



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

**Mejora de la eficiencia operativa en la supervisión de
la seguridad electrónica de las empresas Planinvest,
Martinizing y Fucsa mediante la integración de sus
sistemas en una plataforma PSIM**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Alex Marcelino MEZA ESCOBAR

ASESOR

Mg. Jean Carlos MALCA FERNANDEZ

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Meza, A. (2026). *Mejora de la eficiencia operativa en la supervisión de la seguridad electrónica de las empresas Planinvest, Martinizing y Fucsa mediante la integración de sus sistemas en una plataforma PSIM*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Alex Marcelino Meza Escobar
Tipo de documento de identidad	DNI
Número de documento de identidad	46421080
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Jean Carlos Malca Fernandez
Tipo de documento de identidad	DNI
Número de documento de identidad	45535181
URL de ORCID	https://orcid.org/0000-0001-5633-5182
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa Esther Nuñez Zuñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
Miembro del jurado 1	
Nombres y apellidos	Jorge Elías Moscoso Sánchez
Tipo de documento	DNI
Número de documento de identidad	07206008
Miembro del jurado 2	
Nombres y apellidos	Celso Ysidro Geronimo Huaman
Tipo de documento	DNI
Número de documento de identidad	09191500
Datos de investigación	
Línea de investigación	C.0.6.2 Automatización y control
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: PLANINVEST País: Perú Departamento: Lima Provincia: Lima Distrito: San Isidro Latitud: -12.0920946 Longitud: -77.0433299
Año o rango de años en que se realizó la investigación	2021 – 2022
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01 Robótica, Control automático https://purl.org/pe-repo/ocde/ford#2.02.02



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



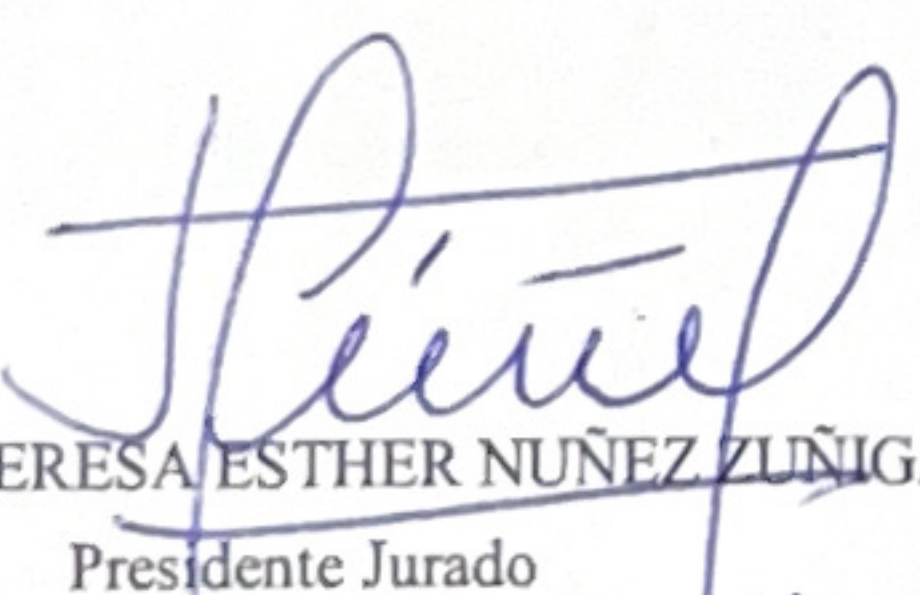
ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°19/FIEE-PPP/2026

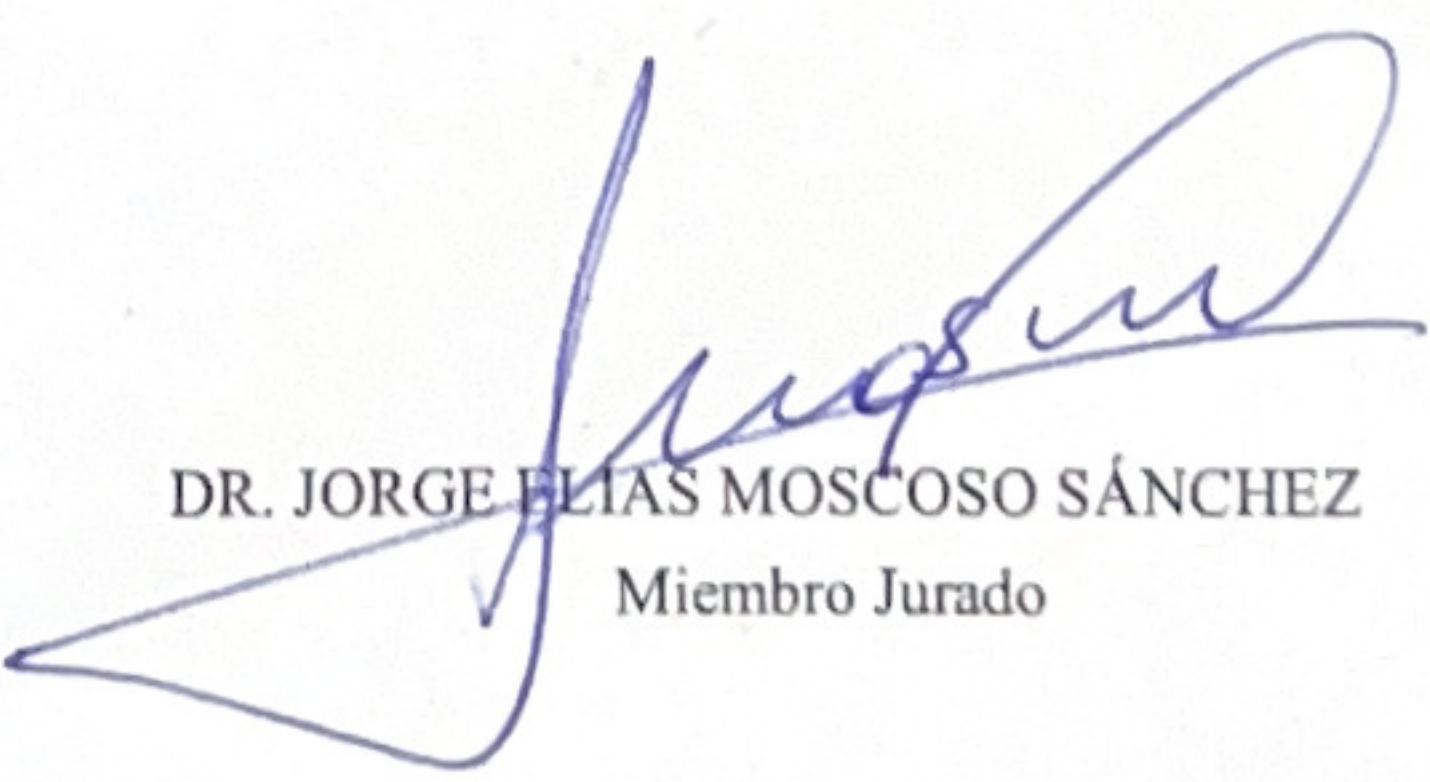
Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 07 de abril del 2026, como presidente de Jurado el **DRA. TERESA ESTHER NUÑEZ ZUÑIGA**, integrado por el Miembro de Jurado el **DR. JORGE ELÍAS MOSCOSO SÁNCHEZ**, el Miembro de Jurado el **DR. CELSO YSIDRO GERONIMO HUAMAN** y Miembro Asesor el **MG. JEAN CARLOS MALCA FERNANDEZ**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **ALEX MARCELINO MEZA ESCOBAR** con código 9190067 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **MEJORA DE LA EFICIENCIA OPERATIVA EN LA SUPERVISIÓN DE LA SEGURIDAD ELECTRÓNICA DE LAS EMPRESAS PLANINVEST, MARTINIZING Y FUCSA MEDIANTE LA INTEGRACIÓN DE SUS SISTEMAS EN UNA PLATAFORMA PSIM**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 17 (Diecisiete).

Ciudad Universitaria, 07 de abril del 2026


DRA. TERESA ESTHER NUÑEZ ZUÑIGA
Presidente Jurado


DR. JORGE ELÍAS MOSCOSO SÁNCHEZ
Miembro Jurado


DR. CELSO YSIDRO GERONIMO HUAMAN
Miembro Jurado


MG. JEAN CARLOS MALCA FERNANDEZ
Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo , **JEAN CARLOS MALCA FERNANDEZ** en mi condición de asesor acreditado con el Dictamen N°24/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **MEJORA DE LA EFICIENCIA OPERATIVA EN LA SUPERVISIÓN DE LA SEGURIDAD ELECTRÓNICA DE LAS EMPRESAS PLANINVEST, MARTINIZING Y FUCSA MEDIANTE LA INTEGRACIÓN DE SUS SISTEMAS EN UNA PLATAFORMA PSIM**, presentado por el bachiller **ALEX MARCELINO MEZA ESCOBAR**, para optar al título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 6% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título de Ingeniero Electrónico.

