada administrador para diferenciar distintos perfiles	Se pueden personalizar los derechos de cada administrador para diferenciar distintos perfiles (mediante el cliente de gestión)	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-189	Alto	**Usuarios**	Derechos de usuario: perfiles de usuario	Se pueden definir categorías ajustadas a la habilidad requerida para el puesto	Se registran las actividades llevadas a cabo en los dispositivos por cada perfil, los perfiles se diferencian por derechos y funciones asociadas	-	-
RQ-190	Alto	**Usuarios**	Inicio de sesión	Mediante directorios activos de Windows, cuentas locales de Windows o cuentas básicas propias del sistema	Mediante directorios activos de Windows, cuentas locales de Windows o cuentas básicas	-	-
RQ-191	Alto	**Usuarios**	Niveles de prioridad de usuario	32.000 (para operadores y secuencias PTZ automáticas)	32.000 niveles para el control PTZ de usuarios, secuencias y esquemas de patrulla. Se pueden iniciar sesioes anónimas de control PTZ	De 1 a 254 (mayor-menor)	-
RQ-192	Alto	**Usuarios**	Número de canales de audio	Ilimitado	-	-	-
RQ-193	Alto	**Usuarios**	Número de perfiles de usuario configurables	Ilimitado	Ilimitado	-	-
RQ-194	Alto	**Usuarios**	Operación manual del PTZ	Control mediante prioridad de usuario (pass through)	Control mediante prioridad de usuario	Control mediante prioridad de usuarios, si coinciden se tiene en cuenta el orden de petición	-
RQ-195	Medio	**Almacenamiento**	Arquitectura de los servidores de grabación	De 64 bits (Windows Server 2012 o Windows 10)	De 64 bits	-	-
RQ-196	Medio	**Almacenamiento**	Contenedores de almacenamiento: capacidad	Definida y limitada sólo por el hardware (discos)	Limitada por los sólo por los discos o el límite definido manualmente para cada contenedor	-	-
RQ-197	Medio	**Almacenamiento**	Contenedores de almacenamiento: definición y estructura	El video se almacena en formato propio y cifrado en una base de datos SQL Server cifrada, en cualquier unidad accesible desde el sistema	Se definen como una base de datos viva y una opcional de archivo, pueden almacenarse en el mismo disco o en discos secundarios o unidades de red	-	-
RQ-198	Medio	**Almacenamiento**	Contenedores de almacenamiento: esquemas de archivado	Definen las etapas de archivado del video y el tiempo de retención antes de que sea borrado	Permiten mover BBDD vivas de un contenedor de almacenamiento al almacenamiento de archivo, manteniéndolas disponibles para el software cliente	-	-
RQ-199	Medio	**Almacenamiento**	Contenedores de almacenamiento: funcionalidad	Es posible definir uno o más contenedores, con esquemas de archivado y tiempos de retención individuales	Es posible definir uno o más contenedores, con esquemas de archivado y tiempos de retención individuales	Es posible definir uno o más contenedores, con esquemas de archivado individuales	-
RQ-200	Medio	**Almacenamiento**	Contenedores de almacenamiento: opciones adicionales	Para una cámara o grupos de cámaras se definen esquemas de almacenamiento para seleccionar la calidad, tiempo de retención y data grooming	Permiten "limpiar" el video para reducir su tamaño, modificando la velocidad de fotogramas (FPS) al archivar los datos de video	Los archivos de video se almacenan como archivos G64 en los discos, incluyendo pequeñas secuencias de video	-
RQ-201	Medio	**Almacenamiento**	Control de las unidades de almacenamiento	Directo, desde el propio cliente de gestión	-	Directo, mediante el uso de roles Archiver que controlan las distintas unidades de almacenamiento	-
RQ-202	Medio	**Almacenamiento**	Limitación de la calidad de video en grabaciones	Limitado solamente por hardware (cámaras o decodificadores)	Sin limitación por software	-	
RQ-203	Medio	**Almacenamiento**	Optimización de las propiedades del flujo para el almacenamiento y usos policiales (forenses)	Sí, mediante un flujo dedicado (afecta a resolución, codificación y frame rate)	-	-	-
RQ-204	Medio	**Almacenamiento**	Reducción del tamaño de almacenamiento de los datos	Via data grooming, reduciendo los FPS al mover las grabaciones antiguas de un contenedor a otro	-	-	-
RQ-205	Medio	**Almacenamiento**	Uso de la caché del cliente	Sí, se puede almacenar una copia de seguridad de la configuración necesaria para acceder a los grabadores	Sí, sirve como backup ante la caida del gestor	Sí, de las cámaras visualizadas, permite reducir el uso de ancho de banda de la red	-
RQ-206	Medio	**Arquitectura**	Almacenamiento en la nube	Sí, es posible instalar los servicios de video en la nube, AWS, Azure o la nube privada de Siemens	Sí, para sites se admite que el software resida en My Cloud Surveillance de Western Digital serie NAS	Sí, se pueden transferir archivos a la nube o que las cámaras graben directamente ahí	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-207	Medio	**Arquitectura**	Archivado (almacenamiento) auxiliar de video	Sí, es posible utilizar sistemas NAS u otros para almacenar archivos históricos o exportaciones	Sí, almacenamiento secundario de medios para ordenar video, audio y metadatos más allá del periodo inicial de retención.	Sí, crea copias extra de las cámaras seleccionadas, pueden tener distintos parámetros de las grabaciones normales	Sí
