Especificaciones de CathexisVision 2020 A&E

Contenido

1 Introducción

Este documento describe los requisitos generales para el software de gestión de vídeo CathexisVision (que en lo sucesivo se denominará "el VMS") y/o los dispositivos periféricos producidos por Cathexis Technologies y suministrados por los distribuidores de Cathexis en determinadas regiones.[1]

Para cualquier consulta, póngase en contacto con support@cat.co.za.

[1] Aunque Cathexis ha hecho todo lo posible para asegurar la exactitud de este documento, no hay garantía de exactitud, ni explícita, ni implícita. Las especificaciones están sujetas a cambios sin previo aviso.

2 Requisitos generales del sistema

Arquitectura del sistema

2.1.1 El sistema será el sistema de videovigilancia CathexisVision.

2.1.2 El sistema deberá ser de naturaleza empresarial, capaz de gestionar múltiples sitios de forma remota.

2.1.2.1 El sistema deberá proporcionar un cliente completo de configuración y mantenimiento remoto.

2.1.2.2 El sistema no deberá depender de aplicaciones de escritorio remoto para la conexión remota.

2.1.3 El sistema deberá soportar la encriptación para todas las conexiones externas del sitio.

2.1.3.1 El sistema deberá ofrecer cuatro niveles de encriptación:

2.1.3.1.1 Desactivado,

2.1.3.1.2 Mínimo: sólo se cifrarán las conexiones críticas,

2.1.3.1.3 Seguro (por defecto) - se cifrarán todas las conexiones, excepto las de alto volumen de vídeo,

2.1.3.1.4 Todo - todas las conexiones, incluyendo las de alto volumen de video, deben ser encriptadas.

2.1.3.2 El motor de cifrado utilizará openssl (hashes SHA512, DH-RSA efímero con forward secrecy (DH 2048 bits) y cifrado simétrico AES-GCM 128 bits) equivalente a TLS 1.3.

2.1.4 El sistema no necesitará un servidor de gestión dedicado, por lo que requerirá menos hardware.

2.1.5 El sistema no requerirá una base de datos SQL dedicada para el registro.

2.1.6 El sistema será de naturaleza "cliente/servidor" con los siguientes componentes:

2.1.6.1 Servidores de gestión de grabación.

2.1.6.2 Estaciones de visualización y gestión de clientes dentro y fuera de las instalaciones.

2.1.6.3 Clientes de teléfonos móviles/tabletas fuera de las instalaciones.

2.1.6.4 Servidor de gestión de alarmas.

2.1.7 El sistema deberá ser capaz de funcionar en entornos de sistemas operativos Windows (32/64 bits) o Linux.

2.1.8 El sistema deberá ser capaz de funcionar en un entorno de máquina virtual.

2.1.8.1 El sistema deberá ser capaz de funcionar en un entorno de servidor virtual, y tendrá conocimiento del hardware subyacente.

2.1.9 El sistema deberá tener licencia para su uso con la aplicación de varias licencias para todo el sitio.

2.1.9.1 El sistema deberá ser fácilmente ampliable mediante la adición de cámaras IP, integraciones de sistemas de terceros, análisis de vídeo y/o licencias de hardware de sistemas analógicos.

2.1.9.2 El sistema proporcionará ciertas funciones integradas que podrán desbloquearse para su uso con una clave de software, lo que permitirá una rápida activación de las funciones requeridas.

2.1.9.3 El sistema deberá ser fácilmente actualizable a versiones posteriores mediante un CD, una llave USB u otro medio similar.

2.1.10 El sistema deberá ser fácilmente ampliable mediante la adición de servidores de grabación, servidores de visualización y gestión y almacenamiento.

Configuración del sistema

2.1.11 El sistema deberá permitir la conexión remota al sistema a través de ADSL, VPN o cualquier otra fuente de comunicación.

2.1.11.1 El sistema deberá ser capaz de realizar todas las funciones de configuración y visualización a través de esta conexión remota.

2.1.12 El sistema deberá almacenar la configuración completa del sitio en el sitio o fuera de él para recuperarla en caso de fallo del disco duro.

2.1.12.1 El sistema deberá permitir que esta configuración se restablezca fácilmente.

2.1.13 El sistema deberá mantener registros de la actividad de los usuarios.

2.1.14 El sistema deberá permitir la sincronización horaria de todos los subsistemas de un centro.

2.1.15 El sistema deberá gestionar un número ilimitado de entradas y salidas de relé.

2.1.16 El sistema proporcionará asistentes de configuración para añadir y configurar de forma rápida y sencilla determinados dispositivos y objetos, como cámaras, dispositivos integrados, mapas del emplazamiento, etc.

2.1.17 El sistema deberá utilizar el Plug and Play Universal (UPnP) y el descubrimiento de dispositivos ONVIF para descubrir dispositivos IP y recuperar la configuración de dichos dispositivos.

2.1.18 El sistema deberá descargar y almacenar localmente todos los recursos del sitio, mapas y otros parámetros específicos del sitio para garantizar un acceso rápido y la gestión del ancho de banda para las conexiones de clientes remotos. Si se han modificado en el emplazamiento, se volverán a cargar desde el mismo a la conexión del cliente remoto en el momento de la reconexión.

Capacidades de audio y vídeo

2.1.19 El sistema global no debe tener límite en el número de cámaras/vídeos.

2.1.20 El sistema deberá ser un sistema de grabación digital de vídeo/audio y de monitorización remota con capacidad para visualizar, grabar, reproducir, buscar y transmitir simultáneamente tanto vídeo como audio.

2.1.21 El sistema deberá ser verdaderamente híbrido por naturaleza, y deberá ser capaz de soportar las siguientes fuentes de video:

2.1.21.1 Cámaras de vídeo IP.

2.1.21.1.1 Se proporcionará una lista separada de las cámaras IP soportadas, o como se indica en el sitio web de CathexisVision.

2.1.21.2 Codificadores de vídeo IP (Cathexis y de terceros).

2.1.21.3 Sistemas de vídeo analógico Cathexis.

2.1.21.4 Dispositivos compatibles con ONVIF.

2.1.22 Cada servidor de gestión de grabaciones deberá ser capaz de gestionar múltiples flujos de vídeo de cámaras IP, limitados únicamente por la capacidad de procesamiento del hardware y el almacenamiento disponible del sistema local/remoto.

2.1.23 El sistema deberá ser compatible con las conexiones de control de cámaras https cuando las proporcione el fabricante de la cámara.

2.1.24 El sistema deberá ser compatible con el vídeo encriptado cuando lo proporcione el fabricante de la cámara.

3 Transmisión de vídeo y audio

Capacidades generales

3.1.1 El sistema deberá gestionar la transmisión en directo, la grabación y la revisión de vídeo y audio de las distintas fuentes.

Transmisión de vídeo

3.1.2 El sistema deberá ser capaz de gestionar simultáneamente vídeo procedente de tarjetas de vídeo analógicas y de fuentes de vídeo IP.

3.1.3 El sistema deberá ser capaz de gestionar simultáneamente MJPEG, MPEG4, H264, H265 y MxPEG, y una combinación de los mismos, según la capacidad de la cámara.

3.1.4 El sistema deberá ser capaz de gestionar flujos de vídeo Unicast o Multicast.

3.1.5 El sistema deberá ser capaz de dirigir los flujos de vídeo seleccionados a los monitores de vídeo seleccionados, para ver y revisar el vídeo.

3.1.6 El sistema deberá ser capaz de mostrar vídeo en HD o superior cuando sea necesario.

3.1.7 El sistema deberá ser capaz de gestionar flujos dinámicos y seleccionar de forma inteligente el flujo de la cámara en función de la resolución de la pantalla del cliente, del servidor y/o del videowall para mejorar la eficiencia de la visualización en directo y reducir el uso de recursos.

3.1.8 El sistema deberá ser capaz de "transcodificar" los flujos de vídeo a un ancho de banda inferior, para la supervisión fuera de las instalaciones (sujeto a la disponibilidad de flujos de vídeo adecuados y a la capacidad de procesamiento de los servidores de vídeo).

Transmisión de audio

3.1.9 El sistema deberá ser capaz de recibir y almacenar el audio sincronizado de las cámaras con capacidad de audio.

3.1.10 El sistema deberá ser capaz de grabar y reproducir audio y vídeo sincronizados.

3.1.10.1 Suponiendo que la fuente de audio y vídeo esté sincronizada en la cámara, el sistema deberá ser capaz de mantener esta sincronización a menos de 500 milisegundos.

3.1.11 El sistema deberá ser capaz de gestionar el audio bidireccional, desde el sistema hasta un dispositivo IP remoto, o una cámara, con la capacidad de audio pertinente.

3.1.12 El sistema deberá ser capaz de transmitir/almacenar y reproducir un número ilimitado de flujos de audio de cámara.

4 Gestión de usuarios y derechos de acceso

Gestión de usuarios

4.1.1 El sistema deberá ser capaz de gestionar los usuarios del sitio y aplicar todos los usuarios y sus derechos de acceso a todos los servidores del sitio.

4.1.2 El sistema deberá permitir a los administradores configurar los usuarios del sitio y asignar nombres de usuario, niveles de acceso y contraseñas.

4.1.2.1 El sistema deberá tener treinta niveles de usuario, siendo el nivel superior de la jerarquía el 30 y el nivel inferior de la jerarquía el 1.

4.1.3 El sistema permitirá asignar a los usuarios individuales del sitio los derechos para:

4.1.3.1 Ver todos los recursos del sitio.

4.1.3.2 Conectarse remotamente.

4.1.3.3 Cambiar su propia contraseña.

4.1.4 El acceso al sistema se realizará mediante nombre de usuario y contraseña, y todas las acciones del usuario se registrarán con su nombre en un registro de auditoría del operador. Este registro de auditoría deberá ser accesible, imprimible y de acceso controlable.

LDAP/Directorio activo

4.1.5 El sistema deberá soportar la importación de usuarios desde un sistema de gestión de usuarios LDAP (Lightweight Directory Access Protocol) sólo en los sitios Professional y Premium.

4.1.6 El sistema deberá soportar la asignación de derechos de acceso VMS a los usuarios LDAP importados.

4.1.7 El sistema deberá utilizar LDAP para comunicarse con sistemas de gestión de usuarios como Active Directory y OpenLDAP.

4.1.8 El sistema deberá consultar al servidor del sistema de gestión en cada inicio de sesión de un usuario registrado en LDAP para comprobar la validez de las credenciales.

4.1.9 No se permitirán ni validarán los inicios de sesión de usuarios LDAP que utilicen la E/S móvil del sistema o la API.

Derechos de acceso

4.1.10 El sistema deberá ser capaz de limitar la disponibilidad de los recursos del sitio a los usuarios en función de los derechos de acceso que les hayan sido asignados por los administradores.

4.1.11 El sistema deberá permitir a los administradores asignar derechos de acceso a los niveles de usuario, ya sea de forma local o remota.

4.1.12 El sistema deberá restringir el acceso a la pestaña de configuración (en la que se realiza la configuración del sitio, por ejemplo, la configuración, la visualización y el control de las bases de datos, las cámaras, el análisis de vídeo, etc.) únicamente a los usuarios administradores.

4.1.13 El sistema debe permitir a los administradores asignar a los usuarios los siguientes derechos de acceso a los recursos del sitio (como cámaras, entradas/salidas, monitores, etc.):

4.1.13.1 Vista en vivo.
4.1.13.2 Revisión.
4.1.13.3 Control manual de PTZ, opciones de menú de PTZ, establecer preajustes de PTZ, controlar recorridos de PTZ.
4.1.13.4 Escucha de audio.
4.1.13.5 Ocultar zonas de privacidad.
4.1.13.6 Exportar datos.
4.1.13.7 Restablecer el tamper de la cámara.

5 Grabación, archivo y almacenamiento

Grabación

5.1.1 El sistema deberá ser capaz de:

5.1.1.1 Grabar frecuencias de cuadro de más de 30 cuadros por segundo, dependiendo de las capacidades de la cámara.

5.1.1.2 Grabar en varias bases de datos configuradas.

5.1.1.3 Grabaciones iniciadas por el usuario. Los usuarios con los derechos de acceso correctos pueden activar manualmente una grabación.

5.1.1.4 Grabación de eventos. Los eventos pueden configurarse para activar una grabación en la cámara correspondiente.

5.1.1.5 Grabaciones programadas. Las cámaras pueden configurarse para grabar en un horario fijo.

5.1.1.6 Grabación continua. Los dispositivos (como los integrados y las cámaras) se graban continuamente y crean marcadores de tiempo en la grabación.