Lima, 07 de Abril del 2026

Firma del Asesor

DNI: 45535181

Nombres y apellidos del asesor:

JEAN CARLOS MALCA FERNANDEZ

DEDICATORIA

Este trabajo está dedicado a todos los que formaron parte de mi desarrollo profesional.

AGRADECIMIENTOS

A mis familiares, compañeros y al equipo de soporte de PRYMS.

RESUMEN

El presente trabajo tiene como objetivo mejorar la eficiencia operativa en la supervisión de los sistemas de seguridad electrónica de las empresas Planinvest, Martinizing y Fucsa, mediante la implementación de una plataforma PSIM que integre sus sistemas de videovigilancia y control de accesos. La metodología aplicada fue de tipo aplicada, estructurada en fases: planificación, instalación, diseño e implementación, pruebas y capacitación. Se utilizó la plataforma AppVision™ del fabricante PRYSM, la cual permitió integrar dispositivos de distintos fabricantes en una sola interfaz de monitoreo centralizado. Como resultado, se obtuvo una solución funcional que consolidó los sistemas de seguridad, optimizó la verificación de eventos, redujo la carga operativa del personal y mejoró la capacidad de respuesta ante incidentes. La integración visual mediante sinópticos interactivos y la correlación automática entre eventos fortalecieron el monitoreo y el análisis forense. Se concluye que el uso de plataformas PSIM representa una solución eficaz para entornos con infraestructura tecnológica heterogénea, permitiendo escalabilidad, control y continuidad operativa sin depender de un único proveedor.

Palabras clave: PSIM, integración, seguridad electrónica, interoperabilidad, monitoreo centralizado.

ABSTRACT

His professional work aims to improve the operational efficiency in the supervision of electronic security systems in the companies Planinvest, Martinizing, and Fucsa through the implementation of a PSIM (Physical Security Information Management) platform that integrates their video surveillance and access control systems. The applied methodology followed a structured sequence: planning, installation, design and implementation, testing, and training. The AppVision™ platform, developed by PRYSM, was used to integrate devices from different manufacturers into a single centralized monitoring interface. As a result, a functional solution was achieved that consolidated security systems, optimized event verification, reduced the operational load on personnel, and improved incident response capabilities. The visual integration through interactive synoptics and the automatic correlation between events strengthened monitoring and forensic analysis. It is concluded that PSIM platforms offer an effective solution for environments with heterogeneous technological infrastructure, allowing scalability, control, and operational continuity without relying on a single vendor.

Keywords: PSIM, integration, electronic security, interoperability, centralized monitoring.

INDICE GENERAL

CARÁTULA	i
DEDICATORIA	ii
AGRADECIMIENTOS	iii
RESUMEN	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	xi
CAPITULO I: INTRODUCCIÓN	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
2.1 Institución – Actividad que desarrolla	3
2.2 Periodo de duración de la actividad	3
2.3 Finalidad y objetivos de la entidad	3
2.4 Razón social	3
2.5 Dirección postal	3
2.6 Nombre y correo electrónico del profesional a cargo	4
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	5
3.1 Organización de la actividad	5
3.2 Finalidad y objetivos de la Actividad	6
3.2.1 <i>Finalidad</i>	6
3.2.2 <i>Objetivos</i>	6
3.3 Problemática	7
3.3.1 <i>Problema General</i>	8
3.3.2 <i>Problemas Específicos</i>	8
3.3.3 <i>Justificación e importancia de la investigación</i>	8

3.4 Metodología	9
3.4.1 Bases teóricas	11
3.4.2 Marco conceptual	12
3.5 Procedimiento	15
3.5.1 Etapa de levantamiento de información	15
3.5.2 Etapa de preparación e instalación del software AppVision	16
3.5.3 Etapa de diseño e implementación de la solución integrada	17
3.5.4 Etapa de pruebas de dispositivos integrados	18
3.5.4.1.1 Pruebas empresa Planinvest	18
3.5.4.1.2 Pruebas empresa Martinizing	21
3.5.4.1.3 Pruebas empresa Fucsa	23
3.5.5 Etapa de pruebas de entorno de trabajo operador	25
3.5.6 Etapa de capacitación	28
3.6 Resultado de la actividad	31
CAPITULO IV: DISCUSION DE RESULTADOS	35
4.1 Descripción de la implementación	35
4.2 Evaluación Económica	37
CAPITULO V: CONCLUSIONES	39
CAPITULO VI: RECOMENDACIONES	41
CAPITULO VII: BIBLIOGRAFÍA	43
CAPITULO IX: ANEXOS	44

LISTA DE FIGURAS

Figura 1. Protocolo para cámaras Hikvision	18
Figura 2. Pruebas de cámaras Hikvision	19
Figura 3. Protocolo para servidor Dorlet	19
Figura 4. Pruebas de con control de acceso Dorlet	20
Figura 5. PIR alarmado -pruebas de sistema de intrusión	20
Figura 6. Sensor alarmado -pruebas de sistema de incendio	21
Figura 7. Pruebas de cámaras Dahua	21
Figura 8. Pruebas de cámaras empresa Martinizing planicie	22
Figura 9. Pruebas de cámaras empresa Martinizing Dasso	22
Figura 10. Pruebas de cámaras empresa Martinizing chacarilla	23
Figura 11. Pruebas con las cámaras Dahua	23
Figura 12. Pruebas con las cámaras Dahua	24
Figura 13. Pruebas con los paneles Bosch	24
Figura 14. Pruebas de alarmas con los paneles Bosch	25
Figura 15. Pruebas de funcionalidad ventana principal	26
Figura 16. Pruebas de funcionalidad ventana principal menú	26
Figura 17. Pruebas botón acceso a históricos	27
Figura 18. Pruebas de funcionalidad ventana Planinvest	27
Figura 19. Pruebas de funcionalidad ventana Martinizing	27
Figura 20. Pruebas de funcionalidad ventana Fucsa	28
Figura 21. Capacitación del personal Planinvest	30
Figura 22 Interfaces de la empresa Planinvest	31
Figura 23. Interfaces de empresa Martinizing	32
Figura 24 Interfaces de integración empresa Martinizing 6 sedes	32
Figura 25 Interfaces de empresa Martinizing primavera	33
Figura 26 Interfaces de la empresa Fucsa	33
Figura 27 Vista principal de la plataforma PSIM	34
Figura A1. Cámara, PIR y sensor magnético	49

Figura B1. Requisitos mínimos de hardware	52
Figura B3. Parámetros de red PC servidor principal	53
Figura B4. Instalación de servidor AppVision	54
Figura B5. Accesos directos AppVSION	55
Figura B6. Ventana de acceso al aplicativo “Configurador” de AppVision	55
Figura B7. Ventana principal del aplicativo “Configurador” de AppVision	56
Figura B8. Licenciamiento del servidor	56
Figura B9. Parámetros de la licencia del servidor AppVision	57
Figura B10. Activación de Servidor AppVision	57
Figura B11. Configuración de redundancia servidor principal	58
Figura B12. Configuración de redundancia	58
Figura B13. Instalación de AppVision cliente	59
Figura B14. Plataforma PRYSM de soporte	59
Figura B15. Manual para la integración de equipos Hikvision	60
Figura B16. Archivos para la integración con Hikvision	60
Figura B17. Manual para la integración de equipos Dahua	61
Figura B18. Archivos para la integración con Dahua	61
Figura B19. Documentos para la integración con Bosch	62
Figura B20. Manual para la integración de equipos Dorlet	62
Figura B21. Archivos para la integración con Dorlet	63
Figura C1. Creación de sinópticos y botones empresa Planinvest	64
Figura C2. Sinóptico y botones. Fuente. Edición Propia	64
Figura C3. Sinóptico y botones para local Espinar	65
Figura C4. Creación de sinóptico y botones	65
Figura C5. Creación de sinóptico “Histórico Alarmas”	66
Figura C6. Ubicación geográfica de símbolo	66
Figura C7. Creación de botones en sinóptico “HeaderView”	67
Figura C8. Creación de símbolo de CCTV en AppVision	67
Figura C9. Creación de símbolo de PIR en AppVision	68
Figura C10. Creación de símbolo del sensor magnético Bosch AppVision	68
Figura C11. Prog. acciones símbolo control de acceso Dorlet en AppVision	69
Figura C12. Programación sistema de detección de incendios AppVision	69
Figura C13. Listado de protocolos creados para la integración	70

Figura C14. Variables para integrar grabador de 16 canales de Hikvision	70
Figura C15. Variables servidor de control acceso con controladora Dorlet	71
Figura C16. Asignación de símbolo variables sistema de incendio	71
Figura C17. Asignación de símbolo y protocolo para integrar Dahua	71
Figura C18. Asignación de símbolo y protocolo para integrar Dahua	72
Figura C19. Asignación de símbolo y protocolo para integrar Bosch	72

LISTA DE TABLAS

Cuadro A1 Parámetros del sistema de CCTV empresa Planinvest	45
Cuadro A2 Parámetros sistema de control de acceso empresa Planinvest	46
Cuadro A3 Parámetros sistema detección incendios empresa Planinvest	46
Cuadro A4 Parámetros del sistema de intrusión empresa Planinvest	47
Cuadro A5 Parámetros sistema de CCTV por sedes empresa Martinizing	48
Cuadro A6 Parámetros del sistema de CCTV empresa Fucsa	49
Cuadro A7 Parámetros del sistema de intrusión empresa Fucsa	50
Cuadro B1 Distribución de IP para el proyecto	52

CAPITULO I: INTRODUCCIÓN

El presente informe surge de la necesidad de mejorar la eficiencia operativa en la supervisión de los sistemas de seguridad electrónica de las empresas Martinizing, Planinvest y Fucsa. Cada una de ellas gestionaba sus dispositivos de manera aislada, sin contar con una supervisión constante ni unificada, lo que limitaba la capacidad de respuesta ante incidentes.