RQ-208	Medio	**Arquitectura**	Cliente de reproducción: edición de exportaciones	Sí, se dispone de herramientas de refinado para las exportaciones, en formato Windows (AVI, MPG, MKV...) o formato propio cifrado y con marca de tiempo	Sí, es posible incluir secuencias de video de intervalos de tiempo diferentes o sobrepuestos de diferentes cámaras en una misma exportación	-	-
RQ-209	Medio	**Arquitectura**	Cliente de reproducción: soporte de cámaras analógicas	Sí, mediante el uso de codificadores de video (de-interlacing)	-	Sí (necesita de un decodificador)	-
RQ-210	Medio	**Arquitectura**	Cliente de video: compatibilidad playback (reproducción) y video en vivo	Sí, no es necesario cerrar uno y abrir el otro	-	-	-
RQ-211	Medio	**Arquitectura**	Cliente de video: opciones de zoom	Zoom digital en vivo y para grabaciones	Zoom digital en vivo y para grabaciones	Zoom digital en vivo y para grabaciones	-
RQ-212	Medio	**Arquitectura**	Cliente de video: reproducción en vivo sin espacio de grabación	Sí	-	-	-
RQ-213	Medio	**Arquitectura**	Cliente de video: sincronización de video	Automática, tanto para video vivo como playback	-	Manual, el layout seleccionado marca el tipo de video (vivo o grabado) a reproducir, precisión de milisegundos	-
RQ-214	Medio	**Arquitectura**	Cliente de video: visualización de metadatos	Mediante el display de un cuadro de texto, diponible en video vivo y playback	Mediante el display de un cuadro de texto, diponible en video vivo y playback	-	-
RQ-215	Medio	**Arquitectura**	Cliente móvil: opciones de audio	Es posible transmitir y recibir audio con el dispositivo móvil mediante la función de Video Push	-	-	-
RQ-216	Medio	**Arquitectura**	Cliente móvil: sistema operativo de los dispositivos móviles	Android 5.0 o superior y iOS 9.3 o superior	Andrioid o iOS	-	-
RQ-217	Medio	**Arquitectura**	Cliente web: adquisición	Incluido con el servidor móvil	-	-	-
RQ-218	Medio	**Arquitectura**	Cliente web: inicio de sesión	Mediante usuario y contraseña o directorio activo de Windows	Mediante usuario y contraseña, admite verificación en dos pasos, mediante el servidor móvil. Lo mismo para el cliente móvil	-	-
RQ-219	Medio	**Arquitectura**	Control de cámaras PTZ: prioridades y uso reservado	El control PTZ se gestiona mediante permisos y prioridades manual o automáticamente mediante reglas, siendo la prioridad el criterio más restrictivo	El control PTZ permite el control manual, activar preposicionamientos, cambiar prioridades, o bloquear preposicionamientos	-	-
RQ-220	Medio	**Arquitectura**	Control de cámaras PTZ: uso simultáneo por varios usuarios	No, pero se informa a los segundos usuarios de que ya está siendo utilizado o de que no se dispone de la prioridad suficiente	-	-	-
RQ-221	Medio	**Arquitectura**	Funcionalidades PTZ	Pausa automática ante eventos, retoma de la secuencia o patrulla ante timeouts de una sesión (retorno a posición home)	Pausa automática ante eventos, se retoma la secuencia después del timeout de la sesión y/o el margen de control ante eventos	-	-
RQ-222	Medio	**Arquitectura**	Idiomas disponibles	Hasta 29 en el sistema, 14 en el cliente de gestión (**ver aclaración**)	Entre 4 y 30 dependiendo del cliente y la funcionalidad (**página 19**)	Francés o inglés en el cliente móvil, no se especifican más	Español, inglés, alemán, italiano (+ bajo pedido)
RQ-223	Medio	**Arquitectura**	Mapas: detección de errores, alarmas o eventos	Mediante indicadores con un código de color, se distinguen tres categorías, alarmas, avisos y errores, se pueden desactivar para un dispositivo concreto	-	-	-
RQ-224	Medio	**Arquitectura**	Mapas: funcionamiendo offline	Sí, se guardan copias locales	-	-	-
RQ-225	Medio	**Arquitectura**	Protocolo de autenticación	Autenticación Kerberos	Autenticación Kerberos	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-226	Medio	**Arquitectura**	Preposicionamientos automáticos	Sí (ante fallos, eventos, alarmas o programados)	Sí (ante eventos o programados)	-	-
RQ-227	Medio	**Arquitectura**	Propagación de informes de estado y reportes de evento por el sistema	Sí (permite la detección proactiva de errores)	Sí (permite la detección proactiva de errores)	-	-
RQ-228	Medio	**Arquitectura**	Reglas y configuraciones del sistema	Ilimitadas, similar a Microsoft Outlook. Del tipo evento, elementos o reacción ante evento para realizar acciones de forma automática	Ilimitadas, similar a Microsoft Outlook, motor dedicado	-	-
RQ-229	Medio	**Arquitectura**	Restauración y copias de seguridad del sistema	Manual, incluye las configuraciones del sistema, mapas, alarmas, vistas de cliente…	Manual, permite recuperar toda la información de configuración del sistema y dispositivos (**página 24**)	-	-
RQ-230	Medio	**Arquitectura**	Servidor móvil: capeado	Transcodificación del video en H264/5 a MJPEG y ajustando la resoclución para limitar el ancho de banda y el consumo de proceso en la decodificación en el móvil	-	-	-