5.1.1.7 Grabación de movimiento simple. Configurable a través del asistente de configuración de la cámara o por separado.

5.1.1.8 Envejecimiento del vídeo: las secuencias de vídeo de una base de datos pueden transcodificarse a un tamaño reducido y almacenarse durante más tiempo en una segunda base de datos.

5.1.2 El sistema proporcionará una función de grabación de pantalla, que permite la grabación de cualquier pantalla de ordenador conectada a cualquier ordenador Windows/Linux. Esta se grabará en el VMS como si fuera una cámara IP estándar.

Archivo (Exportación)

5.1.3 El sistema deberá ser capaz de las siguientes capacidades de archivo de vídeo:

5.1.3.1 Exportar audio y vídeo desde el software en un formato de vídeo propio, con un reproductor independiente opcional.

5.1.3.2 Marcado de las horas de inicio y fin del video a archivar.

5.1.3.3 Archivar varias cámaras simultáneamente.

5.1.3.4 Todos los metadatos de vídeo visibles en el momento de archivar se conservarán en el archivo.

5.1.3.5 Archivar secuencias seleccionadas de una o varias cámaras en DVD, dispositivos de memoria USB o discos duros locales o remotos en los formatos permitidos por el sistema operativo.

5.1.3.6 Guardar el "reproductor" del archivo junto con el vídeo.

5.1.3.7 Archivar y visualizar archivos que contengan caracteres no ASCII (por ejemplo, árabes).

5.1.3.8 Exportar vídeo de un archivo.

5.1.3.8.1 El sistema debe permitir que el vídeo exportado desde un archivo esté en formato MP4 o de archivo.

5.1.3.8.2 El sistema deberá permitir la selección de cámaras archivadas para ser incluidas en la exportación.

5.1.3.9 El sistema deberá proporcionar la capacidad de realizar un archivo programado como se indica a continuación:

5.1.3.9.1 Archivar las cámaras seleccionadas.

5.1.3.9.2 Archivar sólo un período seleccionado de imágenes grabadas.

5.1.3.9.3 Archivar a una hora del día seleccionada.

5.1.4 El sistema deberá emplear las siguientes características de seguridad en relación con el archivo de vídeo y la exportación de vídeo desde un archivo:

5.1.4.1 La capacidad de archivar deberá ser una característica con derechos de acceso controlados.

5.1.4.2 El sistema deberá permitir a los administradores crear "perfiles de archivo" basados en el nivel de usuario para los que se configuran las contraseñas de archivo y las marcas de agua.

5.1.4.2.1 En función de la contraseña y de las opciones de archivo configuradas en el perfil de archivo correspondiente, el sistema deberá exigir a los usuarios que establezcan una contraseña y/o apliquen una marca de agua al archivar el vídeo.

5.1.4.2.2 Para el procesamiento, y otros fines legales, las imágenes archivadas deberán estar firmadas digitalmente con el identificador único del servidor de archivo original que se pierde si se intenta manipular la imagen.

5.1.4.2.3 El sistema deberá poder restringir la capacidad de exportación de un archivo.

5.1.4.2.3.1 El sistema deberá eliminar la firma del servidor del vídeo exportado desde un archivo en formato MP4.

5.1.5 El sistema deberá ser capaz de revisar el vídeo archivado desde el software, así como desde un "reproductor" de archivos independiente (que puede instalarse de forma autónoma). El sistema deberá ser capaz de las siguientes funciones de revisión de archivos:

5.1.5.1 Búsqueda de archivos en el NVR.

5.1.5.2 Revisión simultánea de todas las cámaras de un archivo multicámara.

5.1.5.3 Revisión de vídeo mediante las herramientas habituales de reproducción de vídeo.

5.1.5.4 Ver todos los eventos del sistema asociados a las cámaras archivadas.

5.1.5.5 Seleccionar plantillas de diseño para mostrar las cámaras archivadas.

5.1.5.6 Exportar instantáneas de vídeo mostrando el nombre de la cámara, la hora, el título de la instantánea y cualquier nota que se desee.

5.1.5.7 Superposición de la imagen de la instantánea exportada, con el nombre de la cámara y la hora. El sistema guardará la selección del usuario y la utilizará para posteriores exportaciones.

5.1.5.8 Suavizar la escala y desbarbar el vídeo.

5.1.5.9 Verificación de la autenticidad del archivo, que comprueba la firma digital única del servidor de archivo original.

5.1.5.9.1 La autenticidad de los archivos no puede verificarse si la firma del servidor de archivo original no está presente.

Almacenamiento

5.1.6 El sistema deberá ser capaz de almacenar secuencias de vídeo seleccionadas en bases de datos de vídeo seleccionadas.

5.1.6.1 El sistema deberá ser capaz de almacenar secuencias de vídeo de las mismas cámaras en múltiples bases de datos simultáneamente.

5.1.7 El sistema deberá ser capaz de crear y gestionar múltiples bases de datos.

5.1.8 El sistema deberá ser capaz de gestionar bases de datos que abarquen múltiples dispositivos locales o de almacenamiento en red (NAS).

5.1.9 El sistema deberá ser capaz de acceder a los recursos compartidos de red de Windows desde el software.

5.1.10 El sistema deberá ser capaz de avisar al usuario cuando los discos/compartimientos de red que contengan bases de datos en uso por el software se separen de la gestión del almacenamiento.

5.1.11 El sistema deberá ser capaz de destruir las bases de datos para destruir permanentemente los vídeos más antiguos que el límite máximo de días de grabación.

6 Interfaz gráfica de usuario (GUI)

Capacidades generales de la GUI

6.1.1 El sistema deberá proporcionar una interfaz gráfica de usuario (GUI) que permita a los usuarios ver fácilmente todos los recursos (Cámaras, componentes de Audio, bases de datos, Entradas, Salidas, Diseños, etc.) en un sitio completo, y no deberá estar limitado a IP específicas. 6.1. Servidores de vídeo en red.

6.1.1.1 El sistema deberá proporcionar dos facetas de interfaz de la GUI general; la interfaz del operador y la interfaz de configuración.

6.1.1.1.1 El sistema sólo permitirá a los usuarios administradores acceder a la interfaz de configuración, en la que se realiza toda la configuración del sitio.

6.1.1.1.2 El sistema permitirá a todos los niveles de usuarios ver los recursos disponibles en la interfaz de operador en diferentes grados (dependiendo de sus derechos de acceso asignados).

6.1.2 El sistema deberá admitir la traducción de la interfaz gráfica de usuario a varios idiomas, entre ellos:

6.1.2.1 Árabe,
6.1.2.2 Holandés,
6.1.2.3 inglés,
6.1.2.4 francés,
6.1.2.5 húngaro,
6.1.2.6 Italiano,
6.1.2.7 portugués,
6.1.2.8 Español.

6.1.3 Desde la interfaz del operador, será posible abrir múltiples sitios simultáneamente y mostrarlos en los monitores seleccionados en el sistema. Esto incluye los recursos asociados a los sitios, como los mapas de los sitios, la alimentación de las cámaras, etc.

6.1.4 La interfaz gráfica de usuario deberá poder visualizarse en un máximo de 6 monitores desde un ordenador cliente. El usuario deberá poder personalizar los monitores para poder ver diferentes componentes (por ejemplo, mapas, cámaras, datos de transacciones de integración de sistemas de terceros, etc.) en diferentes monitores o en "pestañas" de ventanas en el mismo monitor.

6.1.5 La disposición de la interfaz del operador deberá ser personalizable, como se indica a continuación:

6.1.5.1 Las funciones o características del sistema que no estén activadas, o a las que el usuario no tenga acceso, estarán ocultas a la vista: el usuario sólo verá las funciones que utilice.

6.1.5.2 Los recursos a los que el usuario no tenga acceso serán inaccesibles para el usuario.

6.1.5.3 La ubicación del panel de recursos puede establecerse a la derecha o a la izquierda de la pantalla de la pestaña de cámaras.

6.1.6 El sistema debe proporcionar una barra de estado en la parte inferior de la interfaz gráfica de usuario para indicar información sobre el software mediante iconos de estado, en los que se puede hacer clic para obtener más información. Por ejemplo:

6.1.6.1 El sistema deberá mostrar una advertencia de licencia para los recursos del sitio que tengan una licencia incorrecta.
6.1.6.2 El sistema debe mostrar el nombre de usuario y el nivel de acceso del usuario conectado.
6.1.6.3 El sistema debe mostrar la licencia del sitio aplicada.
6.1.6.4 El sistema debe mostrar una notificación de cámara si una cámara se cae.
6.1.6.5 El sistema debe mostrar un monitor de rendimiento que indique las estadísticas de rendimiento del sistema.
6.1.6.6 El sistema deberá mostrar el estado de conexión de la unidad actual con el sitio.
6.1.6.7 El sistema deberá mostrar una notificación de análisis de vídeo cuando se produzca un error con una o más de las fuentes de vídeo del sitio.
6.1.6.8 El sistema deberá mostrar una notificación de Failover que proporcione información sobre el estado de los servidores de conmutación existentes.
6.1.6.9 El sistema deberá mostrar una advertencia de manipulación cuando se considere que una o más de las cámaras del sitio han sido manipuladas.

Cámaras

6.1.7 Interfaz de configuración
6.1.7.1 El sistema deberá restringir el acceso a la configuración de la cámara del sitio en la interfaz de configuración a los administradores.
6.1.7.2 El sistema deberá proporcionar un asistente de adición y configuración de cámaras.
6.1.7.3 El sistema deberá ser capaz de configurar grabaciones programadas, grabaciones de movimiento y grabaciones analíticas desde el asistente de configuración.
6.1.7.4 El sistema deberá proporcionar una capacidad de "copiar y pegar" que permitirá a los usuarios copiar fácilmente la configuración de la cámara, incluyendo la información de múltiples flujos de vídeo, a través de múltiples cámaras.
6.1.7.5 Durante la configuración de la cámara, el sistema deberá mostrar la URL/página web de la cámara que puede cargarse en el navegador.
6.1.7.6 El sistema deberá permitir al administrador designar una cámara como "encubierta". En este caso, la cámara sólo podrá ser vista y revisada por los administradores.
6.1.7.7 El sistema deberá admitir el escalado automático de los DPI.
6.1.7.8 El sistema deberá proporcionar informes sobre las cámaras en línea y fuera de línea (fallidas).

6.1.8 Interfaz del operador
6.1.8.1 El sistema deberá permitir a los usuarios ver e interactuar con las cámaras en diferentes grados, dependiendo de los derechos de acceso asignados.
6.1.8.2 El sistema debe permitir al usuario seleccionar cámaras específicas para verlas en monitores seleccionados, o paneles seleccionados dentro de monitores seleccionados.
6.1.8.3 El sistema deberá ofrecer la posibilidad de arrastrar y soltar cámaras desde un panel de recursos a los monitores o paneles seleccionados en el monitor.
6.1.8.4 El sistema deberá permitir la sincronización de las cámaras durante la reproducción.
6.1.8.5 El sistema deberá permitir a los usuarios pausar la reproducción de vídeo e imprimir, copiar en el portapapeles o guardar una imagen en una ubicación de almacenamiento seleccionada.

6.1.8.6 El sistema deberá permitir a los usuarios arrastrar y soltar cámaras, desde un mapa, en los monitores o paneles seleccionados en el monitor.

6.1.8.7 El sistema deberá permitir la configuración y el inicio de recorridos (secuencias) de cámaras en monitores seleccionados o en paneles dentro de un monitor seleccionado.

6.1.8.8 El sistema deberá proporcionar la capacidad de crear y guardar múltiples "diseños" de cámaras que puedan ser fácilmente seleccionadas, ya sea manualmente por un usuario, o automáticamente en un evento.

6.1.8.9 El sistema deberá permitir el inicio de recorridos (secuencias) de "layouts" (también conocido como "salvo") a los monitores seleccionados.

6.1.8.10 El sistema deberá permitir al usuario desanclar el vídeo de las cámaras panorámicas de 180 o 360 grados.

6.1.8.11 El sistema deberá permitir al usuario ver hasta 64 cámaras en un solo monitor.

6.1.8.12 El sistema deberá permitir a los usuarios hacer zoom digital en vistas de cámaras específicas.

6.1.8.13 El sistema deberá permitir a los usuarios elegir qué flujo se mostrará si se han designado varios flujos de cámaras para su visualización en directo.

Recursos del sitio

6.1.9 El sistema deberá permitir a los administradores configurar qué recursos del sitio son visibles en la interfaz del operador.