Con el propósito de superar estas limitaciones, la junta directiva del grupo empresarial impulsó un proyecto estratégico en fases. En una primera etapa se estableció un centro de monitoreo en la sede de Planinvest, dotado de la infraestructura necesaria como videowall y estaciones de trabajo para centralizar la operación. La segunda etapa —que constituye el alcance de este trabajo— consistió en la integración inicial de los sistemas de videovigilancia y control de accesos de las tres empresas en una plataforma PSIM (AppVision™). Finalmente, este proyecto fue concebido con miras a una tercera etapa futura, en la cual se integrarán otras empresas del grupo, ampliando la cobertura del centro de monitoreo centralizado.

Ante este escenario, se identificó la oportunidad de integrar todos los sistemas mencionados mediante una plataforma PSIM (Physical Security Information Management), una solución que permite centralizar el control, supervisión y análisis de múltiples tecnologías de seguridad, sin depender de un único proveedor.

La elección de este tema responde tanto a su relevancia operativa como a su aplicabilidad en otros entornos que presenten desafíos similares de interoperabilidad tecnológica. Además, resulta importante documentar este tipo de experiencias, ya que en el Perú aún no existen muchos antecedentes de proyectos desarrollados con plataformas PSIM, a diferencia de otros países donde su implementación es más común en sectores como salud,

penitenciario o infraestructura crítica. Por tanto, el presente trabajo busca aportar un precedente técnico que sirva de referencia para futuras integraciones de sistemas de seguridad en nuestro contexto local.

Este informe está compuesto por los siguientes capítulos:

Capítulo 1: Describe la estructura general del trabajo de suficiencia profesional.

Capítulo 2: Presenta el entorno institucional donde se desarrolla el proyecto.

Capítulo 3: Define los objetivos del TSP, la problemática, la justificación y la metodología aplicada, así como los fundamentos teóricos necesarios.

Capítulo 4: Expone el procedimiento técnico de integración y la evaluación económica.

Capítulo 5: Presenta recomendaciones para futuros proyectos similares.

Capítulo 6: Contiene las referencias bibliográficas utilizadas.

Capítulo 7: Incluye anexos con información complementaria.

CAPITULO II: INFORMACIÓN DEL LUGAR DE LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

La empresa SENTRIX S.A. brinda servicios de tecnología de seguridad, vigilancia privada y seguridad.

2.2 Periodo de duración de la actividad.

Las actividades iniciaron el mes de setiembre del 2021 hasta diciembre del 2022.

2.3 Finalidad y objetivos de la entidad

La empresa SENTRIX tiene como finalidad ser reconocida a nivel nacional como una empresa líder en servicios de seguridad, con altos estándares de calidad, el mejor talento humano y tecnología, en base a una cultura de alto desempeño y cuidado del medio ambiente, garantizando la tranquilidad y confianza de nuestros clientes.

La empresa SENTRIX tiene como objetivo diseñar e implementar estrategias de seguridad patrimonial con el cuidado, la diligencia y el servicio personalizado a cada uno de sus clientes, que les permitan sentir y disfrutar la tranquilidad y confianza de saber que sus intereses son resguardados eficaz y eficientemente.

2.4 Razón social

SENTRIX SEGURIDAD INTEGRAL SAC

2.5 Dirección postal

Av. Dos de mayo 1225, San Isidro, Lima.

2.6 Nombre y correo electrónico del profesional a cargo.

Erick Guillen Velásquez —jefe de sistemas— correo guillen@sentry.com.pe

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

El trabajo de integración y configuración de la central de monitoreo de seguridad electrónica se desarrolló en el Centro de Monitoreo de la empresa Planinvest S.A.C., ubicado en Calle A, N° 234 – Lima, Perú. Dicho trabajo fue realizado por la empresa Sentrix S.A.C., especializada en soluciones de integración de sistemas de seguridad electrónica y plataformas de gestión PSIM, como parte de un servicio contratado directamente por Planinvest S.A.C. para optimizar su infraestructura de monitoreo.

El servicio incluyó la instalación, configuración y puesta en marcha de la plataforma AppVision™, con el objetivo de centralizar en un único entorno la supervisión de los sistemas de seguridad de Planinvest S.A.C. y de otras empresas asociadas, como Martinizing y Fucsa, permitiendo así una operación más eficiente y unificada.

La ejecución del servicio estuvo bajo la supervisión del área de TI de Planinvest S.A.C., en coordinación con el equipo especializado de Sentrix S.A.C., asegurando el cumplimiento del alcance técnico definido y la validación del funcionamiento de la solución implementada.

La organización de la actividad se presenta en los siguientes puntos:

- Levantamiento de información y preparación del entorno de software.
- Diseño e implementación de la solución integrada.
- Pruebas funcionales y validación operativa.
- Capacitación al personal operativo.

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

La finalidad de la actividad fue permitir que la empresa Planinvest realizara el monitoreo centralizado, eficiente y eficaz de los sistemas de seguridad electrónica implementados en las empresas Planinvest, Martinizing y Fucsa. De este modo se logró un mayor conocimiento de la situación, facilitando la toma de decisiones oportunas ante eventos generados por los sistemas integrados de videovigilancia y control de accesos.

3.2.2 Objetivos

Objetivo general

Mejorar la eficiencia en la supervisión, la respuesta ante eventos y la gestión operativa de la seguridad electrónica en las empresas Martinizing, Planinvest y Fucsa, mediante la implementación de una plataforma PSIM que integre sus sistemas de videovigilancia y control de accesos, los cuales operan con tecnologías y fabricantes distintos.

Objetivos específicos

Realizar el levantamiento de información de los sistemas de seguridad electrónica existentes en las empresas Planinvest, Martinizing y Fucsa, a fin de identificar los requerimientos técnicos y funcionales para la integración.

Implementar la solución integrada en la plataforma PSIM AppVision™, abarcando la instalación, configuración de componentes y desarrollo de sinópticos, drivers y lógica de correlación entre eventos para garantizar la interoperabilidad de los sistemas de CCTV y control de acceso.

Ejecutar pruebas de integración y validación operativa, verificando la conectividad, funcionalidad y representación gráfica de los dispositivos, así como la interacción del operador con la interfaz de monitoreo, menús y reportes, asegurando el correcto funcionamiento del sistema integrado.

Capacitar al personal operativo, instruyéndolos en el uso de la plataforma PSIM para garantizar una operación autónoma y eficiente.

3.3 Problemática

En la actualidad, muchas empresas implementan diversos sistemas de seguridad electrónica, tales como videovigilancia (CCTV), control de accesos, detección de incendios, alarmas de intrusión y analíticas de video. Estos sistemas suelen instalarse de forma escalonada y con distintos fabricantes, seleccionados según conveniencia económica o funcional. Como resultado, se genera un entorno fragmentado y de gestión limitada, donde cada sistema opera de manera independiente, dificultando la supervisión centralizada y reduciendo la capacidad de respuesta ante eventos.

Esta fragmentación provoca múltiples dificultades operativas: incremento en la tasa de alarmas no atendidas, respuestas lentas ante eventos críticos, y falta de trazabilidad unificada de los incidentes. Dichos problemas se agravan en organizaciones que carecen de un centro de monitoreo o de personal dedicado a la supervisión continua, especialmente cuando los dispositivos están distribuidos en distintas instalaciones.

En el caso específico del grupo empresarial conformado por las compañías Planinvest, Martinizing y Fucsa, se identificó que cada una operaba sus sistemas de seguridad electrónica de forma independiente, sin un esquema de monitoreo activo ni operadores asignados. La gestión se limitaba al área de TI, encargada únicamente de verificar la operatividad básica de los dispositivos, sin supervisión en tiempo real. Esta ausencia de seguimiento continuo generaba una falta total de control operativo, dificultando la detección oportuna de incidentes y la evaluación del desempeño de los sistemas. Ante ello, se propuso la implementación de una plataforma PSIM (Physical Security Information Management) como una solución integral para pasar de una gestión pasiva y fragmentada a una supervisión centralizada, escalable y eficiente.