RQ-231	Medio	**Arquitectura**	Servidor móvil: redundancias	Se pueden instalar varios en paralelo para actuar en caso de fallo o para admitir más usuarios	-	-	-
RQ-232	Medio	**Arquitectura**	Soporte SNMP o TRAP	Sí, ambos	SNMP	-	
RQ-233	Medio	**Datos**	Exportaciones: formato de audio	WAV, MKV o AVI, y cualquier formato del que existan codecs en el servidor de gestión, incluyendo al formato propio	AAC, G711 y G726	-	-
RQ-234	Medio	**Datos**	Transmisión y grabación de audio desde micrófonos/altavoces conectados	Sí, full o half duplex para transmisión en un cliente, half duplex para la grabación de audio	-	-	
RQ-235	Medio	**Dispositivos**	Conexión de cámaras mediante HTPPS	Sí	Sí	-	-
RQ-236	Medio	**Dispositivos**	Configuración de acciones por evento	Si se produce VMD con buffers pre y post	Principalmente inicio/parada de grabaciones, cambios de cámara y/o preposicionamiento, notificaciones… (**página 29**)	-	-
RQ-237	Medio	**Dispositivos**	Escaneo de PTZ	Sí (sólo si el hardware lo admite)	-	-	-
RQ-238	Medio	**Dispositivos**	Protección contra sabotajes	Solamente la que traiga la propia cámara	-	-	Detección y aviso de cubrimiento, desenfoque y rotación de cámaras
RQ-239	Medio	**Dispositivos**	Secuencias de cámaras/PTZ: configuración horaria (a lo largo del día)	Se pueden definir esquemas de patrulla con horario propio para cada cámara (P-ej dia/noche/fin de semana)	-	-	
RQ-240	Medio	**Dispositivos**	Secuencias de cámaras/PTZ: opciones de configuración	Tiempo ajustable entre saltos y transiciones, se puede desactivar el VMD para evitar falsas alarmas, todos los ajustes se realizan en el cliente de gestión	Tiempo ajustable entre saltos y transiciones, se puede desactivar el VMD para evitar falsas alarmas, se pueden asignar perfiles temporales	Se pueden combinar secuencias si se activan dos en la misma vista, se detienen ante el control de PTZ y se desactivan si falla una cámara	-
RQ-241	Medio	**Evento/fallo**	Alarmas: compatibilidad de procesos entre sistemas de seguridad	Sí, gestionada por las reglas del sistema	-	-	-
RQ-242	Medio	**Evento/fallo**	Alarmas: documentación (generación de informes)	Se pueden crear reportes de alarma sobre incidentes	Se pueden guardar comentarios asociados al tiempo en el que se produjo la alarma dentro del report	-	-
RQ-243	Medio	**Evento/fallo**	Alarmas: Estructura de gestión	Centralizada, todas las alarmas internas o externas pasan por el mismo servidor en el que se aplican las reglas y se distribuyen a los clientes	Centralizada, todas las alarmas, internas o externas pasan por el nodo central	-	-
RQ-244	Medio	**Evento/fallo**	Alarmas: estructura lógica del sistema	Utiliza soporte de Microsoft Clustering para el servidor de eventos que reside en el servidor de gestión	-	-	-
RQ-245	Medio	**Evento/fallo**	Alarmas: informes asociados	Se guardan reports con el origen y la gestión realizada	Se guardan reports con el origen y la gestión realizada	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-246	Medio	**Evento/fallo**	Alarmas: localización por parte de los usuarios	Se pueden enlazar las alarmas con la posición en un mapa de forma que se visualice sobre éste	Se pueden enlazar las alarmas con la posición en un mapa de forma que se visualice sobre éste	-	-
RQ-247	Medio	**Evento/fallo**	Alarmas: notificaciones sonoras	Sí, modificables para que sigan la jerarquía o prioridad de la alarma producida o para que no solapen otras	Sí, modificables para que sigan la jerarquía o prioridad de la alarma producida, se pueden configurar para que emitan archivos .wav	-	-
RQ-248	Medio	**Evento/fallo**	Analísis de video	Sí	Sí	Sí	Sí
RQ-249	Medio	**Evento/fallo**	Comportamiento del servidor de gestión ante fallos	Conmutación via Windows Server Clustering, Vmware o Hyper-V	Conmutación via Microsoft Windows failover Cluster	-	-
RQ-250	Medio	**Gestión**	Monitoring wall: configuración layouts-monitores	Se puede controlar el tamaño de la cuadricula para cada layout configurado en un monitor	-	Se puede configurar la disposición de los layouts para que coincida con la de los monitores	-
RQ-251	Medio	**Usuarios**	Derechos de usuario: funciones asociadas	Se pueden ajustar las funciones principales o secundarias asignadas a roles (perfiles) concretos (**ver aclaración**)	Se concede acceso a video, audio, metadatos y otros recursos de los sites	-	-
RQ-252	Bajo	**Almacenamiento**	Almacenamiento local en dispositivos	Sí (función Edge Storage), se puede activar manualmente, por horario o por evento	Sí (función Edge Storage) con grabaciones sincronizadas, con distinta calidad y volcado manual o automático (SQVR) (**página 42**)	Sí (función Edge Recording), la transferencia al sistema se realiza de forma manual, por horario o por evento	Sí, (función EdgeStorage y SmartBackfill)