6.1.10 El sistema deberá permitir a los administradores crear carpetas y asignar recursos a las carpetas seleccionadas.

6.1.11 El acceso de los usuarios a los recursos del sitio deberá estar controlado por el nombre de usuario y la contraseña, ya sea en forma local o remota, y restringido por el nivel de acceso del usuario individual.

6.1.12 El usuario deberá ser capaz de ver los disparadores de entrada desde la GUI.

6.1.13 El usuario debe poder controlar las salidas desde la GUI.

Superposiciones de texto y gráficos

6.1.14 La interfaz del operador deberá mostrar opcionalmente información gráfica de dispositivos residentes y de terceros como superposiciones en los paneles de la cámara.

6.1.15 El sistema deberá permitir el reposicionamiento de los bloques de superposición y el cambio de los tamaños de las superposiciones, los tamaños del texto, la transparencia y el color.

6.1.16 La interfaz del operador deberá ser capaz de mostrar opcionalmente el funcionamiento de los algoritmos de análisis mediante la visualización de superposiciones.

Controles PTZ

6.1.17 El sistema deberá ser capaz de controlar las cámaras Pan-Tilt-Zoom (PTZ) desde la interfaz del operador y a través de las acciones de eventos.

6.1.18 El sistema también deberá permitir a los usuarios controlar las cámaras PTZ desde un teclado/joystick conectado.

6.1.19 Los controles PTZ incluyen:

6.1.19.1 Pan, Tilt y Zoom.

6.1.19.2 Velocidad de movimiento PTZ variable.

6.1.19.3 Control de enfoque e iris.

6.1.19.4 Definir posiciones preestablecidas de la cámara PTZ.

6.1.19.5 Asignar nombres únicos a las posiciones preestablecidas de la cámara PTZ.

6.1.19.6 Desplazarse a las posiciones predeterminadas de la cámara PTZ.

6.1.20 El sistema deberá ser capaz de controlar de forma prioritaria una cámara PTZ.

6.1.20.1 Un usuario administrador tiene la máxima prioridad de control sobre la cámara PTZ, tras lo cual la jerarquía de prioridades desciende desde el nivel de usuario 30 hasta el nivel de usuario 1.

6.1.20.2 Dos usuarios del mismo nivel otorgarán al primer usuario el control prioritario, y el segundo usuario deberá esperar hasta que haya transcurrido el periodo de "anulación del domo".

Vista en directo

6.1.21 El sistema deberá permitir a los usuarios ver y pausar las cámaras en directo (dependiendo de los derechos de acceso asignados).

6.1.22 El sistema deberá permitir que determinadas cámaras se vean en directo y se reproduzcan simultáneamente, y que se sincronicen entre sí si así se solicita.

6.1.23 El sistema deberá permitir que la misma cámara se vea en directo en varios monitores o paneles en un solo monitor.

6.1.24 El sistema deberá ser capaz de mostrar rastros de actividad durante un máximo de 15 minutos en modo directo. Véase el apartado 7.10.

Revisar

6.1.25 El sistema deberá permitir la revisión de las cámaras en la misma ventana, y en el mismo panel, mientras se reproduce el vídeo en directo, sin necesidad de abrir una ventana/pestaña de revisión o de base de datos por separado.

6.1.25.1 El sistema deberá permitir a los usuarios reproducir las secuencias grabadas haciendo clic y arrastrando la línea de tiempo de la cámara hasta el punto de revisión deseado.

6.1.25.2 El sistema debe permitir a los usuarios revisar fácilmente cualquier cámara en el sistema, desde cualquier/múltiples clientes conectados al sistema, ya sea fuera o dentro de las instalaciones.

6.1.26 El sistema deberá pedir al usuario que seleccione la base de datos desde la que desea revisar si la cámara seleccionada ha sido configurada para grabar en múltiples bases de datos.

6.1.27 El sistema deberá ser capaz de revisar las grabaciones de las cámaras compatibles con Edge.

6.1.28 El sistema deberá ser capaz de revisar múltiples cámaras simultáneamente y sincronizar los tiempos de revisión de dichas cámaras.

6.1.29 El sistema deberá conservar los tiempos de revisión de las diferentes cámaras seleccionadas para el mismo panel. Si una cámara está en modo de revisión y se abre una nueva cámara en ese panel, la nueva cámara pasará al mismo tiempo de revisión que la cámara original.

6.1.30 El sistema deberá controlar los derechos de acceso para archivar y revisar las secuencias de vídeo archivadas.

6.1.31 El sistema deberá ser capaz de realizar búsquedas inteligentes utilizando las siguientes herramientas de revisión:

6.1.31.1 Búsqueda instantánea. Véase la sección 6.8.

6.1.31.2 Búsqueda de área de movimiento. Véase el apartado 7.11.

6.1.31.3 Visualización de vistas previas de imágenes en miniatura de una grabación al pasar el ratón por encima de la línea de tiempo.

6.1.32 El sistema deberá ser capaz de mostrar rastros de actividad de hasta 60 minutos en modo de revisión. Véase el apartado 7.10.

Zonas de privacidad

6.1.33 El sistema deberá permitir a los usuarios administradores crear y eliminar Zonas de Privacidad en la alimentación de la cámara.

6.1.33.1 Las Zonas de Privacidad deberán ser polígonos negros configurables que oculten las áreas sensibles de la alimentación de la cámara.

6.1.34 El sistema deberá mostrar las zonas de privacidad en vivo, en revisión y en las secuencias de video archivadas.

6.1.35 El sistema deberá permitir a los usuarios con los derechos de acceso correctos ocultar/mostrar las zonas de privacidad.

6.1.36 El sistema deberá mostrar/ocultar las zonas de privacidad en las secuencias archivadas en función de si el usuario las ha ocultado/mostrado o no en el momento del archivo.

Herramientas de revisión de búsqueda inteligente

6.1.37 El sistema deberá ser capaz de buscar de forma inteligente movimiento en el vídeo en revisión utilizando los datos recogidos en la base de datos de movimiento. Estas herramientas son:

6.1.37.1 Búsqueda instantánea:

6.1.37.1.1 En la revisión, el sistema deberá ser capaz de dividir un período de tiempo definido por el usuario en una matriz de imágenes en miniatura definida por el usuario.

6.1.37.1.2 El sistema deberá permitir al usuario reducir el período de búsqueda definido entre las instantáneas mostradas haciendo clic y arrastrando entre las miniaturas deseadas.

6.1.37.1.3 La matriz de miniaturas se reconfigurará para este nuevo periodo de búsqueda.

6.1.37.1.4 El sistema deberá ser capaz de definir periodos de tiempo de búsqueda según segundos, minutos, horas, días y semanas.

6.1.37.1.5 El sistema deberá ser capaz de reproducir las imágenes grabadas a partir de una determinada miniatura tanto en el reproductor de vídeo de la interfaz del operador como en el reproductor de vídeo integrado en la ventana de Snap-Search.

6.1.37.1.6 El sistema deberá ser capaz de archivar vídeo desde el reproductor de vídeo incrustado en la ventana Snap-Search.

6.1.37.2 Búsqueda de movimiento:

6.1.37.2.1 En la revisión, el sistema deberá ser capaz de seleccionar ciertas áreas de la imagen de la cámara para buscar movimiento reciente dentro del área seleccionada.

6.1.37.2.2 El sistema utiliza los datos de movimiento recogidos en la Base de Datos de Movimiento para indicar el movimiento reciente en el área seleccionada.

6.1.37.2.3 El sistema mostrará todo el movimiento en el área seleccionada como barras de movimiento rojas a lo largo de la línea de tiempo de revisión de la cámara; cuanto más alta sea la barra de movimiento, más movimiento habrá en el área seleccionada en ese punto de la grabación.

Rutas de actividad:

6.1.38 El sistema debe ser capaz de mostrar dónde y cuán recientemente ha ocurrido la actividad en varias áreas de la alimentación de la cámara mediante la visualización de las rutas de actividad.

6.1.39 El sistema utiliza los datos de movimiento recogidos en la Base de Datos de Movimiento, y las grabaciones de las cámaras, para generar rastros de actividad.

6.1.40 El sistema debe mostrar las rutas de actividad en colores que van del verde al rojo para indicar la actividad pasada y presente en un área.

6.1.40.1 Cuanto más verde sea una superposición, más atrás en el tiempo habrá ocurrido la actividad en esa zona.

6.1.40.2 Cuanto más roja sea la superposición, más reciente es la actividad en esa zona.

6.1.41 El sistema deberá mostrar la hora de la actividad (en minutos y segundos) en la parte superior de la superposición del rastro de actividad para indicar cuánto tiempo atrás desde la hora actual se produjo la actividad en esa zona.

6.1.42 El sistema deberá ser capaz de mostrar superposiciones del rastro de actividad para ciertos períodos de tiempo que se determinan por el modo de visualización y las grabaciones de la cámara;

6.1.42.1 En la vista en directo, y/o si no se han configurado las grabaciones de la cámara, el sistema es capaz de mostrar rastros de actividad para la actividad que ha ocurrido en los últimos 15 minutos de la hora actual.

6.1.42.2 En la revisión (siempre que se hayan configurado las grabaciones de las cámaras), el sistema puede mostrar los rastros de actividad que se hayan producido en los últimos 60 minutos de la hora actual.

6.1.43 El sistema deberá ser capaz de activar y desactivar los rastros de actividad.

6.1.44 El sistema deberá ser capaz de cambiar a la hora de la actividad indicada por una superposición de rastro de actividad haciendo doble clic en la superposición de rastro de actividad deseada.

6.1.45 El sistema deberá mostrar el movimiento en la alimentación de la cámara como barras de movimiento rojas a lo largo de la línea de tiempo de revisión de la cámara; cuanto más alta

sea la barra de movimiento, más movimiento habrá en la alimentación de la cámara en ese punto de la grabación

Mapas de calor

6.1.46 El sistema deberá ser capaz de mostrar una superposición de mapas de calor utilizando datos cotejados de la base de datos de movimiento para indicar las áreas de movimiento.

6.1.47 El sistema deberá mostrar las zonas de mayor a menor movimiento utilizando un espectro de colores de rojo a verde, respectivamente.

6.1.48 El sistema deberá ser capaz de refinar los resultados del mapa de calor utilizando determinados parámetros:

6.1.48.1 Periodo de análisis, que determina durante qué tiempo se analizará el movimiento de la cámara. Los periodos de análisis incluyen:

6.1.48.1.1 Día de la semana,

6.1.48.1.2 Semana del mes,

6.1.48.1.3 Mes del año,

6.1.48.1.4 Trimestre del año,

6.1.48.1.5 Año.

6.1.48.2 Las instantáneas mostradas en el desglose de resultados pueden desglosarse según:

6.1.48.2.1 Día de la semana,

6.1.48.2.2 Semana del mes,

6.1.48.2.3 Mes del año,

6.1.48.2.4 Trimestre del año.

6.1.48.3 Las instantáneas mostradas en el desglose de resultados pueden ajustarse en tamaño.

6.1.48.4 Las superposiciones pueden ajustarse para mostrar el porcentaje de tiempo (fuera del período de análisis definido) durante el cual se produjo el movimiento.

6.1.48.5 Los ajustes de sensibilidad y umbral permiten filtrar el movimiento en las escenas con un nivel de actividad alto/bajo.

Mapeo de cámaras adyacentes

6.1.49 El sistema deberá ofrecer la posibilidad de enlazar cámaras físicamente próximas en el software, para permitir una navegación simplificada entre las cámaras enlazadas en la interfaz del operador cuando se sigan objetos/sospechosos en movimiento a través de múltiples cámaras.

6.1.50 El sistema deberá proporcionar una pantalla de mapeo para configurar las cámaras adyacentes, seleccionando las cámaras de los recursos del sitio disponibles para ser configuradas como cámaras adyacentes y definiendo las relaciones bidireccionales entre cada par de cámaras adyacentes.

6.1.51 El sistema deberá ser capaz de gestionar las cámaras adyacentes mediante "páginas" en las que se utilicen carpetas y subcarpetas para organizarlas.

6.1.51.1 El sistema deberá permitir que la misma cámara se añada a varias páginas, subcarpetas y carpetas diferentes.

6.1.52 El sistema deberá permitir que una cámara y todos los enlaces direccionales asociados a otras cámaras mapeadas se eliminen de cualquiera de ellas:

6.1.52.1 Una única página, subcarpeta o carpeta sin eliminarla de otras páginas, subcarpetas o carpetas; o

6.1.52.2 Todas las páginas, subcarpetas o carpetas.

6.1.53 En la interfaz del operador, el sistema deberá ser capaz de lo siguiente:

6.1.53.1 Mostrar flechas como superposiciones en las cámaras configuradas, apuntando en las direcciones de las cámaras físicamente adyacentes.