3.3.1 Problema General

¿Cómo mejorar la eficiencia en la supervisión, la respuesta ante eventos y la gestión operativa de la seguridad electrónica en las empresas Martinizing, Planinvest y Fucsa, a través de la implementación de una plataforma PSIM que integre los sistemas de videovigilancia y control de accesos, los cuales operan con tecnologías y fabricantes distintos?

3.3.2 Problemas Específicos

La ausencia de información técnica consolidada sobre los sistemas de seguridad electrónica de las empresas Planinvest, Martinizing y Fucsa dificulta identificar los requerimientos técnicos y funcionales necesarios para su integración.

La falta de una infraestructura base de integración, incluyendo la instalación del software PSIM AppVision™ y sus componentes asociados, limita la posibilidad de implementar una solución que unifique los sistemas de CCTV y control de accesos.

La conectividad y funcionalidad de los dispositivos integrados no pueden asegurarse sin pruebas controladas, que validen su interoperabilidad, representación gráfica y la interacción del operador con la interfaz de monitoreo.

El personal operativo no cuenta con la capacitación necesaria para gestionar la plataforma PSIM de manera autónoma y eficiente, lo que compromete la sostenibilidad del sistema a largo plazo.

3.3.3 Justificación e importancia de la investigación

El presente trabajo de suficiencia profesional se justifica por la necesidad concreta de mejorar la eficiencia operativa de la seguridad electrónica en las empresas Martinizing, Planinvest y Fucsa, las cuales contaban con sistemas de videovigilancia y control de accesos independientes, gestionados únicamente por sus áreas de TI para verificar la operatividad básica de los

equipos, sin contar con monitoreo activo ni supervisión continua. Esta situación generaba una falta de control centralizado, ausencia de trazabilidad de incidentes y una limitada capacidad de respuesta ante eventos críticos.

A través de la implementación de una plataforma PSIM (Physical Security Information Management), se integraron en una sola interfaz los sistemas de seguridad de las tres empresas, permitiendo establecer por primera vez un esquema de supervisión centralizada, la correlación automática entre eventos de acceso y videovigilancia, y la visualización en tiempo real de los dispositivos sobre planos interactivos. Esta solución permitió transformar la gestión pasiva de los sistemas en una operación activa y coordinada, optimizando la toma de decisiones en el centro de control de Planinvest, mejorando la verificación de incidentes y eliminando la necesidad de utilizar múltiples softwares de distintos fabricantes.

Por tratarse de un desarrollo aplicado en un entorno real, el presente proyecto tiene un impacto inmediato en la gestión de seguridad de las organizaciones involucradas y demuestra la viabilidad de utilizar tecnologías de integración como PSIM para resolver problemas de interoperabilidad y falta de supervisión en entornos con sistemas heterogéneos de seguridad electrónica.

3.4 Metodología

Enfoque del proyecto:

El presente trabajo de suficiencia profesional se desarrolló de manera individual, con un enfoque aplicado, basado en la implementación real de una solución tecnológica orientada a la mejora operativa de la seguridad electrónica. El objetivo fue integrar, mediante una plataforma PSIM del fabricante PRYSM, los sistemas de videovigilancia y control de accesos de las empresas Martinizing, Planinvest y Fucsa, los cuales operaban con tecnologías y fabricantes distintos.

La metodología empleada se basó en el ciclo de vida típico de un proyecto de integración de sistemas, compuesto por etapas claramente definidas: planificación, instalación, diseño e implementación, pruebas y capacitación.

Etapas del proyecto:

Planificación: Se realizó el levantamiento de información técnica de los sistemas de seguridad electrónica existentes en cada empresa, incluyendo marcas, modelos, versiones de firmware, cantidades de dispositivos, topologías de red, direcciones IP y credenciales de administrador. A partir de esta información, se definió el alcance del proyecto y los requerimientos funcionales de la interfaz. También se coordinó con el fabricante PRYSM la entrega o creación de los drivers necesarios según lo identificado en el levantamiento.

Preparación: Se preparó la infraestructura tecnológica: servidores y estaciones de trabajo. Se instalaron los sistemas operativos correspondientes (Windows Server y Windows 10), así como los módulos cliente, servidor principal y servidor redundante de la plataforma PSIM. Además, se configuraron los drivers definidos previamente y se realizaron pruebas de conectividad entre los diferentes componentes del sistema.

Diseño e implementación: Se creó la estructura organizativa dentro de la plataforma PSIM para cada empresa, incorporando planos, logotipos, vistas personalizadas, variables por dispositivo y símbolos gráficos representativos. Se diseñó la interfaz principal para los operadores, incorporando las funcionalidades definidas en la etapa de planificación. Entre estas, se implementó la correlación específica entre eventos del sistema de control de accesos y las cámaras de videovigilancia cercanas, con el objetivo de facilitar la verificación visual inmediata ante una apertura o intento de acceso.

Pruebas funcionales: Se realizaron pruebas por empresa y subsistemas. Se validaron los cambios de estado de las variables, su correspondencia gráfica y el comportamiento de los dispositivos. Se generaron eventos reales como la apertura de puertas, generando alarmas que fueron verificadas mediante las cámaras asociadas.

Capacitación: Se capacitó al personal operativo encargado del monitoreo centralizado, abordando el uso de la plataforma, la navegación en la interfaz, el reconocimiento de eventos y la gestión de incidentes. Además, se

recibieron observaciones que, tras ser aprobadas por el área de sistemas, fueron implementadas como ajustes finales.

Este enfoque metodológico permitió asegurar que la solución fuera implementada de forma ordenada, validada y adaptada a las necesidades reales del cliente, mejorando significativamente la eficiencia operativa de la seguridad electrónica de las tres empresas.

3.4.1 Bases teóricas

Uno de los aportes teóricos más relevantes en el campo de la integración de sistemas de seguridad mediante plataformas PSIM proviene del trabajo de Pappalardo (2013). En su tesis doctoral titulada *A Framework for Threat Recognition in Physical Security Information Management*, el autor analizó los desafíos asociados a la integración, fusión y gestión de información en sistemas de seguridad física, tanto desde la perspectiva de la industria como desde la investigación académica. La propuesta central del estudio se orientó a mejorar la capacidad de respuesta de los operadores ante amenazas complejas, mediante el uso estratégico de todos los recursos disponibles en entornos con múltiples subsistemas distribuidos. Para ello, se desarrolló el software DETECT (Decision Triggering Event Composer & Tracker), que opera en conjunto con una plataforma PSIM realizando correlaciones lógicas, espaciales y temporales de eventos detectados por cada subsistema. Este enfoque permitió alcanzar un conocimiento situacional más preciso, reduciendo la cantidad de notificaciones poco relevantes y mejorando la discriminación entre alarmas reales y falsas. Como resultado, los operadores actuaron de forma más eficiente, guiados por procedimientos automatizados o semiautomatizados definidos según parámetros específicos del entorno.

Otro aporte relevante es el trabajo de Espillico (2015), quien en su tesis desarrolló el diseño e implementación de un sistema integral de seguridad, monitoreado de forma local y remota mediante redes de comunicación para las agencias de la Caja Rural – Los Andes S.A. El objetivo principal del proyecto fue optimizar los tiempos de respuesta ante eventos críticos mediante la interconexión del sistema de alarmas y cámaras, así como

centralizar la supervisión de las agencias a través de un centro de monitoreo. La solución planteada integró un sistema de monitoreo que permitía gestionar de forma conjunta las alarmas del sistema de intrusión y el sistema de videovigilancia (CCTV) a través de una plataforma común, lo cual permitió mejorar significativamente la eficiencia operativa y la capacidad de reacción ante incidentes. Este trabajo demostró cómo una arquitectura centralizada puede contribuir a la toma de decisiones rápidas y al manejo eficaz de eventos distribuidos.

También se considera el trabajo de Pérez (2016), quien en su tesis desarrolló el diseño de un sistema de seguridad electrónica con monitoreo centralizado para una instalación minera. El objetivo principal fue implementar un sistema que permitiera gestionar de forma unificada el control y la supervisión de cámaras de videovigilancia y alarmas desde un único centro de control de seguridad. Uno de los aportes clave de esta tesis fue la interrelación entre los sistemas de intrusión y el CCTV, permitiendo que, ante una detección de intrusión, el operador pudiera visualizar automáticamente la cámara más cercana al punto del evento. Esta funcionalidad buscó reducir los tiempos de respuesta ante emergencias y minimizar las falsas alarmas. La solución propuesta se basó en la adquisición de la plataforma BIS del fabricante Bosch, lo cual exigió la instalación de todos los sistemas (CCTV e intrusión) del mismo fabricante para asegurar la integración. Este caso reflejó cómo una arquitectura homogénea, aunque más limitada en cuanto a marcas, puede ofrecer una integración efectiva entre subsistemas de seguridad electrónica para entornos críticos.

3.4.2 Marco conceptual

A continuación, se definen los conceptos fundamentales involucrados en el desarrollo de la plataforma PSIM implementada en este trabajo, con el fin de facilitar la comprensión técnica del proyecto y sus componentes.