RQ-253	Bajo	**Almacenamiento**	Supervisión de la capacidad disponible	Sí, mediante un menú dedicado, del espacio usado y espacio disponible total e individualizado para cada cámara	Sí, acceso al espacio y memoria disponibles, uso de CPU tiempo de retención y espacio usado por cámaras y servidores	Sí, del espacio usado y disponible para cada unidad de almacenamiento	-
RQ-254	Bajo	**Arquitectura**	Activación (simulación) manual de eventos	Sí, opción de "simular evento", sirve para probar las reglas de comportamiento asociadas a eventos desde el cliente de gestión	-	-	-
RQ-255	Bajo	**Arquitectura**	Almacenamiento de las configuraciones y los informes (logs)	En una base de datos SQL de Microsoft, accesible sólo desde el servidor de gestión	En un servidor SQL, sirve como BBDD para el servidor de gestión, el servidor de eventos y el servidor de informes. Sincronización en hora y fecha	-	-
RQ-256	Bajo	**Arquitectura**	Asignación cámaras-layouts	Arrastrando las cámaras a las vistas desde el cliente de video hasta el monitoring wall. Se pueden configurar asignaciones automáticas por defecto	Arrastrando las cámaras desde el cliente de video hasta el monitoring wall	Doble click o arrastrando la cámara	-
RQ-257	Bajo	**Arquitectura**	Compromiso de protección de datos	Clausula Copenhage, para definir el comportamiento ético de la empresa en lo referente a videovigilancia y sistemas abiertos	-	-	-
RQ-258	Bajo	**Arquitectura**	Cliente de gestión: funcionalidades	Permite administrar servidores de grabación, dispositivos, las reglas y el logging	Permite administrar todas las partes del VMS, pensado para ejecutarse en el ordenador de un administrador	-	-
RQ-259	Bajo	**Arquitectura**	Cliente de reproducción: opciones de control de la reproducción de grabaciones	Reproducción frame a frame, ajuste de velocidad (x1,x2,x4,x8…) por evento o alarma, VMD o yendo a la fecha deseada	Velocidad de reproducción, navegación frame a frame, por secuencias, búsqueda por fecha	Avance, retroceso, play/pause, conmutación a live view y acceso a imágenes en miniatura	-
RQ-260	Bajo	**Arquitectura**	Cliente de reproducción: opciones de reproducción	Video y audio archivado, incluyendo exportaciones	Grabaciones, video archivado, audio y exportaciones. Mediante lineas temporales (**página 37**)	-	-
RQ-261	Bajo	**Arquitectura**	Cliente de reproducción: visualización de metadatos	Sí, los que estén sincronizados con las exportaciones, aparecen en cuadros de texto	-	-	-
RQ-262	Bajo	**Arquitectura**	Cliente de video: gestión del almacenamiento de las visualizaciones	Asignación centralizada desde el servidor de gestión	-	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-263	Bajo	**Arquitectura**	Cliente de video: asignación de vistas-cámaras	Arrastrando el icono sobre la vista	Arrastrando el icono sobre la vista	-	-
RQ-264	Bajo	**Arquitectura**	Cliente de video: atajos de teclado	Permiten seleccionar ventanas específicas o cámaras específicas dentro de una ventana y preposicionamientos PTZ mediante joysticks o teclado	Permiten el acceso directo al cliente, selección de ventanas o cámaras y layouts	-	-
RQ-265	Bajo	**Arquitectura**	Cliente de video: búsqueda de cámaras	Filtros por cámara, tipo de cámara o vista. Se pueden crear vistas temporales de todas las cámaras que coincidan con el criterio de búsqueda	Filtros por cámara, tipo de cámara o vista, marcadores, por detección de movimiento, opción de previsualizar la secuencia búscada	-	-
RQ-266	Bajo	**Arquitectura**	Cliente de video: búsqueda de grabaciones para reproducción	Mediante una linea temporal (simple o avanzada). Se puede previsualizar las grabaciones manuales y marcadores (**página 15**)	Mediante una linea temporal (simple o avanzada). Se puede previsualizar las grabaciones manuales y marcadores sobre dicha linea	Mediante marcadores, por detección de movimiento o por fecha y hora	-
RQ-267	Bajo	**Arquitectura**	Cliente de video: grabaciones manuales, características	Una vez iniciada, el estado de la grabación es accesible para todos los usuarios activos en el sistema	Es necesario definir un tiempo máximo a partir del cual la grabación se detiene automáticamente	-	-
RQ-268	Bajo	**Arquitectura**	Cliente de video: importación de mapas	Admite importación de mapas HTML estáticos o activos	Es compatible con los servicios de mapas de Bing, Google y OpenStreet (mapas GIS)	-	-
RQ-269	Bajo	**Arquitectura**	Cliente de video: interfaz (I)	Pestañas dedicadas para el explorador de secuencias, gestor de alarmas, monitor del sistema, visualización en vivo y playback	Pestañas de reproducción en vivo, explorador de secuencias, pestaña de acceso al gestor de alarmas, se pueden añadir y modificar más	-	-
RQ-270	Bajo	**Arquitectura**	Cliente de video: interfaz (II)	Personalización del color (tema), claro u oscuro	-	-	-
RQ-271	Bajo	**Arquitectura**	Cliente de video: opciones básicas de búsqueda de grabaciones	Por tiempo/fecha, por actividad o evento, por detección de movimiento. SmartSearch	Por tiempo/fecha, metadatos o VMD, búsqueda inteligente para ignorar zonas dentro de la vista de una cámara	-	BBDD VCA para cámaras propias. Función SmartFinder