6.1.53.2 Cambiar a cámaras adyacentes al seleccionar la flecha de la cámara adyacente correspondiente.

6.1.53.3 Permitir al usuario seleccionar Cámara adyacente en el menú desplegable de Recursos en la pestaña Cámaras.

6.1.53.4 Visualización de las cámaras adyacentes al hacer clic en la flecha de la cámara correspondiente.

Marcadores

6.1.54 El sistema deberá ser capaz de crear marcadores de revisión.

6.1.54.1 El marcador almacenará un instante en el tiempo para revisar en una fecha posterior. Al acceder al marcador almacenado se navegará al estado de revisión, en el momento en que se guardó en el software.

6.1.54.2 Los marcadores pueden crearse con múltiples cámaras y se almacenan por usuario de catexis.

6.1.54.3 Los marcadores serán diferentes para cada usuario conectado al software de Cathexis.

6.1.54.4 Los marcadores se almacenarán en el momento del sistema local.

6.1.54.5 El sistema almacenará los marcadores localmente. Los marcadores guardados en una unidad no serán accesibles desde otra.

6.1.54.6 La exportación de las cámaras marcadas puede realizarse 60 minutos antes y 60 minutos después de la hora de ser marcadas.

6.1.54.7 El software permitirá al usuario crear un archivo de las filmaciones, que podrá ser visualizado en el reproductor de archivos cathexis.

6.1.54.8 Seleccione la base de datos de la cámara que el archivo debe utilizar al exportar.

6.1.54.9 Es posible restaurar un marcador, a partir de imágenes en directo o de revisión, utilizando el diseño personalizado de la cámara.

6.1.54.10 Un marcador está limitado a 8 cámaras en revisión.

6.1.54.11 El sistema sólo permitirá a los usuarios crear marcadores con recursos a los que el usuario tenga acceso.

6.1.54.12 El sistema no debe guardar en el marcador:

6.1.54.13 Posición PTZ,

6.1.54.14 Parámetros actuales del zoom digital,

6.1.54.15 Secuencias en vivo que se ejecutan en un panel.

6.1.54.16 El sistema no evitará que los datos se sobrescriban en el servidor por la creación de un marcador.

Sistema de gestión de imágenes de referencia

6.1.55 El sistema proporcionará una interfaz para la creación, mantenimiento y comparación de imágenes de referencia (puntos de referencia) de todas las cámaras de un servidor.

6.1.56 El sistema deberá permitir ver, exportar o eliminar las imágenes de referencia.

6.1.57 El sistema deberá permitir la comparación entre las imágenes de referencia capturadas y/o la orientación actual de las cámaras de un servidor.

6.1.58 El sistema deberá mostrar las diferencias entre las imágenes de referencia comparadas.

Pared de vídeo

6.1.59 El sistema deberá proporcionar un software de videowall que se ejecute en ordenadores dedicados a la visualización de las señales de vídeo.

6.1.60 El sistema deberá ser capaz de mostrar múltiples cámaras del sitio en los monitores de la pared de vídeo.

6.1.61 El sistema deberá ser capaz de controlar múltiples monitores conectados a múltiples ordenadores desde un único punto a través de un panel MIMIC.

6.1.62 El sistema deberá ser capaz de arrastrar y soltar las cámaras en su lugar para mostrarlas en el mural de vídeo desde sitios distintos al sitio del monitor.

6.1.63 El sistema deberá permitir a los administradores configurar las disposiciones de las cámaras del videowall, el recorrido de las disposiciones (salvo) y los derechos de acceso a los videowalls.

7 Análisis de vídeo

Capacidades generales

7.1.1 El sistema deberá tener sus propios análisis y algoritmos, incorporados en el software, para ser utilizados como activadores de eventos.

7.1.1.1 Esto incluirá la detección de movimiento de vídeo y el análisis de seguimiento de objetos.

7.1.2 El sistema deberá permitir que se configure el análisis de vídeo en las secuencias en vivo y grabadas.

7.1.3 El sistema deberá restringir el acceso a la configuración de los análisis únicamente a los administradores.

7.1.4 El sistema deberá ser capaz de utilizar la analítica integrada en la cámara IP o el codificador para iniciar un evento al que se puedan asociar las acciones seleccionadas.

7.1.5 El sistema deberá ser capaz de integrarse con conjuntos de análisis de terceros.

7.1.6 El sistema deberá ser capaz de realizar las siguientes funciones de clasificación de objetos en los análisis de seguimiento de objetos en las suites de análisis básico, intermedio y avanzado:

7.1.6.1 Clasificar los objetos rastreados y mostrar los siguientes metadatos sobre la clasificación:

7.1.6.1.1 Tipo de objeto,

7.1.6.1.2 Color del objeto,

7.1.6.1.3 Tamaño del objeto,

7.1.6.1.4 Velocidad del objeto.

7.1.6.1.5 Persona

7.1.6.1.6 Animal

7.1.6.1.7 Vehículo

7.1.6.2 Almacenamiento de objetos clasificados en una base de datos de seguimiento de objetos.

7.1.6.2.1 Se mostrarán los metadatos de clasificación de objetos.

Análisis de detección de movimiento

7.1.7 El sistema deberá contar con algoritmos de detección de movimiento por vídeo (VMD) integrados, y será capaz de realizarlos en los flujos de vídeo recibidos.

7.1.8 El sistema ofrecerá las siguientes opciones de VMD Básico y Inteligente.

7.1.8.1 VMD básico

7.1.8.1.1 Algoritmo básico de detección de movimiento.

7.1.8.1.2 Supresión básica del ruido.

7.1.8.2 VMD inteligente

7.1.8.2.1 Filtrado avanzado de movimientos repetitivos como árboles o hierba.

7.1.8.2.2 Seguimiento de las cargas de luz.

7.1.8.2.3 Algoritmos avanzados de detección de movimiento diseñados para escenas exteriores.

7.1.9 La detección de movimiento integrada básica e inteligente deberá tener las siguientes características:

7.1.9.1 Sensibilidad variable.

7.1.9.2 Enmascaramiento de tamaño.
7.1.9.3 Rechazo de objetos más pequeños/grandes que un tamaño especificado.
7.1.9.4 Áreas VMD multizona por cámara con la posibilidad de variar la sensibilidad en cada zona.
7.1.9.5 Capacidad de ajuste día/noche para permitir diferentes ajustes VMD para el día y la noche.
7.1.9.6 La conmutación automática día/noche o la conmutación a horas determinadas serán opcionales.
7.1.9.7 Una programación que habilite/deshabilite los activadores de eventos VMD seleccionados en determinados momentos del día.

7.1.10 Para la configuración de VMD, el sistema deberá permitir a los usuarios ver vídeo en directo o grabado, con fines de configuración/prueba de VMD.

7.1.11 El sistema deberá tener la capacidad de mostrar áreas de enmascaramiento de VMD, incluyendo:
7.1.11.1 Activadores de VMD.
7.1.11.2 Áreas de detección VMD.

Análisis básico, intermedio y avanzado

7.1.12 El sistema deberá ser capaz de proporcionar opciones de análisis de vídeo básicas, intermedias y avanzadas.

7.1.13 El sistema deberá ser capaz de desencadenar eventos basados en los desencadenantes generados por los análisis básicos, intermedios y avanzados.

7.1.14 El sistema ofrece las siguientes opciones de activación de eventos:
7.1.14.1 Analítica básica.
7.1.14.2 Activadores básicos de cruce de líneas.
7.1.14.3 Disparos básicos de presencia.
7.1.14.4 Análisis intermedios.
7.1.14.5 Activadores avanzados de cruce de líneas.
7.1.14.6 Activadores de presencia avanzados.
7.1.14.7 Análisis avanzado.
7.1.14.8 Activadores avanzados de cruce de líneas.
7.1.14.9 Activadores de presencia avanzados.
7.1.14.10 Detección de velocidad.
7.1.14.11 Filtros de tamaño y dirección.

Recuento de cabezas

7.1.15 El sistema deberá proporcionar los siguientes algoritmos de recuento de cabezas y opciones de capacidad:
7.1.15.1 Rastreador de cabezas de arriba abajo; el algoritmo en una cámara de color estándar que mira hacia abajo ofrece la activación de eventos cuando las cabezas cruzan una línea.
7.1.15.2 Rastreador de cabezas oblicuo; el algoritmo en una cámara de color estándar montada en ángulo ofrece la activación de eventos cuando las cabezas cruzan una línea.

Algoritmo de longitud de la cola

7.1.16 El sistema ofrecerá la activación de eventos cuando una cola supere una longitud determinada.

Algoritmo de objetos fijos

7.1.17 El sistema ofrecerá la activación de eventos cuando un objeto haya sido abandonado durante un periodo de tiempo.

Detección de manipulación de la cámara

7.1.18 El sistema debe venir de serie con análisis de vídeo de detección de manipulación de la cámara.

7.1.18.1 La manipulación de la cámara incluye:

7.1.18.1.1 Cobertura de la lente (por ejemplo, pintura en aerosol)

7.1.18.1.2 Movimiento de la cámara,

7.1.18.1.3 Re/desenfoque del objetivo.

7.1.19 El sistema deberá permitir que a cualquier cámara configurada se le añada la detección de manipulaciones.

7.1.20 El sistema deberá permitir que la manipulación de la cámara active eventos.

7.1.21 El sistema deberá mostrar una notificación de alarma en la interfaz del operador cuando se detecte una manipulación.

7.1.22 El sistema deberá eliminar las falsas alarmas exigiendo que una manipulación persista durante 60 segundos antes de ser considerada una verdadera manipulación.

7.1.23 El sistema deberá restringir la capacidad del usuario para restablecer una manipulación de la cámara en función de los derechos de acceso asignados por el administrador.

Base de datos de movimiento

7.1.24 El sistema deberá permitir la creación de una Base de Datos de Movimiento que recoja los datos de movimiento de las cámaras seleccionadas.

7.1.24.1 El sistema deberá permitir que los datos de movimiento de la Base de Datos de Movimiento se utilicen para informar de las funciones de Rutas de Actividad y Búsqueda de Áreas de Movimiento de la interfaz del operador en las cámaras seleccionadas.

7.1.25 El sistema deberá permitir que el seguimiento de los datos de movimiento se configure con distintos niveles de sensibilidad; cuanto más alta sea la sensibilidad, más fino será el seguimiento del movimiento.

7.1.26 El sistema deberá permitir que el tamaño de la cuadrícula en la que se rastrean los datos de movimiento se establezca utilizando:

7.1.26.1 Ajustes de relación de aspecto y granularidad (cuanto más fina sea la granularidad, más movimiento se detecta en áreas más pequeñas de la imagen).

7.1.26.2 Ajuste manual del tamaño de la cuadrícula.

8 Activadores, eventos y acciones

Capacidades generales

8.1.1 El sistema deberá restringir el acceso a la gestión de eventos únicamente a los administradores.

8.1.2 El sistema deberá ser capaz de generar un evento del sistema basado en los disparadores del sistema configurados, y realizar acciones de eventos configurados.

8.1.3 El sistema deberá ser capaz de almacenar automáticamente todos los eventos del sistema en una base de datos de eventos del sistema, incluso cuando no haya ningún vídeo asociado al evento. Consulte la sección Bases de datos para obtener más información.

Activadores de eventos

8.1.4 El sistema deberá tener la capacidad de generar eventos a partir de los siguientes disparadores:

8.1.4.1 Disparador de cámaras/codificadores en la red. Esto incluye entradas físicas o activadores de análisis de vídeo de las cámaras.

8.1.4.2 Detección y análisis de movimiento propios del sistema.

8.1.4.3 Dispositivos de terceros (por ejemplo, control de acceso, paneles de incendio, paneles de alarma, puntos de venta, etc.).

8.1.4.4 Eventos de usuarios locales (eventos iniciados por un operador).

8.1.4.5 Grabaciones iniciadas por un horario.

Configuración de eventos

8.1.5 El sistema tendrá una función "Y" que impedirá que se produzcan disparos a menos que haya un disparador de eventos Y una entrada de E/S.

8.1.6 El sistema deberá ser capaz de asignar horarios a un evento, durante los cuales el evento se considera válido. El evento no estará activo durante los tiempos fuera de las horas especificadas en el horario asignado.

8.1.7 El sistema deberá proporcionar un ajuste para limitar la frecuencia de los disparos.

8.1.8 El sistema deberá proporcionar un ajuste que descarte los disparos de eventos cortos, dando lugar a que los eventos sólo se activen si los niveles de disparo permanecen altos durante la duración del período de filtrado (o lo superan).