PSIM (Physical Security Information Management)

Es una plataforma de software que permite integrar diversos sistemas de seguridad electrónica, tales como videovigilancia (CCTV), control de accesos, alarmas técnicas, detección de incendios e intrusión, dentro de una interfaz unificada. Su propósito es mejorar la supervisión, la toma de decisiones y la respuesta ante eventos, facilitando el conocimiento situacional en tiempo real (Nilsson, 2012; Cuppens & Cuppens, 2015).

AppVision

Desarrollado por la empresa Prysm Software, AppVision™ es un sistema PSIM que permite gestionar dispositivos heterogéneos a través de controladores (drivers) que se comunican mediante protocolos estándares. Permite crear interfaces sinópticas, definir reglas automáticas, gestionar alarmas, personalizar vistas de operador y generar reportes de eventos. Es escalable y adaptable a proyectos multisitio (Prysm Software, 2021).

Sinóptico

Es una interfaz gráfica que representa un plano o mapa de las instalaciones, en el cual se colocan íconos o símbolos que representan dispositivos de seguridad (cámaras, sensores, puertas, etc.). Estos elementos están vinculados a variables en tiempo real que permiten al operador supervisar, controlar e interactuar con los sistemas desde una interfaz visual (Prysm Software, 2021).

Variable

En el contexto de AppVision™, una variable representa un punto de datos que puede reflejar el estado o valor de un dispositivo. Por ejemplo, una variable puede indicar si una puerta está abierta o cerrada, si una alarma está activa o si una cámara está grabando. Las variables son fundamentales para definir eventos, acciones y reglas dentro del PSIM (Prysm Software, 2021).

SDK (Software Development Kit)

Un SDK es un conjunto de herramientas, bibliotecas y documentación que permite a los desarrolladores extender las funcionalidades de un software. En AppVision™, el SDK permite crear plugins o módulos adicionales para integrar

dispositivos o funciones que no están disponibles de forma nativa (Microsoft, 2020).

API (Application Programming Interface)

Es una interfaz de programación que permite que distintas aplicaciones se comuniquen entre sí. AppVision™ puede utilizar APIs para integrarse con otros softwares externos, sistemas de gestión o bases de datos, permitiendo el intercambio de datos en tiempo real (Red Hat, 2022).

Protocolos

Los protocolos son normas que permiten la comunicación entre AppVision™ y los sistemas a integrar. La plataforma soporta múltiples protocolos de comunicación mediante controladores, como Modbus, OPC, SNMP, SMTP, SMS, Bacnet, entre otros. Estos protocolos permiten al sistema interpretar eventos y estados de los dispositivos conectados (Modbus Organization, 2012; OPC Foundation, 2021; Prysm Software, 2021).

Sistema de intrusión

Sistema compuesto por sensores de movimiento, contactos magnéticos, panel de control y dispositivos de alarma sonora o visual, cuyo objetivo es detectar accesos no autorizados. En el contexto del PSIM, estos eventos pueden ser correlacionados con cámaras para verificación inmediata (Honeywell, 2019).

Sistema de CCTV

Sistema de videovigilancia compuesto por cámaras, grabadores (DVR/NVR), y software de visualización. Permite la supervisión y grabación de imágenes en tiempo real. Cuando se integra a un PSIM, puede vincularse a otros sistemas como control de accesos o detección de intrusión para mejorar la respuesta operativa (Bosch Security Systems, 2020).

Dirección IP

Es un identificador único asignado a cada dispositivo conectado a una red. Todos los elementos del sistema, como cámaras, controladores, servidores y

estaciones de trabajo utilizan direcciones IP para comunicarse entre sí dentro de la infraestructura tecnológica del PSIM (Microsoft, 2020).

3.5 Procedimiento

3.5.1 Etapa de levantamiento de información

La primera fase del proyecto consistió en la planificación general de la implementación y en el levantamiento técnico detallado de la infraestructura de seguridad electrónica de las empresas Planinvest, Martinizing y Fucsa. Esta etapa fue clave para definir los alcances del proyecto, los recursos necesarios y las limitaciones técnicas presentes.

Se identificó que cada empresa operaba de forma independiente, con sistemas diversos de videovigilancia, control de accesos y sensores, lo cual representaba un reto para la integración. Se realizaron visitas técnicas presenciales a las sedes, coordinadas con los responsables del área de TI de cada empresa, a fin de recolectar información sobre los modelos de dispositivos (cámaras, paneles, sensores), métodos de comunicación, versiones de firmware, direcciones IP, licencias de software propietario y el estado general de la red. También se elaboraron planos técnicos específicos de ubicación de los dispositivos, ya que solo se contaba con planos arquitectónicos generales.

En paralelo, se estableció contacto con los representantes locales de los fabricantes involucrados, con el fin de validar las posibilidades de integración a través de APIs, SDKs, drivers existentes o identificar posibles restricciones de compatibilidad.

Posteriormente, se documentaron los requerimientos funcionales del cliente para la interfaz de monitoreo, en coordinación con el área de TI de Planinvest, empleando técnicas de lluvia de ideas, sesiones de trabajo y recomendaciones del fabricante PRYSM. Entre los requerimientos clave se incluyeron:

- Un mapa general con coordenadas geográficas de todas las empresas.
- Una matriz de cámaras por cliente.
- Barra de alarmas en tiempo real.
- Planos 3D interactivos por sede.
- Inclusión del logo de la empresa Planinvest.
- Visualización de fachadas y distribución por pisos.
- Relación entre subsistemas (cámaras, sensores, alarmas).
- Workflows para eventos críticos.
- Acceso directo a históricos por usuario.

Esta etapa permitió establecer un panorama claro del entorno técnico sobre el cual se implementaría la plataforma PSIM, identificar puntos críticos de integración y tomar decisiones fundamentadas respecto al licenciamiento, protocolos de integración y diseño de la solución.

El detalle completo se encuentra en el Anexo A – Etapa 1: Planificación y Levantamiento de Información.

3.5.2 Etapa de preparación e instalación del software AppVision

Durante esta fase se realizó la preparación e instalación de todos los componentes necesarios para el funcionamiento inicial de la plataforma PSIM AppVision™. Esta plataforma está compuesta por un aplicativo servidor, que centraliza la gestión del sistema, y un aplicativo cliente, que se instala en las estaciones de trabajo de los operadores para acceder a las funcionalidades del sistema.

Se instalaron y configuraron ambos aplicativos (servidor y cliente) en los equipos correspondientes: el servidor principal y el servidor redundante, incluyendo el licenciamiento respectivo. Se estableció el esquema de redundancia entre los servidores, asegurando la continuidad operativa ante posibles fallos.

Además, se asignaron direcciones IP estáticas a cada equipo según la planificación del área de TI de Planinvest, y se procedió con la instalación de

los drivers necesarios para integrar los dispositivos de distintos fabricantes (Hikvision, Dahua, Bosch y Dorlet), seleccionados con base en el levantamiento técnico previo.

Por último, se instalaron los clientes en las estaciones de monitoreo de los operadores y se realizaron pruebas de conectividad y comunicación entre los diferentes componentes, verificando el correcto enlace entre servidores y clientes.

Para mayor detalle del proceso técnico, ver Anexo B – Etapa 2: Etapa de preparación e instalación del software AppVision.

3.5.3 Etapa de diseño e implementación de la solución integrada

Durante esta etapa se desarrolló la interfaz de monitoreo para el operador en la plataforma AppVision™, iniciando con la creación del proyecto principal que concentró toda la configuración del sistema. Se organizó una estructura de carpetas por empresa (Planinvest, Martinizing y Fucsa), lo que permitió desarrollar sinópticos independientes por cada sede o piso, así como sinópticos globales, históricos y de navegación centralizada.

A partir de la información técnica levantada en la Etapa 1, se diseñaron sinópticos gráficos interactivos que representaban visualmente los entornos físicos de las empresas y sus dispositivos, con correspondencia directa con la realidad física mostrada en los planos. Estos incluían coordenadas geográficas, contactos de emergencia y elementos de alarma. Se programaron botones de navegación entre diferentes niveles, vistas y funcionalidades específicas como históricos y cabeceras personalizadas. También se integraron mapas georreferenciados mediante OpenStreetMap, que muestran en tiempo real el estado operativo de cada empresa y sus sedes.

Además, se desarrollaron símbolos personalizados para cada sistema a integrar (videovigilancia, intrusión, control de accesos), los cuales fueron programados con animaciones y menús contextuales según el estado de las variables asociadas. Se configuraron los protocolos de comunicación

necesarios para establecer la conexión con los distintos sistemas y se crearon las variables requeridas según la documentación técnica de cada fabricante (Hikvision, Dahua, Bosch y Dorlet).

Esta etapa fue clave para dejar lista la estructura lógica del sistema, habilitando la interacción entre la plataforma PSIM y los dispositivos físicos, como preparación para las pruebas funcionales de la siguiente etapa. Para mayor detalle técnico del proceso, consultar el Anexo C – Etapa 3: Diseño e Implementación.