RQ-272	Bajo	**Arquitectura**	Cliente de video: selección de cámaras para reproducción de grabaciones	Mediante búsqueda filtrada o arrastrando el icono a la ventana de playback	-	-	-
RQ-273	Bajo	**Arquitectura**	Cliente de video: uso de ventanas (I)	Las ventanas secundarias tienen funcionalidad completa, pueden funcionar de forma independiente o de forma sincronizada con la principal	Las ventanas secundarias tienen funcionalidad completa, pueden funcionar de forma independiente o de forma sincronizada con la principal	-	-
RQ-274	Bajo	**Arquitectura**	Cliente de video: uso de ventanas (II)	Soporta una ventana principal y un número ilimitado de ventanas secundarias flotantes o maximizadas	-	-	-
RQ-275	Bajo	**Arquitectura**	Cliente móvil: acceso a múltiples servidores/sites	Sí, se pueden añadir credenciales propias para cada usuario (de Windows o local)	Sí, mediante distintos perfiles asignados a cada uno de los servidores o sites	-	-
RQ-276	Bajo	**Arquitectura**	Control de cámaras PTZ: control manual vs sistemas de patrulla	Es posible tomar el control de una cámara mientras patrulla, después de un tiempo de inactividad retoma la patrulla automáticamente	Es posible tomar el control de una cámara ante eventos, o solicitudes de alta prioridad después de un tiempo de inactividad retoma la patrulla automáticamente	-	-
RQ-277	Bajo	**Arquitectura**	Control de cámaras PTZ: mecanismos de control PTZ	Mediante preposicionamientos, point-and-click, joystick virtual o botones widget (overlay)	Mediante teclado, joysticks, ratón, botones virtuales para los preposicionamientos	Mediante teclados generales o específicos para CCTV, point-and-click o widgets	-
RQ-278	Bajo	**Arquitectura**	Control de cámaras PTZ: opciones adicionales	Zoom PTZ a un rectángulo definido	Zoom PTZ a un rectángulo definido, reserva del control a un usuario, consulta de quién utiliza el control y el tiempo al que se limita ese control	Zoom a un rectángulo definido, centrado con un click, widgets, se pueden definir valores predeterminados de zoom digital	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-279	Bajo	**Arquitectura**	Control de cámaras PTZ: visualización en 360º	Sí (soporta cámaras "ojo de pez" 1x2 o 2x2). (**página 15**)	Sí (soporta cámaras "ojo de pez") mediante ImmerVision	Sí (soporta cámaras "ojo de pez"), se puede corregir la distorsión mediante zoom (**página 181 MU**)	-
RQ-280	Bajo	**Arquitectura**	Creación de marcadores (indicadores)	Manuales, programadas o por evento	Manuales o programadas	Manuales	-
RQ-281	Bajo	**Arquitectura**	Direccionamiento de los servidores (addresing)	IPv4 y IPv6, incluyendo multicast	IPv4 y IPv6	IPv4 y IPv6	-
RQ-282	Bajo	**Arquitectura**	Display en monitores de redes federadas o sites interconectados	Sí, Mediante control manual o automático	-	-	-
RQ-283	Bajo	**Arquitectura**	Enrutamiento del tráfico (demanda) entre cámaras y clientes	Para video vivo, grabaciones y exportaciones	-	-	-
RQ-284	Bajo	**Arquitectura**	Estructura de la red, gestión de los servidores	Centralizada o distribuida (federada)	Centralizada o distribuida (basada en componentes para garantizar la escalabilidad)	Centralizada o distribuida	-
RQ-285	Bajo	**Arquitectura**	Gestor del servidor de grabaciones: funcionalidades	Muestra mensajes de estado, inicio/parada del servicio y modificaciones en la configuración de la red, estado de dispositivos, disco, memoria y CPU	-	-	-
RQ-286	Bajo	**Arquitectura**	Mapas: interacción con los layouts	Se pueden arrastrar las cámaras sobre el mapa hasta un layout	Se pueden arrastrar las cámaras sobre el mapa hasta un layout o Video wall	-	-
RQ-287	Bajo	**Arquitectura**	Mapas: formatos de mapa soportados	JPG, GIF, PNG, TIF y mapas multicapa	BMP, GIF, JPEG, JPG, PNG, TIF, TIFF y WMP	-	-
RQ-288	Bajo	**Arquitectura**	Mapas: funcionalidad PTZ	Se pueden mostrar las zonas de visión de cámaras, al clickar sobre ellas se pueden controlar las cámaras PTZ	Se puede representar la vista de campo de las cámaras y seleccionar preposicionamientos desde el mapa	-	-
RQ-289	Bajo	**Arquitectura**	Mapas: funcionalidades	Vista general del sistema y acceso a todos los componentes del sistema	Vista general del sistema y acceso a todos los componentes del sistema, pueden ser estáticos o dinámicos	-	-
RQ-290	Bajo	**Arquitectura**	Mapas: información mostrada de los sistemas	Para cámaras y servidores, resolución, FPS, uso de la red y espacio en disco, configurable	Para cámaras y servidores, resolución, FPS, uso de red espacio de disco.	-	-
RQ-291	Bajo	**Arquitectura**	Mapas: interacción con dispositivos (cámaras + otros)	Mediante mecanismos de drag and drop y point and click (**página 17**). Control integrado de puertas, luces y CCAA	Mediante función smart Maps para mostrar la ubicación geográfica de las cámaras dentro de los emplazamientos. Escucha y conversación mediante los dispositivos de audio	-	-
RQ-292	Bajo	**Arquitectura**	Mapas: interacción con las cámaras	Previsualización al poner el ratón sobre una, se pueden mostrar todas las cámaras sobre el mapa con un click	Mediante un icono y un cono que indica la visión, con previsualización al posar el ratón encima y control PTZ integrado	-	-