8.1.9 El sistema deberá proporcionar un ajuste de "nivel de prioridad" para los eventos que deban enviarse como alarmas a la interfaz del operador o a la pasarela de gestión de alarmas.

Acciones de los eventos

8.1.10 El sistema deberá ser capaz de realizar una o más de las siguientes acciones al recibir un evento:

8.1.10.1 Realizar una acción ya sea "mientras" ocurre un evento o "cuando" ocurre un evento.

8.1.10.2 Grabar imágenes de vídeo de una o más cámaras en una base de datos seleccionada.

8.1.10.3 Grabar eventos previos de una o más cámaras.

8.1.10.4 Grabar vídeo y audio sincronizados.
8.1.10.5 Conmutar o alternar una o más salidas de relé proporcionadas por el sistema o por las cámaras/codificadores conectados al sistema.
8.1.10.6 Pulsar una o más salidas de relé proporcionadas por el sistema o las cámaras/codificadores conectados al sistema.
8.1.10.7 Controlar una entrada virtual.
8.1.10.8 Mover una o más cámaras PTZ a posiciones "preestablecidas".
8.1.10.9 Cambiar una o más cámaras seleccionadas a uno o más monitores seleccionados conectados al sistema.
8.1.10.10 Cambiar la "disposición" de una cámara a un monitor seleccionado.
8.1.10.11 Grabar datos de un sistema de terceros (por ejemplo, punto de venta, control de acceso, paneles de alarma).
8.1.10.12 Iniciar una acción gráfica en un mapa.
8.1.10.13 Reproducir un clip de audio pregrabado a través del servidor cliente local O a través de una salida de audio en una cámara o codificador IP.
8.1.10.14 Enviar un correo electrónico a los destinatarios seleccionados.
8.1.10.15 Enviar una alarma a la interfaz del operador y a la de gestión de alarmas (véase el apartado 12).
8.1.10.15.1 Al enviar una notificación a un Gateway de Alarmas, el sistema debe permitir al usuario definir vistas previas de video para ser enviadas con la notificación del evento.
8.1.10.15.2 Los eventos configurados con "niveles de prioridad" presentarán a los usuarios alarmas con los niveles de prioridad correspondientes.
8.1.10.16 Detener una acción previamente iniciada.
8.1.10.17 El sistema debe permitir que todas las acciones estén sujetas a horarios definidos por el usuario.
8.1.10.18 El sistema deberá ofrecer la posibilidad de crear "plantillas de eventos" que permitirán a los usuarios asociar fácilmente acciones comunes en varias cámaras.

9 Integración

Capacidades generales

9.1.1 El sistema debe tener la capacidad de integrar productos y dispositivos de terceros.

9.1.2 El sistema no debe ejecutar integraciones de terceros como plug-ins en el cliente del software.

9.1.3 El sistema no deberá requerir servidores de gestión adicionales para ejecutar los servicios de integración de terceros.

9.1.4 El sistema deberá centralizar todas las integraciones en un punto del software.

9.1.5 El sistema debe ser capaz de configurar bases de datos específicas para cada integración, utilizando controladores específicos de integración. Ver Sección de bases de datos para más información.

9.1.6 El sistema dejará de conectarse y recibir estados y notificaciones de los dispositivos de integración que se ejecuten en sitios con CathexisVision 2017, y anteriores.

9.1.7 La capacidad de integración dependerá del dispositivo integrado, pero el sistema deberá ser capaz de las siguientes características:

9.1.7.1 Recepción de datos del dispositivo de terceros.

9.1.7.2 Recuperar activadores de eventos específicos y realizar acciones de eventos dependientes de los datos específicos recibidos.

9.1.7.3 Almacenar los datos en campos lógicos en una base de datos seleccionada.

9.1.7.4 Asociar una o más cámaras con objetos del dispositivo de integración y sus eventos asociados.

9.1.7.5 Visualizar los datos recibidos como una superposición en las cámaras asociadas en modo directo y de revisión (cuando sea posible).

9.1.7.6 Mostrar y configurar las propiedades del dispositivo de integración, como por ejemplo:

9.1.7.6.1 Configurar los objetos del dispositivo de integración.

9.1.7.6.2 Configurar y ver las propiedades de estado de los objetos del dispositivo de integración.

9.1.7.6.3 Ver eventos del dispositivo de integración.

9.1.7.6.4 Configurar grupos de objetos de dispositivos de integración.

9.1.7.6.5 Configurar otros ajustes del dispositivo de integración, como superposiciones, tiempos de espera, etc.

Lista de dispositivos de integración

9.1.8 El sistema debe ser capaz de integrarse con varios productos y dispositivos de terceros, incluyendo (pero no limitado) a los siguientes:

9.1.8.1 Control de acceso.

9.1.8.2 Punto de venta.

9.1.8.3 Paneles de alarma.

9.1.8.4 Paneles de incendio.

9.1.8.5 Reconocimiento automático de matrículas.

9.1.8.6 Vigilancia de vallas y perímetros.

9.1.8.7 Monitorización ambiental.

9.1.8.8 Análisis de vídeo de terceros.

9.1.8.9 Teclados y controladores.

9.1.9 El sistema deberá integrarse con los dispositivos de E/S para controlar las salidas y recibir las entradas de los dispositivos de E/S. Estos dispositivos pueden estar en una cámara de red, en un codificador (servidor) o en un dispositivo de E/S de red dedicado.

10 Reconocimiento automático de matrículas (ANPR)

Capacidades generales

10.1.1 El sistema deberá incluir el reconocimiento automático de matrículas como característica opcional.

10.1.2 El sistema deberá integrarse con tres categorías de motores ANPR:
10.1.2.1 Algoritmos ANPR de terceros, que envían disparos ANPR a CathexisVision;
10.1.2.2 Cámaras ANPR, con detección ANPR incorporada, que envían disparos al VMS; y
10.1.2.3 Motores ANPR incorporados al VMS, que se desbloquean con las licencias correspondientes.

10.1.3 El sistema incorporado deberá tener las siguientes capacidades:
10.1.3.1 Soportar múltiples bibliotecas de idiomas y caracteres de matrículas, incluyendo el árabe.
10.1.3.2 Soportar la configuración para la detección de matrículas para las siguientes soluciones de detección:
10.1.3.2.1 Solución disparada, que utiliza un disparador físico para iniciar una detección (como un bucle de tierra, un rayo IR o una solución VMD), y
10.1.3.2.2 Solución de flujo libre, que detecta las matrículas de los vehículos en movimiento.
10.1.3.3 Apoyar la superposición de los datos de las matrículas detectadas en los flujos de video en vivo y grabados.

10.1.4 El sistema deberá incluir la capacidad de importar/exportar datos ANPR existentes en un formato de archivo CSV.

Detectores ANPR integrados en el sistema

10.1.5 El sistema deberá permitir la configuración de múltiples detectores ANPR en la interfaz de configuración de las cámaras ya instaladas, siempre que se disponga de las licencias necesarias.

10.1.6 El sistema deberá soportar las siguientes opciones de detectores:
10.1.6.1 Configuración específica de la cámara, como la resolución y la frecuencia de imagen.
10.1.6.2 Selección del área de captura de la matrícula del vehículo.
10.1.6.3 Configuración del tamaño, la pendiente y la inclinación de los caracteres de la matrícula.
10.1.6.4 Configuración del análisis de la matrícula en función de una activación de entrada, como un bucle de tierra o en movimiento.
10.1.6.5 Pruebas (análisis de matrículas) de la configuración del ANPR utilizando imágenes grabadas del lugar para el ajuste fino del algoritmo.

Normas ANPR

10.1.7 El sistema deberá incluir la capacidad de agrupar los datos de las matrículas en categorías específicas como visitantes, personal, lista blanca, lista negra, etc.

10.1.8 El sistema deberá ser capaz de configurar las siguientes reglas de análisis de tráfico que generan mensajes del sistema cuando se detectan patrones de tráfico definidos:
10.1.8.1 La regla de ubicación de la visita se activa si una matrícula se ve en la misma ubicación varias veces.

10.1.8.2 La regla de área de visita se activa si una matrícula es vista en múltiples ubicaciones en un período de tiempo determinado.

Eventos ANPR

10.1.9 El sistema deberá ser capaz de crear eventos activados mediante el reconocimiento de matrículas.

10.1.10 El sistema deberá ser capaz de configurar eventos basados en la matrícula específica y los datos del evento.

10.1.11 El sistema deberá ser capaz de configurar eventos basados en los datos específicos del grupo de matrículas.

10.1.12 El sistema deberá ser capaz de desencadenar acciones de eventos que incluyan, entre otras, la activación de dispositivos de E/S para el control de acceso.

10.1.13 El sistema deberá ser capaz de generar informes de eventos ANPR:

10.1.13.1 Los reportes de eventos deberán ser exportables en formato de archivo PDF o CSV.

10.1.13.2 Los reportes de eventos deberán ser generados en base a filtros de datos pertenecientes a los datos ANPR del vehículo.

10.1.13.3 Los reportes de eventos deben ser generados en base a períodos de tiempo específicos.

Alarmas ANPR

10.1.14 El sistema deberá ser capaz de generar alarmas basadas en eventos ANPR, tales como:

10.1.14.1 Los datos de eventos ANPR que aparezcan en una lista negra de datos deberán crear una alarma.

10.1.14.2 Los datos de eventos ANPR para el mismo vehículo que se registran múltiples veces dentro de un período de tiempo especificado crearán una alarma.

10.1.14.3 Los datos de eventos ANPR para el mismo vehículo que se registran múltiples veces dentro de múltiples zonas dentro de un período de tiempo específico crearán una alarma.

11 Pasarela de Gestión de Alarmas

Capacidades generales

11.1.1 El sistema debe proporcionar una función de gestión de alarmas para informar y gestionar las alarmas locales y remotas del sistema.

11.1.2 El sistema deberá ser capaz de conectarse a una unidad AMG a través de la interfaz del operador.

11.1.3 El sistema deberá permitir la conexión de los sistemas mediante TCP/IP, a través de LAN/WAN.

11.1.4 La solución de la sala de control del sistema deberá ser capaz de transmitir y supervisar el audio de forma bidireccional.

11.1.5 El sistema de gestión de alarmas deberá supervisar las conexiones con las unidades remotas a través de un latido del sitio a intervalos establecidos. Generará un disparo cuando una unidad de alarma remota no envíe su latido.

11.1.6 El sistema de gestión de alarmas deberá permitir el envío de SMS de alarmas técnicas y de eventos.

11.1.7 La interfaz de alarmas deberá ser de acceso controlado, independiente del resto del software, y tendrá su propia utilidad de gestión de usuarios.

Interfaz AMG

11.1.8 El sistema deberá permitir a los operadores de la sala de control utilizar múltiples interfaces de monitor, con los escritorios de Alarmas, Recursos, Mapas y otro software repartido entre los monitores.

11.1.9 La interfaz de alarma del sistema deberá contar con un indicador gráfico claramente visible del estado de la conexión de la pasarela (conectada o desconectada). El sistema se configurará opcionalmente para que, al conectarse, el operador vea la configuración del escritorio/pantalla personalizada por el cliente, la información de la alarma y el mapa correspondiente a esa alarma en particular.

11.1.10 El sistema deberá permitir la configuración del mapa para que un icono de alarma de evento parpadee en el punto apropiado donde se inició la alarma.

11.1.11 El sistema deberá mostrar las alarmas en paneles separados según su estado:
11.1.11.1 Entrante (a la espera de ser atendida por un operador).
11.1.11.2 En curso (siendo tratada por un operador).
11.1.11.3 Archivado (ya manejado por un operador).

11.1.12 El sistema debe permitir personalizar las notificaciones de audio de las alarmas entrantes.

11.1.13 El sistema deberá mostrar las alarmas según su prioridad, indicada por diferentes colores, tal y como se ha configurado para las alarmas de eventos.

11.1.14 En una cola de alarmas entrantes no atendidas, el sistema hará sonar la notificación de audio de la alarma de mayor prioridad durante treinta segundos hasta que sea atendida.

11.1.15 Cuando varios operadores manejen las alarmas, el sistema mantendrá a todos los operadores informados sobre el estado de una alarma, y sobre quién está manejando cada alarma.

11.1.16 Incluso cuando se navegue fuera del escritorio de la cola de alarmas, el sistema deberá mostrar una barra de estado de alarmas que indique el número de alarmas entrantes y no gestionadas por prioridad codificada por colores.