3.5.4 Etapa de pruebas de dispositivos integrados

Durante esta fase se validó la conectividad y operatividad de los sistemas de seguridad electrónica integrados en la plataforma PSIM AppVision™, según los dispositivos levantados en la Etapa 1. Se realizaron pruebas individuales para cada empresa (Planinvest, Martinizing y Fucsa), verificando el funcionamiento correcto de los sistemas de CCTV, control de accesos, intrusión y detección de incendios. Se comprobó que los protocolos establecidos conectaran adecuadamente, sin errores, y que los elementos en la interfaz coincidieran con los dispositivos físicos instalados.

3.5.4.1 Pruebas de Dispositivos Integrados

3.5.4.1.1 Pruebas empresa Planinvest

Pruebas sistema de CCTV

Se verificó que el protocolo se conectara correctamente con el equipo, sin mostrar mensajes de error (ver Figura1).

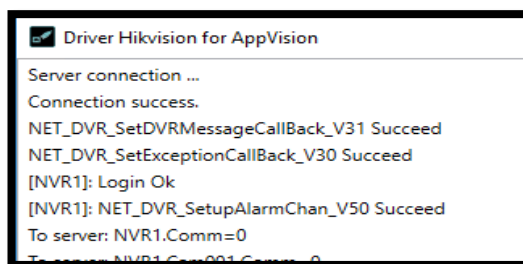


Figura 1. Protocolo para cámaras Hikvision. Fuente. Edición Propia.

Se accedió a la interfaz creada para esta empresa y se interactuó con todos los símbolos del sistema de CCTV según la Tabla 1, validando que la ubicación y visualización correspondieran con cada cámara (ver Figura).2

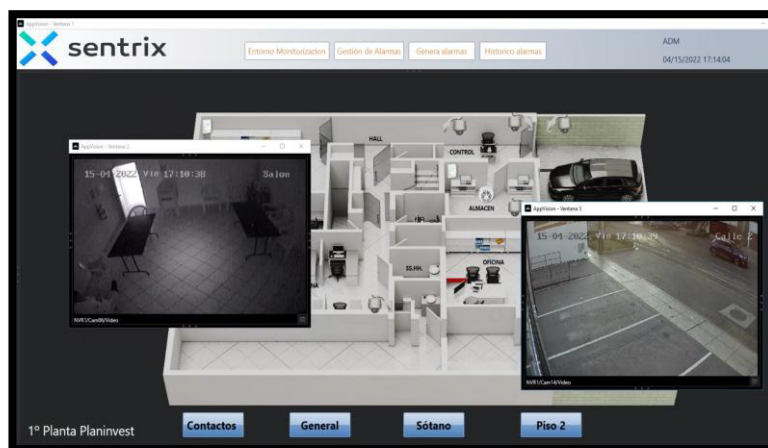


Figura 2. Pruebas de cámaras Hikvision. Fuente. Edición Propia.

Pruebas sistema de control de acceso.

Se confirmó que el protocolo se conectara correctamente con el equipo, sin mostrar mensajes de error (ver Figura 3).

En la interfaz de la empresa, se interactuó con los símbolos de control de acceso según la Tabla 2, validando ubicación y funcionamiento (ver Figura 4).

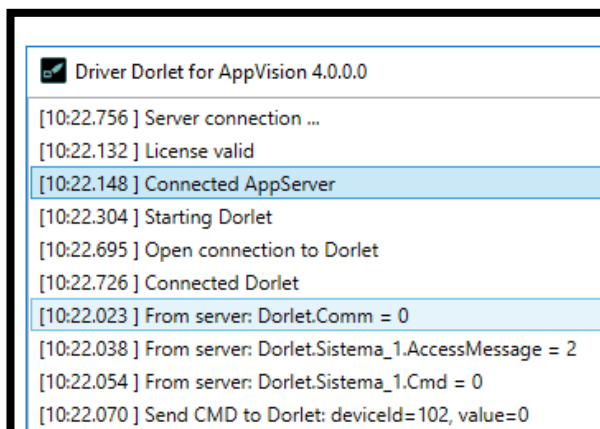


Figura 3. Protocolo para servidor Dorlet. Fuente. Edición Propia.

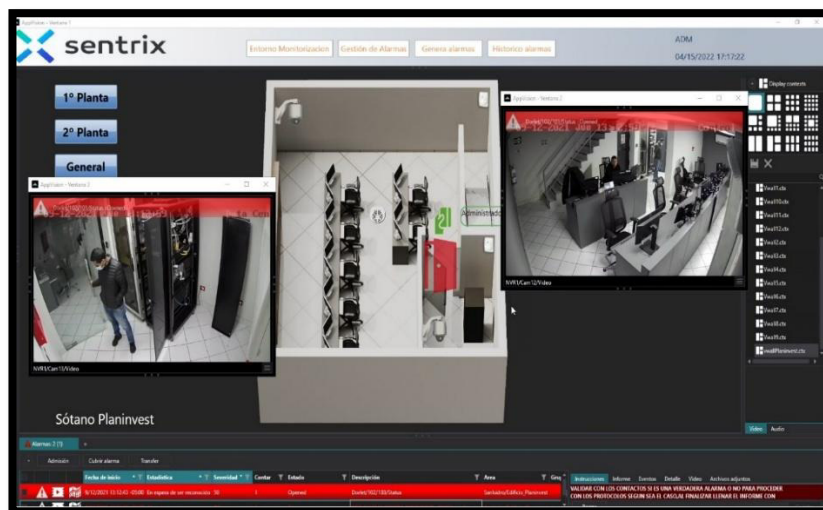


Figura 4. Pruebas de con control de acceso Dorlet. Fuente. Edición Propia.

Pruebas sistema de intrusión.

Para generar cambios de estado en las variables, se activaron desde el menú configurado en la opción “Generar alarmas”. Se realizaron las pruebas correspondientes a cada dispositivo (ver Figura 5).

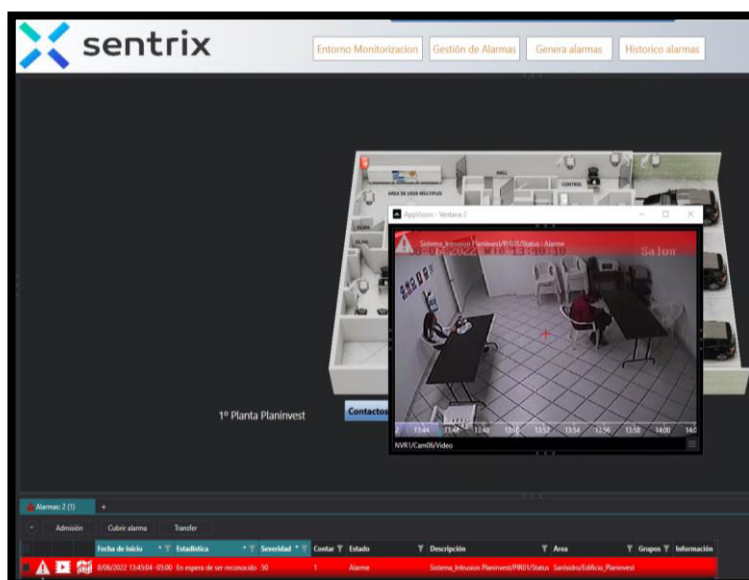


Figura 5. PIR alarmado -pruebas de sistema de intrusión. Fuente. Edición Propia.

Pruebas sistema de incendios.

De igual forma, se generaron cambios de estado en las variables desde el menú “Generar alarmas” y se realizaron las pruebas correspondientes (ver Figura 6).

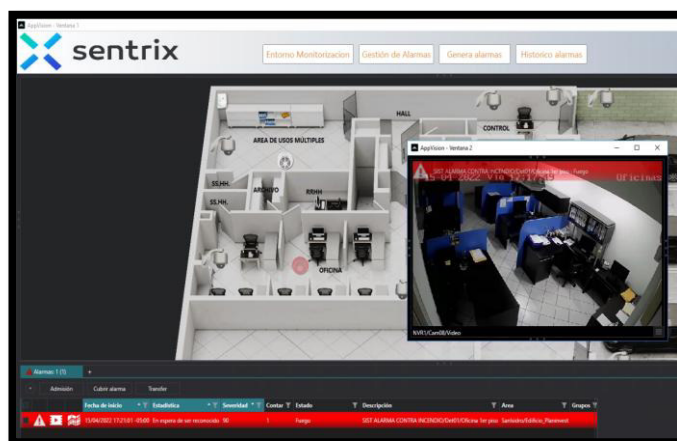


Figura 6. Sensor alarmado -pruebas de sistema de incendio. Fuente. Edición Propia.

3.5.4.1.2 Pruebas empresa Martinizing

Pruebas sistema de CCTV

Se verificó que los protocolos se conectaran correctamente con los equipos, sin presentar mensajes de error (ver Figura 7).