RQ-293	Bajo	**Arquitectura**	Mapas: jerarquía	Sí, la monitorización también la sigue. Por ejemplo, Parcela Edifico - Planta -Estancia..	Sí, función Smart Maps (**página 41**)	-	-
RQ-294	Bajo	**Arquitectura**	Mapas: monitorización del estado de los sistemas	En tiempo real, se incluyen cámaras, servidores y dispositivos I/O mediante códigos de color para el estado	En tiempo real, mediante indicadores con código de color	-	-
RQ-295	Bajo	**Arquitectura**	Mapas: personalización	Se pueden editar los nombres (alias) de los dispositivos y añadir referencias	Se pueden editar los nombres (alias) de los dispositivos y añadir referencias (descripciones)	-	-
RQ-296	Bajo	**Arquitectura**	Mapas: regiones	Se pueden crear infinitas regiones para los distintos niveles (calle, edificio, habitación…)	Se pueden definir distintos niveles o regiones para transicionar de un mapa a otro	-	-
RQ-297	Bajo	**Arquitectura**	Mapas: visualización de las cámaras	Mediante una ventana flotante hasta un máximo de 25 ventanas, una por cámara	Mediante una ventana flotante hasta un máximo de 25 cámaras	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-298	Bajo	**Arquitectura**	Marcadores: búsqueda y visualización	Directamente desde el timeline de búsqueda, se pueden listar y previsualizar al buscar grabaciones	-	Mediante la tarea de búsqueda propia, se puede filtrar por texto, tiempo o cámara. Arrastrar un marcador a un layout visualiza el video asociado	-
RQ-299	Bajo	**Arquitectura**	Marcadores: creación	Manual o automática, simple o detallada mediante función bookmark o programadas por reglas, aplicable a cualquier tramo de grabación	-	Mediante widget, se abre un cuadro de texto opcional	-
RQ-300	Bajo	**Arquitectura**	Marcadores: opciones adicionales	Se pueden añadir marcadores en los reportes de incidentes. Se pueden editar, comentar y exportar junto a las grabaciones	-	Añadir un marcador inicializa la grabación de video, al añadir un marcador a una exportación sólo se guarda en ésta	-
RQ-301	Bajo	**Arquitectura**	Monitoring wall: reproducción de grabaciones	Sí, desde el cliente de video un usuario autorizado puede asignar una reproducción (playback) a los monitores	-	-	-
RQ-302	Bajo	**Arquitectura**	Monitorización del sistema	Mediante función System Monitor, (**página 18**)	Mediante el panel de control del sistema	-	-
RQ-303	Bajo	**Arquitectura**	Monitorización del sistema: datos disponibles	Documentación total o parcial de la configuración del sistema, y sites específicos. Configuración de indicadores de rendimiento, alarmas, espacio libre etc.	Estado de las cámaras y servidores, uso de CPU, memoria disponible, espacio libre, tiempos de retención, FPS, espacio usado etc.	-	-
RQ-304	Bajo	**Arquitectura**	Monitorización del sistema: informes, reports, logs…	Via función System Monitor, provee informes de uso, históricos, capacidad disponible, uso de la red e informes de performance de las cámaras	Via función monitor, los usuarios pueden definir informes específicos de la configuración del sistema, con notas libres y personalizables	Se pueden añadir fragmentos de video tanto a los informes como a las alarmas y eventos	-
RQ-305	Bajo	**Arquitectura**	Opciones de búsqueda de archivos en el sistema	Secuencias guardadas, marcadores y grabaciones en una o múltiples cámaras al mismo tiempo	Secuencias guardadas, marcadores y grabaciones, alarmas, detección de movimiento, fecha, cámara y site	-	-
RQ-306	Bajo	**Arquitectura**	Opciones de la pared de monitores (monitoring wall)	Acceso a layouts predefinidos, configuración de layouts y contenido (vista) de las cámaras, desde otro cliente y ante eventos o alarmas	Acceso a layouts predefinidos, configuración de layouts y contenido de las cámaras arrastrandolas sobre la vista o monitor correspondiente	-	-
RQ-307	Bajo	**Arquitectura**	Operación centralizada geográficamente dispersa	Sí (solamente compatible con software del mismo tipo)	Sí	-	-
RQ-308	Bajo	**Arquitectura**	Perfiles temporales: opciones adicionales	Es posible definir perfiles que funcionen según las horas diarias de luz solar, definida una posición GPS para tener en cuenta amanecer y anochecer	Es posible definir perfiles que funcionen según las horas diarias de luz solar, definida una posición GPS. (**página 30**)	-	-
RQ-309	Bajo	**Arquitectura**	Previsualización de secuencias de video	Sí, la reproducción es automática y se pueden exportar directamente	Sí, la reproducción es automática y se pueden exportar directamente	-	-
RQ-310	Bajo	**Arquitectura**	Adaptación automática de flujo(s) de una cámara	Sí (**ver aclaración**)	-	Sí (ajusta la calidad automáticamente en función del tamaño de la cuadrícula de visualización)	-
RQ-311	Bajo	**Arquitectura**	Servidor de gestión: compatibilidad con Windows	Ejecución como Windows service, mediante cuentas de administrador locales, del dominio o cuentas del sistema	-	-	-