Acciones del operador

11.1.17 El sistema deberá permitir a los operadores responder a una alarma y conectarse automáticamente al sitio desde donde se inició la alarma.

11.1.18 El sistema deberá ser capaz de deshabilitar temporalmente (bloquear) las alarmas inválidas repetitivas durante períodos específicos. Este bloqueo se especificará desde la unidad de la pasarela, y requerirá un comentario explicativo por parte del operador que bloquea.

11.1.19 El sistema deberá permitir a los operadores borrar simultáneamente múltiples alarmas de la cola de entrada.

11.1.20 El sistema deberá permitir a los operadores manejar múltiples alarmas remotas simultáneamente - una pestaña de interfaz separada deberá representar cada conexión.

11.1.21 El sistema debe permitir a los operadores añadir comentarios a las alarmas actuales y archivadas. Para facilitar las respuestas rápidas, los comentarios predeterminados se podrán seleccionar desde un menú, pero también será posible añadir comentarios de texto personalizados.

11.1.22 El sistema deberá permitir a los operadores modificar el menú de comentarios por defecto con comentarios personalizados más adecuados.

11.1.23 El sistema deberá permitir a los operadores escalar electrónicamente una alarma a un "caso", y asignar personas para investigar, alertando e involucrando así a las estructuras de gestión de la seguridad.

11.1.24 El sistema deberá notificar la asignación de casos a los usuarios a los que se les haya escalado.

11.1.25 El sistema deberá permitir a los operadores crear un caso independientemente de una alarma.

11.1.26 El sistema deberá proporcionar una utilidad de gestión de casos con la que gestionar los casos, permitir la colaboración electrónica entre todas las partes asignadas, comprometer al personal importante en el proceso, y garantizar que el caso tiene que ser debidamente resuelto/firmado antes de que pueda ser "cerrado".

11.1.27 El sistema deberá permitir a los gestores de casos escalar los casos a niveles superiores de inspección.

11.1.28 El sistema deberá permitir a los operadores filtrar las alarmas históricas utilizando sus grabaciones y metadatos asociados. Los parámetros de filtrado deberán incluir:

11.1.28.1 Alarmas, sesiones (cuando se hayan enviado varias alarmas en una sola conexión).

11.1.28.2 Operador de la sala de control (basado en la información de acceso).

11.1.28.3 Casos (alarmas que fueron escaladas para una mayor investigación).

11.1.29 El sistema debe permitir a los operadores hacer doble clic en una entrada (alarma, sesión, inicio de sesión del operador, caso) desde la interfaz de alarmas históricas, para mostrar una pantalla de información/acción más detallada relacionada con esa entrada, desde la cual será posible hacer lo siguiente:

11.1.29.1 Ver el nombre del sitio de la alarma.

11.1.29.2 Ver el nombre del servidor de alarmas.

11.1.29.3 Ver la descripción de la alarma.

11.1.29.4 Ver el operador de la sala de control que manejó una alarma o una sesión.

11.1.29.5 Ver el nombre de la unidad de la sala de control a través de la cual se gestionó una alarma o una sesión.

11.1.29.6 Ver la hora de un evento de alarma.

11.1.29.7 Ver la hora en que se envió un evento de alarma a la sala de control.

11.1.29.8 Ver la hora de llegada de una alarma a la sala de control.

11.1.29.9 Ver el tiempo que tarda el operador de la sala de control en gestionar una alarma.

11.1.29.10 Ver los comentarios asociados a las alarmas, sesiones y casos.

11.1.29.11 "Añadir comentario y cerrar alarma" al añadir un comentario desde la ventana de reproducción de vídeo de la alarma. Una vez añadido el comentario, la alarma se cerrará.

11.1.29.12 Ver las grabaciones asociadas a una alarma.

11.1.29.13 Conectar con el sitio histórico de la alarma para obtener más grabaciones asociadas a la alarma, si todavía existen en la base de datos del sitio remoto.

11.1.29.14 Ver los casos asociados a una alarma.

11.1.29.15 Mostrar toda la Sesión en la que se ha gestionado una alarma.

11.1.29.16 Añadir más comentarios a las alarmas, sesiones y casos históricos.

11.1.29.17 Escalar una alarma histórica a un Caso para una mayor investigación y resolución.

11.1.29.18 Mostrar los inicios de sesión del Operador de la sala de control asociados a una sesión de alarma.

11.1.29.19 Ver todas las alarmas asociadas a una sesión.

11.1.29.20 Ver la duración del inicio de sesión del operador de la sala de control, la hora de inicio y la hora de finalización.

11.1.29.21 Ver el número de sesiones gestionadas por un operador de sala de control durante un inicio de sesión.

11.1.29.22 Ver todas las sesiones gestionadas por un operador de la sala de control durante un inicio de sesión.

11.1.29.23 Ver la descripción de un caso.

11.1.29.24 Ver el nombre del usuario que escaló una alarma a un Caso, con la fecha-hora.

11.1.29.25 Ver el nombre del usuario que cerró un Caso, con la fecha-hora.

11.1.29.26 Vea una lista de usuarios de Casos, con su Estado relacionado con un Caso (Activo - aún trabajando en él, o Inactivo - ya no trabajando en él).

11.1.29.27 Ver una línea de tiempo de las acciones del usuario relacionadas con un caso.

11.1.29.28 Ver el estado de un caso.

11.1.29.29 Ver todas las alarmas asociadas a un caso.

11.1.29.30 Ver todos los comentarios asociados a un caso.

Informes AMG

11.1.30 El sistema debe proveer reportes detallados y personalizables basados en conexiones, tiempos de respuesta, inicios de sesión y tiempos de manejo.

11.1.31 El sistema debe establecer una pista de auditoría y una línea de tiempo de las respuestas de los casos.

11.1.32 El sistema deberá registrar los inicios de sesión de los operadores y las respuestas a las llamadas entrantes, y proteger esta información contra la manipulación.

11.1.33 El sistema deberá ser capaz de programar el sistema para ejecutar informes automáticamente, y realizar acciones automatizadas con los informes, tales como enviarlos por correo electrónico a los destinatarios.

12 Teclado integrado

Teclado/Controlador nativo

12.1.1 El sistema deberá contar con un control de teclado integrado.

12.1.2 El sistema deberá permitir que la sensibilidad de paneo/inclinación/zoom sea configurada en el software.

12.1.3 El teclado debe permitir la selección rápida de cámaras, preajustes, monitores, salidas, recorridos de cámara (secuencias) y diseños de pantalla.

12.1.4 Los botones de función de la cámara PTZ deberán ser accesibles a los dedos de la mano del joystick, para que los operadores no tengan que renunciar al control del mismo.

12.1.5 La pantalla LCD del teclado deberá poder ser escrita por el sistema de vigilancia digital.

12.1.6 Los LED de las teclas del teclado deberán indicar el estado de las teclas y las funciones.

Teclado/Controlador de terceros

12.1.7 El sistema deberá soportar la integración de teclados y controladores de terceros.

13 Bases de datos

Capacidades generales

13.1.1 El sistema deberá proporcionar un acceso rápido y fácil a todas las bases de datos desde la interfaz del operador.

13.1.2 El sistema deberá permitir la configuración de múltiples bases de datos y la dirección de múltiples cámaras y/o grupos de cámaras a una o más bases de datos.

13.1.3 El sistema deberá restringir la visualización de las entradas de la base de datos, permitiendo que sólo los usuarios con los derechos de acceso a la cámara adecuados puedan ver determinadas cámaras de la base de datos.

Base de datos de vídeo

13.1.4 El sistema deberá proporcionar un sistema de base de datos de vídeo propio, que no dependa de motores de bases de datos de terceros (como PostgreSQL y MySQL).

13.1.5 El sistema deberá ser capaz de dividir las bases de datos en múltiples discos y/o dispositivos de almacenamiento en red.

13.1.6 El sistema debe continuar escribiendo en una base de datos incluso si uno o varios discos fallan.

13.1.7 El sistema soporta las siguientes características de la base de datos:
13.1.7.1 Tamaños de disco variables
13.1.7.2 Distribución de la carga de escritura en varios discos.
13.1.7.3 Las bases de datos se pueden exportar y mover de un NVR a otro.
13.1.7.4 Ampliación de la base de datos existente añadiendo más espacio de almacenamiento.
13.1.7.5 Ofrecer la posibilidad de recuperación de la corrupción del sistema de archivos con pérdida mínima de datos.

13.1.8 El sistema deberá ser capaz de visualizar las entradas de la base de datos según la selección de la fecha y la hora.

13.1.9 El sistema deberá permitir la configuración de un período máximo de registro.

Base de datos de metadatos (integración)

13.1.10 El sistema deberá ser capaz de crear bases de datos de integración específicas para cada integración. Las bases de datos de integración deberán:
13.1.10.1 Tener un reproductor de vídeo integrado.
13.1.10.2 Vincular los datos del dispositivo integrado con los datos de vídeo extraídos de las cámaras asociadas.
13.1.10.3 Reproducir vídeo y datos de forma simultánea y sincronizada en el reproductor de vídeo de la base de datos integrada.
13.1.10.4 Mostrar todas las cámaras asociadas a los eventos del dispositivo.
13.1.10.5 Realizar una "búsqueda fácil" a través de una interfaz de usuario desplegable que filtre instantáneamente las entradas según las opciones de búsqueda fácil disponibles (únicas para cada integración).

13.1.10.6 Proporcionar la capacidad de "minar" la base de datos para encontrar los datos/transacciones seleccionados y los datos de vídeo asociados, utilizando filtros específicos de la integración y opciones de visualización/búsqueda/ordenación.
13.1.10.7 Ser capaz de exportar las entradas de la base de datos en formato PDF y CSV.
13.1.10.8 Ser capaz de archivar vídeo y metadatos asociados desde el reproductor de vídeo de la base de datos de integración.
13.1.10.9 Ser capaz de crear informes programados de la base de metadatos.
13.1.10.10 Ser capaz de ampliar el filtrado de informes

Base de datos de eventos del sistema

13.1.11 El sistema deberá ser capaz de crear una base de datos específica de eventos a la cual todos los eventos del sistema son dirigidos automáticamente, sin necesidad de configurar una acción de evento a registrar.

Base de Datos de Integración ANPR

13.1.12 El sistema deberá ser capaz de crear una base de datos de integración ANPR designada.

13.1.13 El sistema deberá ser capaz de ver, ordenar y "buscar fácilmente" la base de datos ANPR por lo siguiente:
13.1.13.1 Matrículas.
13.1.13.2 Grupos de matrículas.
13.1.13.3 Detectores ANPR/LPR.

13.1.14 El sistema debe ser capaz de filtrar la base de datos ANPR por un número de opciones, incluyendo pero no limitado a lo siguiente:
13.1.14.1 Hora/fecha.
13.1.14.2 Matrículas/Grupos
13.1.14.3 Confianza (precisión de la captura de matrículas en porcentaje).
13.1.14.4 Detector ANPR.
13.1.14.5 Cámara.
13.1.14.6 Nombre del conductor/empresa.
13.1.14.7 Tipo/marca/modelo/color del vehículo.
13.1.14.8 Lugar de emisión (específico de la región).
13.1.14.9 Color de fondo, color del texto y forma de la matrícula.
13.1.14.10 Posición de la matrícula en el vehículo (delante/detrás).
13.1.14.11 Posición del coche en el carril (entrada/salida).

Base de datos de clasificación de objetos

13.1.15 El sistema deberá ser capaz de crear una base de datos de integración para almacenar el vídeo grabado asociado al seguimiento y la clasificación de objetos.

13.1.16 Además de poseer todas las características de la base de datos de integración (apartado 13.3), la base de datos de seguimiento de objetos deberá proporcionar metadatos sobre el objeto clasificado, que podrán mostrarse en superposiciones.

13.1.17 Los metadatos de clasificación de objetos incluyen:
13.1.17.1 Clasificación de objetos realizada.

13.1.17.2 Nivel de confianza de la clasificación.
13.1.17.3 Color y color alternativo del objeto.
13.1.17.4 Hora de inicio y fin de la clasificación.
13.1.17.5 Tamaño (anchura y altura en cm) del objeto.
13.1.17.6 Velocidad del objeto.

14 Failover

Capacidades generales

14.1.1 El sistema deberá ser capaz de realizar una Failover de n:1 y n:n servidores.

14.1.1.1 Un servidor de Failover puede asumir las funciones de cualquier servidor que falle.

14.1.1.2 Para ello se utilizará una estructura hotspare.

14.1.2 El sistema deberá ser capaz de fallar sobre el Servidor Maestro/Gestión, y todas las funciones asociadas, incluyendo pero no limitado a:

14.1.2.1 Grabación y revisión de video.

14.1.2.2 Visualización de vídeo en directo, incluyendo las funciones de control del videowall.

14.1.2.3 Configuración y gestión de eventos.

14.1.3 El sistema deberá ofrecer la opción de una configuración sencilla de Failover durante el proceso de instalación del software VMS.