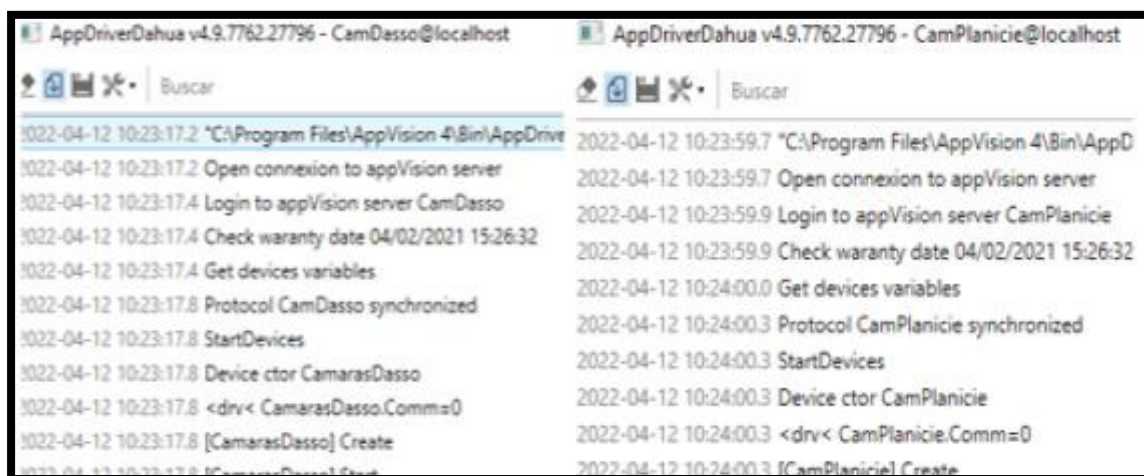


Figura 7. Pruebas de cámaras Dahua. Fuente. Edición Propia.

Se accedió a la interfaz de la empresa y se interactuó con los símbolos de las cámaras instaladas, revisando una por una según la Tabla 5 para validar ubicación y correspondencia.

Se realizaron pruebas en las sedes Planicie, Dasso y Chacarilla (ver Figuras 8 a 10).

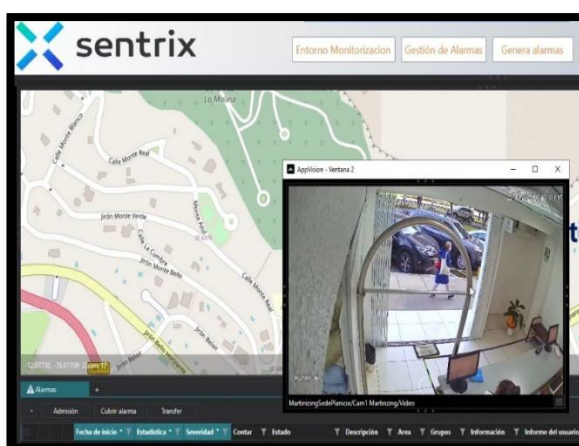


Figura 8. Pruebas de cámaras empresa Martinizing planicie. Fuente. Edición Propia.



Figura 9. Pruebas de cámaras empresa Martinizing Dasso. Fuente. Edición Propia.



Figura 10. Pruebas de cámaras empresa Martinizing chacarilla. Fuente. Edición Propia.

3.5.4.1.3 Pruebas empresa Fucsa

Pruebas sistema de CCTV

Se verificó la correcta conexión del protocolo con el equipo, sin mostrar errores (ver Figura 11).

Se interactuó con los símbolos de cámaras para validar ubicación y funcionamiento (ver Figura 12).

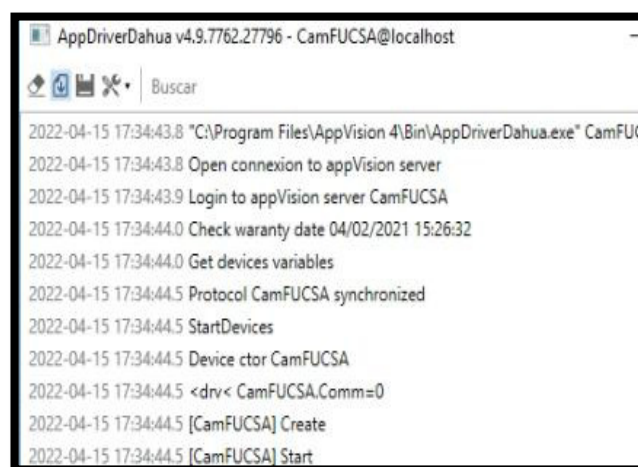


Figura 11. Pruebas con las cámaras Dahua. Fuente. Edición Propia.

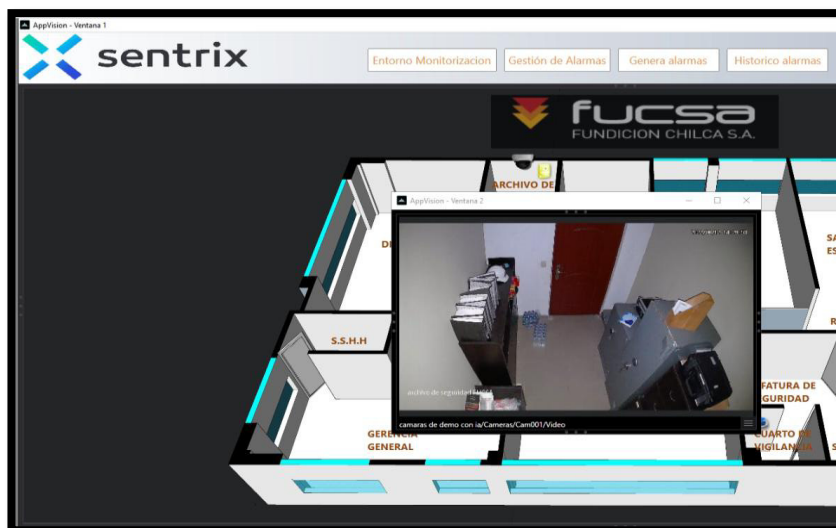


Figura 12. Pruebas con las cámaras Dahua. Fuente. Edición Propia.

Pruebas sistema de intrusión.

Se comprobó la conexión correcta del protocolo con el equipo (ver Figura 13).

En la interfaz se interactuó con los símbolos del sistema de intrusión para validar ubicación y funcionamiento de sensores (ver Figura 14).

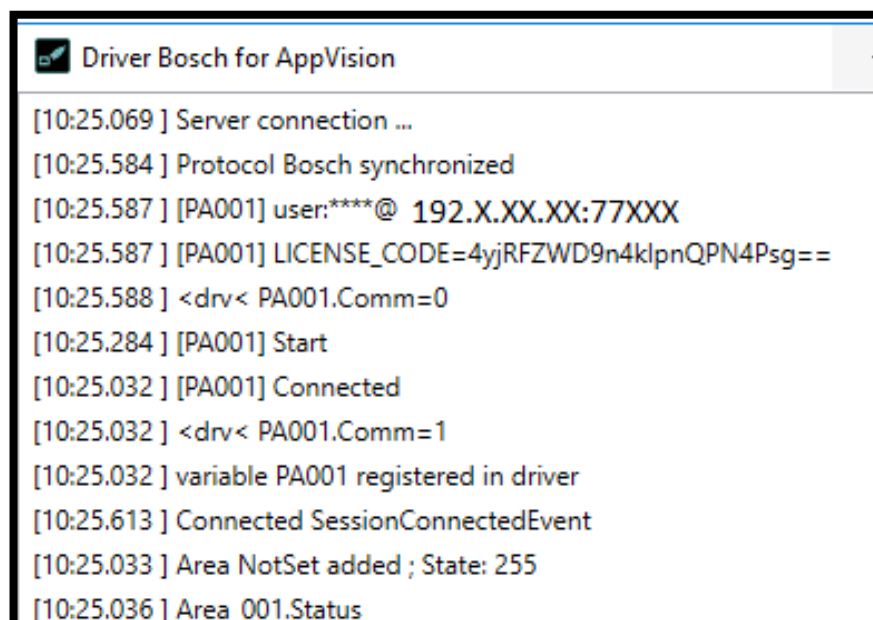


Figura 13. Pruebas con los paneles Bosch. Fuente. Edición Propia.



Figura 14. Pruebas de alarmas con los paneles Bosch. Fuente. Edición Propia.

3.5.5 Etapa de pruebas de entorno de trabajo operador

En esta etapa se evaluó el entorno gráfico diseñado para los operadores. Se probaron menús, botones interactivos, navegación entre planos, vistas específicas por empresa y acceso a históricos de eventos. Se verificó que cada funcionalidad respondiera correctamente y se ajustara a los requerimientos definidos previamente. Esta validación fue fundamental para garantizar una experiencia de usuario clara y eficiente antes de la capacitación final.

Pruebas de entorno de trabajo operador

En esta etapa se probaron todas las funcionalidades programadas para los operadores, con el fin de identificar y corregir posibles incidencias antes de la capacitación final.