RQ-312	Bajo	**Arquitectura**	Servidor móvil: configuración del cliente móvil	No es necesaria, se realiza en el servidor y se descarga en el propio cliente una vez introducido usuario y contraseña	-	-	-
RQ-313	Bajo	**Arquitectura**	Servidor móvil: opciones adicionales	Decoficación acelerada por hardware si el dispositivo lo permite	Métodos de autenticación básica, mediante directorios Activos de Windows o en dos pasos. Función Smart Connect	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-314	Bajo	**Arquitectura**	Servidores de grabación: compatibilidad con Windows	Ejecución como Windows service, mediante cuentas de administrador locales, del dominio o cuentas del sistema	Sí, tanto físicos (UPS) como virtualizados (mediante VMWare o Microsoft Hyper V)	-	-
RQ-315	Bajo	**Arquitectura**	Servidores de grabación: modificaciones en la configuración	Via cliente de gestión, los cambios se aplican instantáneamente sin parar la grabación	-	-	-
RQ-316	Bajo	**Arquitectura**	Servidores de grabación: configuración local	Se guarda una copia local cuando el cliente de gestión no está disponible, para funcionar de forma autónoma hasta que vuelva a estar disponible	-	-	-
RQ-317	Bajo	**Arquitectura**	Servidores de grabación: setup	Descarga e instalación desde la web via servidor de gestión y Windows	-	-	-
RQ-318	Bajo	**Arquitectura**	Sistema operativo	Windows de 64 bits	-	-	Linux
RQ-319	Bajo	**Arquitectura**	Streaming multi-live	Sí, permite definir las propiedades individuales de cada flujo de forma manual o automática para ajustar el flujo de video al tamaño de cada vista del layout	Sí, se alternan las transmisiones de video vivo para optimizar el ancho de banda, en servidores locales y remotos	Sí, se pueden definir distintas configuraciones de flujos de video (en vivo, remoto, grabaciones de alta calidad…) optimizando ancho de banda	-
RQ-320	Bajo	**Datos**	Exportaciones: añadir comentarios	Sí, sólo para el formato propio	Sí, para formato propio y multimedia	-	
RQ-321	Bajo	**Datos**	Exportaciones: opciones adicionales	Es posible juntar grabaciones de distintas cámaras en una misma exportación. Ventana de previsualización. Zoom digital (solamente en formato propio)	Es posible programar la exportación de video de los sites hacia el nodo central. Se pueden exportar secuencias de distintas cámaras simultáneamente	Es posible definir un cuadrante y exportar el video de todas las cámaras que lo visualizan en un único clip	-
RQ-322	Bajo	**Datos**	Metadatos: Estructura de recepción y almacenamiento	Se procesan en los servidores de grabación y se envían a los clientes	-	-	
RQ-323	Bajo	**Dispositivos**	Activación manual de relés	Sí, es posible acceder y activar todas las salidas digitales de los dispositivos conectados mediante reglas definidas en el cliente de gestión	-	-	-
RQ-324	Bajo	**Dispositivos**	Ajuste de la detección de movimiento (VMD)	Manual o automático, se pueden definir zonas de exclusión para evitar falsas alarmas	Manual o automático, se pueden definir zonas de exclusión y grabar con una tasa de FPS distinta a la habitual	-	-
RQ-325	Bajo	**Dispositivos**	Atajos de teclado para cámaras	Sí (se les asigna un número del teclado)	-	-	-
RQ-326	Bajo	**Dispositivos**	Cliente de video: capturas de pantalla	Sí, instantánea, en formato JPEG se puede guardar como archivo o enviar directamente a una impresora	Sí, se pueden guardar o imprimir directamente	Sí, instantánea mediante widget y con vista previa, se guardan como PNG por defecto aunque se puede cambiar a JPEG (**páginas 194-197 MU**)	-
RQ-327	Bajo	**Dispositivos**	Compatibilidad con dispostivos con más de un puerto de input/output	Sí	-	-	-
RQ-328	Bajo	**Dispositivos**	Opciones de ajuste ajuste de parámetros en el video codificado	Ajuste del GOP para MPEG4 y H264, para limitar el número de imágenes entre k-frames	Para MPEG4, H264 y H265 es posible grabar el flujo completo o cuadros (frames) clave. Para MJPEG se puede configurar cualquier valor de FPS	-	-
RQ-329	Bajo	**Dispositivos**	Opciones de ajuste de los parámetros de imagen en cámaras	Brillo, contraste, compresión, bit rate, resolución y rotación para una o varias cámaras simultáneamente	Brillo, color, compresión, tasa de bits, resolución y FPS. Se incluye una función de desentrelazado. Para una o varias cámaras simultáneamente	-	-
RQ-330	Bajo	**Dispositivos**	Tratamiento de los dispositivos sin usar o en mantenimiento	Se pueden activar o desactivar para permitir su desconexión y evitar que salten falsas alarmas	Se pueden activar o desactivar de forma automática para la realización de un mantenimiento	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-331	Bajo	**Dispositivos**	Verificación de los ajustes en las cámaras	Mediante una ventana de previsualización de forma individual o colectivamente tanto para cámaras como para grabadores	-	-	-
RQ-332	Bajo	**Evento/fallo**	Acciones programadas: inicio y parada	Manual o automáticas, activadas por eventos, tiempo o ambos, desactivadas por eventos o después de un cierto tiempo	Manual o automáticas, una sola regla puede iniciar varias acciones programadas	-	-