14.1.4 El sistema debe proporcionar una base de datos de Failover que resida en el propio servidor de Failover

Proceso de Failover

14.1.5 El servidor de Failover supervisará continuamente los servidores de gestión y grabación.

14.1.6 El servidor de Failover asumirá la funcionalidad de un servidor fallido, permitiendo que las funciones del sitio continúen.

14.1.7 El sistema reintroducirá automáticamente el vídeo en la base de datos del servidor de grabación original al recuperarse el servidor que ha fallado.

14.1.8 El sistema generará una alarma si un servidor del sitio falla y es sustituido por otro.

14.1.9 El sistema deberá generar una alarma si un servidor de Failover no funciona.

14.1.10 El sistema deberá proporcionar una función de resumen del sitio que muestre todos los servidores del sitio, indicando el servidor que está siendo conmutado por error.

15 Salud del sistema

Informes Técnicos

15.1.1 El sistema deberá ofrecer una amplia información sobre el hardware y el software que componen el sitio, manteniendo registros técnicos y permitiendo la generación de informes técnicos.

15.1.2 El sistema deberá restringir el acceso a la configuración de los informes técnicos únicamente a los administradores.

15.1.3 El sistema deberá permitir a los usuarios guardar sus informes como "plantillas" para facilitar la generación de futuros informes.

15.1.4 El sistema deberá permitir a los usuarios exportar informes en formato html comprimido.

15.1.4.1 En formato html, el sistema deberá permitir la generación automática de un índice de contenidos y de hipervínculos a las secciones.

15.1.5 El sistema deberá permitir que los informes se envíen por correo electrónico, se impriman y se archiven (guarden).

15.1.6 El sistema deberá ser capaz de compilar y enviar automáticamente por correo electrónico los informes seleccionados a los destinatarios seleccionados de acuerdo con un calendario especificado.

15.1.7 El sistema deberá ser capaz de generar informes técnicos específicos del servidor/hardware sobre lo siguiente:

15.1.7.1 Fallos de la cámara, registros, estado y tiempo de reparación.

15.1.7.2 Uso de la base de datos:

15.1.7.2.1 Desglose por cámara.

15.1.7.2.2 Tasa por cámara/hora/cámara por hora.

15.1.7.2.3 Histograma de frecuencia de eventos.

15.1.7.2.4 Eventos por hora.

15.1.7.3 Disco.

15.1.7.4 Entorno.

15.1.7.5 Eventos.

15.1.7.6 Sistemas de archivos.

15.1.7.7 Hardware.

15.1.7.8 Características de la licencia.

15.1.7.9 Licencias.

15.1.7.10 Consultas NTP.

15.1.7.11 Reinicios y causas de reinicios, incluyendo:

15.1.7.12 Reinicios del servidor de software.

15.1.7.13 Reinicios por fallo de alimentación.

15.1.7.14 Reinicios de usuario.

15.1.7.15 Reinicios de usuarios remotos.

15.1.7.16 Hora de reinicio.

15.1.7.17 Instalación y configuración de la grabación, tiempos (del sistema por cámara) y fallos de grabación.

15.1.7.18 Instalación y configuración del sistema.
15.1.7.19 Fallos del servidor de software.
15.1.7.20 Tiempo de funcionamiento de la unidad.
15.1.7.21 VMX:
15.1.7.21.1 Contadores.
15.1.7.21.2 Temperaturas.
15.1.7.21.3 Alertas de salud en la barra de estado. Se mostrará un mensaje si el disco en el que está instalado el NVR se está llenando.

Alarmas técnicas

15.1.8 El sistema deberá ser capaz de generar alarmas técnicas específicas del servidor/hardware, incluyendo pero no limitándose a:
15.1.8.1 Alarmas de fallo de latido.
15.1.8.2 Fallos de la cámara, si:
15.1.8.2.1 Por ejemplo, las cámaras fallan más de un número determinado de veces en un periodo de tiempo específico.
15.1.8.2.2 Por ejemplo, las cámaras no funcionaron durante más de un porcentaje específico de tiempo en un período determinado.
15.1.8.3 Alarmas de base de datos (generadas cuando se dispara un evento pero no se recibe vídeo).
15.1.8.4 Alarmas de disco.
15.1.8.4.1 Por ejemplo, parámetros SMART del disco duro fuera de las normas requeridas por el sistema.
15.1.8.5 Alarmas de entorno (dependientes del servidor/hardware).
15.1.8.5.1 Por ejemplo, temperatura, velocidad del ventilador.
15.1.8.6 Alarmas de Failover.
15.1.8.7 El servidor ha fallado.
15.1.8.8 El servidor de Failover falla.
15.1.8.9 Alarmas de la base de datos de integración.
15.1.8.10 Alarmas de E/S de red.
15.1.8.11 Alarmas de conectividad de red.
15.1.8.11.1 Por ejemplo, si falla un medio de comunicación, como Ethernet o un módem.
15.1.8.11.2 Por ejemplo, si ha fallado un ping rutinario de la pasarela de gestión de alarmas de una estación de captura.
15.1.8.12 Alarmas de reinicio, Por ejemplo, si la frecuencia de reinicio es inusualmente alta.
15.1.8.13 Alarmas de periodo de grabación/fallo.
15.1.8.13.1 Por ejemplo, si el número de eventos registrados en un día concreto es inferior al que debería ser (basado en una media histórica), lo que indica un posible fallo técnico.
15.1.8.14 Alarma de archivo programado.
15.1.8.15 Alarma de monitorización del servidor.
15.1.8.15.1 Por ejemplo, si se ha producido una secuencia de apagado inusual (por ejemplo, si un usuario retira el cable de alimentación).
15.1.8.15.2 P. ej., todos los sistemas deberán comprobar continuamente el "tiempo de actividad" de todos los demás sistemas del sitio y, si alguno de ellos no responde, podrá enviarse una alarma.

15.1.8.16 Alarma de fallo de software.

15.1.8.17 Alarma de prueba.

15.1.8.18 Deberá ser posible activar una alarma técnica de prueba desde una sola unidad dentro de un sitio de unidades.

15.1.8.19 El envío de alarmas deberá contar con filtros que permitan a los usuarios limitar el número de alarmas enviadas. Estos ajustes deberán incluir:

15.1.8.19.1 Enviar alarma cada vez que ocurra un evento.

15.1.8.19.2 Enviar alarma inmediatamente y luego cada período de tiempo especificado.

15.1.8.19.3 Enviar la alarma sólo una vez.

16 Registros de auditoría

Capacidades generales

16.1.1 El sistema debe permitir que el sitio y los servidores sean auditados, proporcionando un registro histórico de todas las acciones basadas en el usuario.

16.1.2 El sistema debe restringir el acceso a la auditoría de sitios y servidores sólo a los administradores.

16.1.3 El sistema debe permitir que los registros de auditoría sean filtrados por lo siguiente:

16.1.3.1 Tiempo/Periodo de tiempo

16.1.3.2 Usuarios

16.1.3.3 Recursos

16.1.3.4 Acciones del usuario

16.1.4 El sistema deberá permitir que los registros de auditoría filtrados por usuarios muestren un registro histórico de las acciones del operador, a través de todos los nombres de inicio de sesión del usuario.

16.1.5 El sistema debe permitir exportar los registros de auditoría en formato de archivo CSV.

17 Herramienta forense

Capacidades generales

17.1.1 El sistema deberá disponer de una herramienta forense que ofrezca un análisis del sitio y una solución de problemas para obtener los siguientes datos históricos del servidor del sitio:

17.1.1.1 Resumen de la cámara de red: rendimiento total de la red, proporción de caídas y recuento de paradas de la cámara.

17.1.1.2 Escrituras en la base de datos: tasa de bits de escritura en el disco y caídas en el almacenamiento local o de red.

17.1.1.3 Paquetes perdidos - red externa, UDP interno entre servidores y fotogramas de vídeo internos.

17.1.1.4 Transmisión de vídeo - enviado, recibido y decodificado para su visualización en directo.

17.1.1.5 Compresor de software - tasa de píxeles codificada y decodificada, y porcentaje de fotogramas.

17.1.1.6 Mensajería interna - paquetes UDP perdidos y recibidos entre procesos, y número de registros por minuto enviados.

17.1.1.7 Fotogramas de vídeo - perdidos y recibidos entre procesos internos.

17.1.1.8 El sistema deberá disponer de una herramienta forense para solucionar problemas y obtener los siguientes datos históricos específicos de la cámara:

17.1.1.9 Cámaras de red - tasa de bits, paquetes perdidos, cámaras paradas, cámaras caídas y número de eventos por cámara.

17.1.1.10 Cámaras de la base de datos: tasa de bits, bytes escritos en el disco, cámaras inactivas y número de eventos por cámara.

17.1.2 El sistema deberá tener una disposición para presentar los datos forenses en un formato gráfico basado en lo siguiente:

17.1.2.1 Selección de fecha y hora.

17.1.2.2 Selección del marco temporal.

17.1.2.3 El sistema deberá contar con una disposición, mientras que en la Ventana Gráfica, para facilitar lo siguiente:

17.1.2.4 Acercarse a un periodo de tiempo de los datos.

17.1.2.5 Ver los valores de los datos.

17.1.2.6 Exportar como archivo CSV.

18 Ciberseguridad

Capacidades generales

18.1.1 El sistema debe emplear medidas de seguridad de hardware, software y ciberseguridad para reducir el riesgo de acceso a la información y la manipulación de los datos.

18.1.1.1 Estas medidas deben ser empleadas por el VMS junto con los procedimientos estándar de seguridad informática, incluyendo:

18.1.1.1.1 Controlar adecuadamente el acceso a la red con técnicas como:

18.1.1.1.1.1 Implementar cortafuegos.

18.1.1.1.1.2 Utilizar conmutadores de red inteligentes.

18.1.1.1.1.3 Gestionar y controlar el acceso "físico" a la red.

18.1.1.1.2 Prevención del acceso no autorizado al sistema operativo con técnicas como:

18.1.1.1.2.1 Impedir la apertura de puertos no autorizados que permitan el uso de elementos como ftp, telnet, correo electrónico, etc. Si es necesario que la comunicación se produzca a través de estos medios, asegúrese de que se utilizan protocolos de seguridad como SSH/SFTP.

18.1.1.1.2.2 Desactivar el acceso "root" al sistema operativo.

18.1.1.1.2.3 Asegurar niveles de contraseñas fuertes.

18.1.1.1.2.4 Añadir software antivirus y antimalware (que debe actualizarse con frecuencia).

18.1.1.1.2.5 Restringir el acceso a Internet.

Comunicación segura entre los componentes del VMS

18.1.2 El sistema debe garantizar una comunicación segura entre los componentes del VMS, incluyendo:

18.1.2.1 Servidores de grabación a clientes.

18.1.2.2 Servidores de grabación a otros servidores de grabación.

18.1.2.3 Servidores de grabación a Video Walls.

18.1.2.4 Servidores de grabación a la pasarela de gestión de alarmas.

18.1.3 Las siguientes medidas de seguridad se emplean durante la comunicación entre los componentes del VMS:

18.1.3.1 El motor de encriptación deberá utilizar openssl (hashes SHA512, DH-RSA efímero con forward secrecy [DH 2048 bit] y cifrados simétricos AES-GCM de 128 bits) equivalente a TLS 1.3.

18.1.3.2 Las contraseñas nunca se almacenan como texto plano, sino que se etiquetan con hash usando SHA512.

18.1.3.3 Las credenciales de inicio de sesión se negocian utilizando RSA1024.

18.1.3.4 Los canales de comunicación sensibles son encriptados usando AES128/CBC.

18.1.3.5 Se utiliza HMAC para la verificación de la integridad.

18.1.3.6 Todas las conexiones externas del sitio soportan varios niveles de encriptación:

18.1.3.6.1 Desactivado.

18.1.3.6.2 Mínimo - sólo se cifrarán las conexiones críticas.

18.1.3.6.3 Seguro (por defecto) - todas las conexiones excepto las de alto volumen de video deben ser encriptadas.

18.1.3.6.4 Todo - todas las conexiones, incluyendo las de alto volumen de video, deben ser encriptadas.

18.1.3.7 La infraestructura de clave pública (PKI) es gestionada internamente por el VMS para mayor seguridad.

Seguridad de vídeo

18.1.4 El sistema debe garantizar la seguridad e integridad del video grabado a través de los siguientes medios:

18.1.4.1 Se utilizan claves dobles RSA1024 (para la firma) para asegurar la integridad del vídeo que se exporta/archiva.

18.1.4.2 El cifrado opcional utiliza el cifrado de bloques AES128 con un IV aleatorio por bloque y una frase de contraseña generada por el usuario.

18.1.4.3 El vídeo puede llevar una marca de agua para indicar el origen de la información (es decir, información del usuario).

18.1.4.4 Las secuencias de vídeo y los metadatos están restringidos a la reproducción a través del reproductor de vídeo propietario del VMS.

18.1.4.5 El vídeo exportado/archivado puede estar restringido a la reproducción controlada por contraseña.

Seguridad de las cámaras IP

18.1.5 El sistema deberá, en la medida en que estas medidas sean admitidas por los fabricantes, garantizar la seguridad de las cámaras IP conectadas por los siguientes medios:

18.1.5.1 Conexión segura de la cámara:

18.1.5.1.1 HTTP: protocolo de transferencia de hipertexto.

18.1.5.1.2 Conexiones de control cifradas HTTPS.

18.1.5.1.3 SSL/TLS cifrado.

18.1.5.1.4 Soporte de CURL (biblioteca de transferencia de URL del lado del cliente).

18.1.5.2 Control seguro de la cámara:

18.1.5.2.1 RTSP - protocolo de transmisión en tiempo real.

18.1.5.2.2 Control cifrado HTTPS.

18.1.5.3 Transmisión segura de vídeo:

18.1.5.3.1 RTP - control de transporte en tiempo real.

18.1.5.3.2 Vídeo encriptado.

19 Editor de mapas

Software del Editor de Mapas

19.1.1 Capacidades generales

19.1.1.1 El sistema debe instalar automáticamente una facilidad de mapa interactivo multi-capa al instalar el software del servidor/cliente VMS.

19.1.1.2 La instalación de mapas deberá ser jerárquica con capacidad de "drill-down".

19.1.2 Interfaz

19.1.2.1 La interfaz del Editor de Mapas deberá ser capaz de hacer lo siguiente:

19.1.2.1.1 Añadir/configurar objetos de mapa (como formas, imágenes y texto).

19.1.2.1.2 Agregar recursos del sitio al mapa (como cámaras, dispositivos de integración, eventos).

19.1.2.1.3 Agregar acciones a los objetos del mapa.

19.1.2.1.4 Conectarse al sitio(s) y ver los recursos del sitio.

19.1.3 Funciones

19.1.3.1 El sistema debe incluir, entre otras, las siguientes funciones de creación de mapas:

19.1.3.1.1 Asistente de configuración de mapas para ofrecer una función de creación rápida.

19.1.3.1.2 Importación de gráficos en formato JPG o PNG.

19.1.3.1.3 Crear hipervínculos desde el mapa a otros mapas del sitio.

19.1.3.1.4 Los objetos del mapa pueden ser configurados para realizar acciones del mapa al recibir ciertos disparadores.

19.1.3.1.5 Capas del mapa; las capas tienen opciones de transparencia / ocultar.

19.1.3.1.6 Capacidad de asociar capas con posiciones PTZ preestablecidas.

19.1.3.1.7 Capacidad de activar o desactivar capas en respuesta a un evento del sistema (por ejemplo, para indicar la apertura/cierre de una puerta).

19.1.3.1.8 PTZ con preajustes asociados y editables.

19.1.3.1.9 Arrastre todos los recursos de sitio disponibles desde una lista de recursos de sitio directamente al mapa.

19.1.3.1.10 Añadir cámaras con iconos de arrastrar y soltar (fijas o PTZ).

19.1.3.1.11 Añadir E/S mediante iconos de arrastrar y soltar.

19.1.4 Acciones de los objetos del mapa

19.1.4.1 Los objetos de mapa pueden ser configurados para realizar ciertas acciones al recibir determinados disparadores. Ejemplos de disparadores que pueden desencadenar una acción de objeto de mapa incluyen, pero no se limitan a, los siguientes:

19.1.4.1.1 Hacer clic con el botón izquierdo del ratón en la pestaña Mapa de la interfaz de usuario de VMS.

19.1.4.1.2 Hacer clic con el botón derecho del ratón en la pestaña Mapa de la interfaz de usuario VMS.

19.1.4.1.3 Cambio de entrada,

19.1.4.1.4 Cambio de estado del dispositivo,

19.1.4.1.5 Eventos del dispositivo de integración.

19.1.4.1.6 Los ejemplos de acciones que los objetos de mapa pueden realizar cuando se recibe un activador incluyen, entre otros, los siguientes

19.1.4.1.7 Conectar a un sitio,

19.1.4.1.8 Ir a un preajuste de cámara,
19.1.4.1.9 Realizar una animación,
19.1.4.1.10 Mostrar un menú emergente,
19.1.4.1.11 Establecer una salida de relé.

Mapas en la interfaz del operador VMS

19.1.5 El sistema deberá permitir que los mapas creados en el software Editor de mapas y guardados se carguen en la pestaña Mapa de la interfaz del operador VMS.

19.1.6 El sistema debe permitir que se añadan múltiples mapas a un sitio.

19.1.7 El sistema deberá permitir, opcionalmente, que los usuarios remotos vean automáticamente el mapa del sitio.

19.1.8 El sistema deberá permitir a los clientes remotos descargar y almacenar los mapas localmente para evitar la necesidad de descargar el mapa para cada conexión.

19.1.9 El sistema deberá permitir la gestión de los mapas del sitio, lo que implica:
19.1.9.1 Establecer un mapa por defecto,
19.1.9.2 Borrar mapas,
19.1.9.3 Añadir mapas.

19.1.10 El sistema deberá permitir que todas las acciones del objeto de mapa que se configuraron para el objeto en el software Editor de Mapas sean visibles/funcionantes/interactivas (cuando sea relevante) en el mapa en la interfaz de usuario del VMS.

19.1.11 El sistema debe permitir al usuario:
19.1.11.1 Acercarse/alejarse del mapa,
19.1.11.2 Arrastrar y soltar cámaras del mapa a los monitores para su visualización,
19.1.11.3 Ocultar/mostrar objetos del mapa,
19.1.11.4 Ocultar/mostrar/cambiar la transparencia de las capas.

20 Aplicación móvil

Capacidades generales

20.1.1 El sistema deberá proporcionar una aplicación móvil gratuita.

20.1.2 El sistema no deberá requerir la instalación de software adicional del lado del servidor, plug-ins adicionales o un servidor móvil especial para permitir la visualización y revisión de vídeo en el móvil.

20.1.3 El sistema deberá hacer que esta aplicación esté disponible en la iStore de Apple y en Google Play Store.

20.1.3.1 Deberá ser accesible a través de una interfaz HTTP.

20.1.4 La aplicación deberá soportar las siguientes funciones:

20.1.4.1 Control PTZ de las cámaras.

20.1.4.2 Acercar/alejar el zoom.

20.1.4.3 Control de E/S.

20.1.4.4 Vista de múltiples cámaras (hasta cuatro cámaras).

20.1.4.5 Guardar detalles para múltiples servidores.

21 Interfaz de programación de aplicaciones

Capacidades generales

21.1.1 El sistema debe incluir una Interfaz de Protocolo de Aplicación (API) que permita al software de terceros recuperar y gestionar la información del VMS, así como controlar los recursos del sistema.

Información de la lista de sitios

21.1.2 El sistema deberá incluir lo siguiente con respecto a la información de la Lista de Sitios:

21.1.2.1 El acceso al sitio deberá ser a través de la autenticación de digest, y restringido en base a los niveles de acceso preconfigurados del usuario. La API deberá tener acceso a los detalles del sitio, a través del servidor de acceso. Esto incluye el nombre del sitio y el número de identificación único.

21.1.3 El sistema deberá incluir lo siguiente con respecto a los Recursos de la Cámara:

21.1.3.1 La API deberá proporcionar la capacidad de listar todas las cámaras y recursos de cámaras de un sitio, excepto:

21.1.3.1.1 Los feeds con formatos de video no soportados por RTSP serán excluidos de la lista de cámaras de la API.

21.1.4 El sistema deberá incluir lo siguiente con respecto a la información de alimentación de la cámara:

21.1.4.1 Nombre,
21.1.4.2 ID único,
21.1.4.3 Alimentación de audio (sí/no),
21.1.4.4 Información sobre el nivel de acceso,
21.1.4.5 Estado de la cámara "Online/Offline",
21.1.4.6 Estado de PTZ,
21.1.4.7 Información de patrones/preajustes,
21.1.4.8 Información de la pista de vídeo en directo,
21.1.4.9 Información de la pista de vídeo de revisión.
21.1.4.10 La capacidad de reasignar la dirección IP del servidor interno que la API publica para una cámara.
21.1.4.11 Una interfaz de línea de tiempo.

21.1.5 El sistema deberá incluir lo siguiente en lo que respecta a la transmisión en directo:

21.1.5.1 La API deberá permitir la transmisión de video en vivo de la cámara, utilizando el protocolo RTSP.
21.1.5.2 La transmisión de video en vivo debe requerir autenticación del cliente.
21.1.5.3 Cambiar cámaras a monitores.
21.1.5.4 Transmisión web compatible con HTTP/HTML5.

21.1.6 El sistema deberá incluir lo siguiente respecto a la revisión de cámaras:

21.1.6.1 La API deberá permitir la revisión de las secuencias de video grabadas.
21.1.6.2 Se deberá acceder a través del protocolo RTSP.

21.1.6.3 La API deberá permitir la revisión de secuencias de vídeo a partir de una fecha y hora determinadas.
21.1.6.3.1 Si no hay secuencias de vídeo a la hora especificada, el servidor devolverá las secuencias de vídeo más cercanas a la hora solicitada.
21.1.6.4 La API debe permitir un campo en la solicitud que haga que la sesión se transmita tan rápido como lo permita el cliente/conexión.
21.1.6.5 Deberán admitirse los siguientes transportes de streaming:
21.1.6.5.1 RTP sobre UDP.
21.1.6.5.2 RTP sobre TCP.

21.1.7 El sistema debe incluir lo siguiente con respecto a la llamada/escucha de audio:
21.1.7.1 La API deberá permitir la transmisión de entradas y salidas de audio independientes hacia y desde las entradas y salidas de audio en el servidor.
21.1.7.2 "Independiente" significa aquí que el audio no debe estar ligado al vídeo.
21.1.7.3 Esto deberá realizarse a través del protocolo SIP.

21.1.8 La API debe permitir el siguiente control sobre las cámaras PTZ:
21.1.8.1 Mover
21.1.8.2 Ir a preselección
21.1.8.3 Guardar preajuste
21.1.8.4 Control de enfoque/iris
21.1.8.5 Ejecutar patrón de preajuste (tour)
21.1.8.6 El control de la PTZ deberá ser vía HTTP.

21.1.9 El sistema deberá incluir lo siguiente en relación a la gestión de recursos de entrada/salida (HTTP; monitorear los cambios de estado de los recursos de E/S, controlar las salidas):
21.1.9.1 La API deberá soportar el monitoreo de todas las E/S del sitio.
21.1.9.2 A petición, la API proporcionará todas las E/S actuales del sitio.
21.1.9.3 La API también mantendrá una conexión abierta, por el tiempo que el cliente desee, y actualizará los recursos de E/S a través de esta conexión. Estas actualizaciones serán:
21.1.9.3.1 Cambios de estado de los recursos
21.1.9.3.2 Recursos añadidos
21.1.9.3.3 Recurso eliminado
21.1.9.3.4 Recurso modificado (cambio de nombre)
21.1.9.3.5 Los controles de salida deben ser Set, Clear y Pulse.

21.1.10 El sistema deberá incluir lo siguiente respecto a la recepción de eventos/alarmas técnicas:
21.1.10.1 La API deberá permitir la recepción de alarmas desde el servidor. Tanto las alarmas técnicas (alarmas relacionadas con el funcionamiento del sitio), como las alarmas de eventos (alarmas disparadas por eventos de VMS y E/S).
21.1.10.2 El servidor deberá entregar la siguiente información de alarmas:
21.1.10.2.1 ID del sitio de origen.
21.1.10.2.2 Nombre del sitio de origen.
21.1.10.2.3 Tipo de alarma (técnica/evento).
21.1.10.2.4 Nombre de la alarma.
21.1.10.2.5 Recursos de cámara asociados.