RQ-333	Bajo	**Evento/fallo**	Alarmas: búsqueda y listado	Previsualización de alarmas en el video vivo y playback, las listas se pueden filtrar mediante una pestaña propia en cada cliente	Previsualización de alarmas en el video vivo y playback, con imágenes relacionadas al instante de la alarma	-	-
RQ-334	Bajo	**Evento/fallo**	Alarmas: clasificaciones	Se pueden definir categorías dependiendo del tipo y naturaleza de la alarma de forma personalizada por los usuarios con permisos para ello	Se pueden definir categorías y prioridades totalmente personalizadas con acciones programadas manuales o automáticas asociadas	-	-
RQ-335	Bajo	**Evento/fallo**	Alarmas: desactivación de las alarmas	Manuales o programadas para que no se activen en determinados periodos u horarios	La desactivación manual permite ignorar alarmas de un dispositivo durante un lapso de tiempo definido	-	-
RQ-336	Bajo	**Evento/fallo**	Alarmas: interacción con los mapas	Permite mostrar y visualizar las alarmas directamente sobre el mapa incluso después de que se haya rearmado	Permite mostrar y visualizar las alarmas directamente y automáticamente sobre el mapa incluso después de que se haya rearmado o desactivado	-	-
RQ-337	Bajo	**Evento/fallo**	Categorías de eventos reconocidas	Que afecten a hardware, dispositivos, grabaciones o externas (**página 11**)	Que afecten a hardware, dispositivos, sites, servidores de grabación, o personalizados (manuales)	-	-
RQ-338	Bajo	**Evento/fallo**	Ejecución de acciones programadas o por eventos	Motor dedicado	Motor dedicado	-	-
RQ-339	Bajo	**Evento/fallo**	Grabaciones bloqueadas: gestión	Búsqueda y filtro de las grabaciones, edición de comentarios modificación del tiempo de retención y anulación del bloqueo (**ver aclaración**)	Búsqueda y filtro de las grabaciones, edición de comentarios modificación del tiempo de retención y anulación del seguro de evidencia	-	-
RQ-340	Bajo	**Evento/fallo**	Grabaciones bloqueadas: opciones adicionales	Se pueden añadir y editar títulos y descripciones para añadir información adicional	Se pueden añadir y editar títulos e información adicional que se guardan como metadatos asociados	Distintos límites de tiempo de duración del bloqueo, una vez finaliza se tienen 24 horas para restaurar el bloqueo antes de borrar	-
RQ-341	Bajo	**Evento/fallo**	Impresión física de informes/reportes	Sí, pueden incluir imágenes, información específica o comentarios del usuario (**ver aclaración**)	Sí, pueden incluir imágenes, información específica o comentarios del usuario	-	-
RQ-342	Bajo	**Evento/fallo**	Monitoring wall: gestión de alarmas	Se pueden definir monitores dentro de un videowall para el envío de alarmas mediante reglas automáticas	-	Se pueden configurar los monitores para recibir alarmas de forma automática, mostrando una descripción	-
RQ-343	Bajo	**Gestión**	Gestión de los informes y reportes (logs)	Se almacenan el servidor SQL Server de gestión, se puede ajustar el tamaño y exportar a clientes	Se pueden identificar por, la hora, la fuente del log, tipo de fuente, usuario, regla, evento etc.	-	-
RQ-344	Bajo	**Gestión**	Gestión de los monitores (monitoring wall)	Se crean y configuran desde el cliente de gestión, la visualización se gestiona desde el cliente de video	-	-	-
RQ-345	Bajo	**Gestión**	Instalación del sistema: cliente de video	Descarga e instalación desde la web en el servidor de gestión. Se guarda un repositorio con todos los clientes actualizados y los instaladores para los servidores	-	-	-

ID	NIVEL DE IMPORTANCIA	CATEGORÍA	DESCRIPCIÓN	SIEMENS	MILESTONE	GENETEC	DALLMEIER
RQ-346	Bajo	**Gestión**	Licencias: Consulta de licencias	Visión general de cada licencia individual de los sites ejecutados en el mismo SLC, desde el cliente de gestión	Visión general de cada licencia individual de los sites ejecutados en el mismo SLC	Ventana dedicada	-
RQ-347	Bajo	**Gestión**	Notificación de actualizaciones	Sí, automático al iniciar sesión	-	-	-
RQ-348	Bajo	**Usuarios**	Aplicación de video: modos disponibles	Modo vivo, modo playback, modo setup, modo alarmas, modo explorador de secuencias y modo supervisión	Modo vivo, modo playback, modo setup y modo explorador de secuencias	-	-
RQ-349	Bajo	**Usuarios**	Aplicación de video: opciones disponibles	Visualizar la hora, cámaras, indicadores, parámetros por defecto, control de los periféricos ...(**página 12**)		-	-
RQ-350	Bajo	**Usuarios**	Derechos de usuario: configuración de los monitores	Sí, se asignan los permisos para ello desde el cliente de gestión	-	-	-
RQ-351	Bajo	**Usuarios**	Derechos de usuario: edición de los mapas	Sí, se asignan los permisos para ello desde el cliente de gestión	-	-	-
RQ-352	Bajo	**Usuarios**	Derechos de usuario: layouts disponibles	Asignados desde la aplicación de gestión	-	-	-
RQ-353	Bajo	**Usuarios**	Derechos de usuario: personalización de la aplicación	Desde la aplicación de gestión se definen qué menús o pestañas deben aparecer a cada usuario o grupo de usuarios	-	-	-