Se realizaron verificaciones en:

- Ventana principal (ver Figura 15).
- Menú principal (ver Figura 16).
- Botón de acceso a históricos (ver Figura 17).
- Ventana Planinvest (ver Figura 18).
- Ventana Martinizing (ver Figura 19).
- Ventana Fucsa (ver Figura 20).

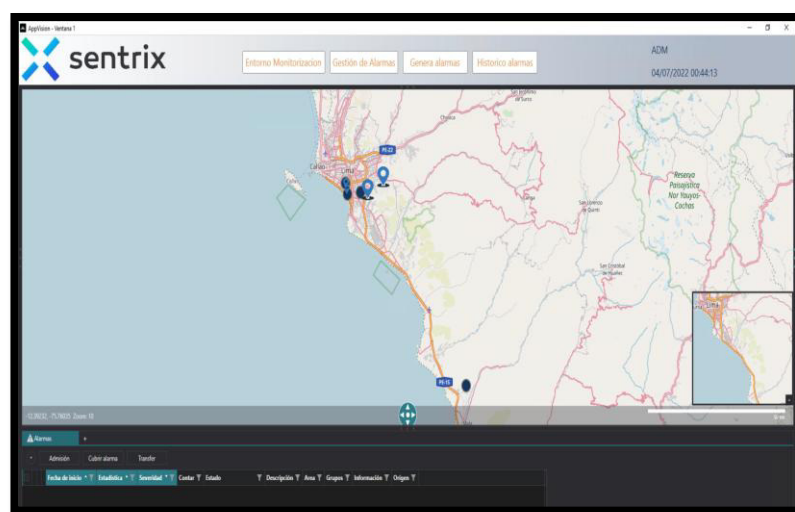


Figura 15. Pruebas de funcionalidad ventana principal. Fuente. Edición Propia.

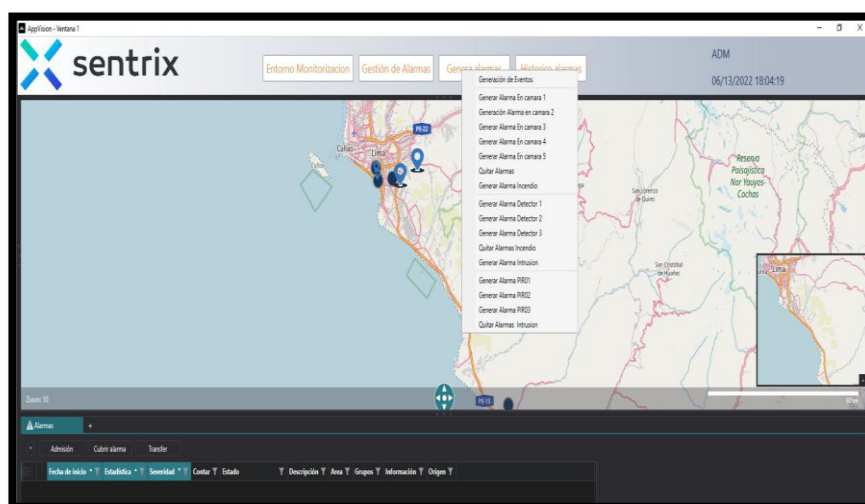


Figura 16. Pruebas de funcionalidad ventana principal menú. Fuente. Edición Propia.



Figura 17. Pruebas botón acceso a históricos. Fuente. Edición Propia.

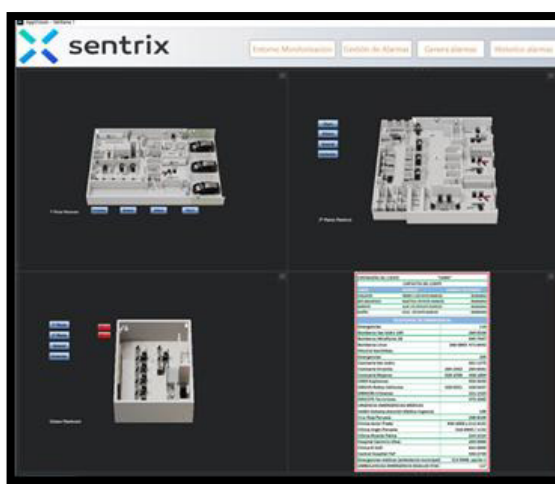


Figura 18. Pruebas de funcionalidad ventana Planinvest. Fuente. Edición Propia.



Figura 19. Pruebas de funcionalidad ventana Martinizing. Fuente. Edición Propia.

Contenido de la capacitación:

Durante las 3 sesiones, se abordaron los siguientes puntos:

Introducción al entorno PSIM AppVision

- Conceptos básicos de la plataforma.
- Arquitectura general del sistema y roles de los servidores principal y redundante.
- Descripción de los protocolos y drivers instalados para la integración.

Gestión de alarmas en tiempo real

- Identificación de eventos generados por los sistemas integrados.
- Procedimiento para reconocer, priorizar y cerrar alarmas.
- Diferenciación entre alarmas reales y alarmas simuladas (modo demo).

Uso de interfaces gráficas personalizadas

- Navegación por mapas, planos 3D y vistas específicas de cada empresa.
- Acceso a matrices de cámaras.
- Consultas rápidas mediante menús y accesos directos.

Acceso y consulta de históricos

- Búsqueda de eventos pasados por filtros de fecha, cliente o tipo de dispositivo.
- Exportación de registros para informes internos o auditorías.

Flujos de trabajo y procedimientos internos

- Ejecución de tareas según protocolos definidos por el cliente.
- Escalamiento de incidentes y comunicación con otras áreas.

Prácticas guiadas en entorno real

- Simulación de eventos de intrusión, incendio y fallas técnicas.
- Interacción con el sistema .
- Resolución de casos prácticos con supervisión del capacitador.

Metodología

La capacitación combinó teoría breve con prácticas directas en la sala de control, utilizando el sistema en funcionamiento real.

Se empleó una metodología participativa, donde los operadores pudieron interactuar con la interfaz desde las estaciones de monitoreo asignadas.

Resultado esperado

Con esta etapa se aseguró que todos los operadores:

- Reconozcan y gestionen adecuadamente las alarmas generadas por los sistemas integrados.
- Utilicen las herramientas gráficas y de consulta de manera ágil.
- Respondan a incidentes siguiendo los protocolos de seguridad establecidos.

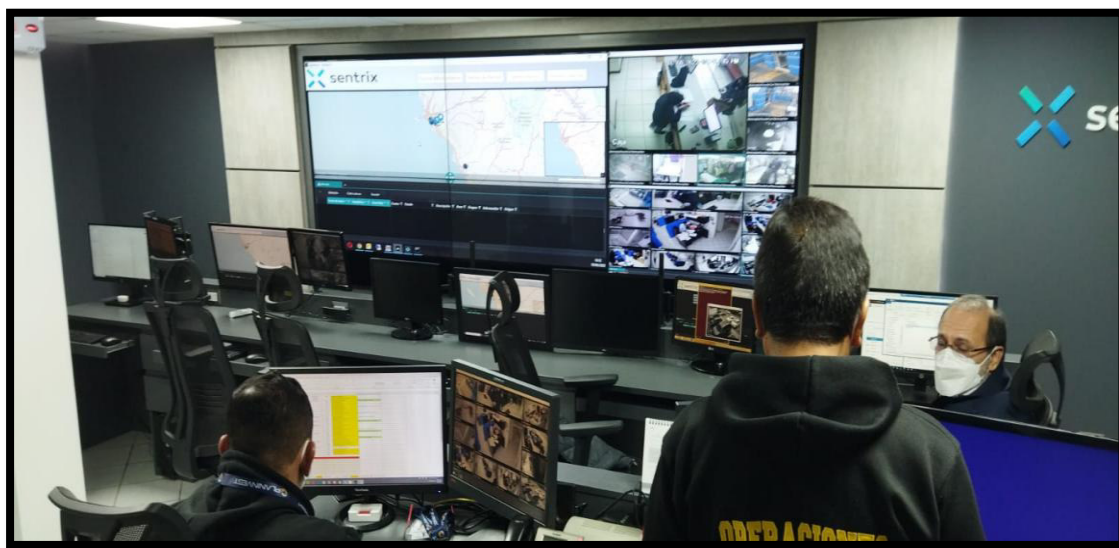


Figura 21. Capacitación del personal Planinvest. Fuente. Edición Propia.

3.6 Resultado de la actividad

Como resultado se obtuvo lo siguiente:

En primer lugar, una plataforma PSIM implementada, que integra el sistema de CCTV, sistema de intrusión, sistema de detección de incendios y sistema de control de acceso de la empresa Planinvest. Los dispositivos están representados mediante iconos que muestran su estado (alarmado, conectado, desconectado), facilitando la supervisión en tiempo real por parte de los operadores. Además, se ha configurado la correlación entre eventos de control de acceso y videovigilancia, permitiendo una verificación visual inmediata cuando ocurre una apertura (ver Fig.22).

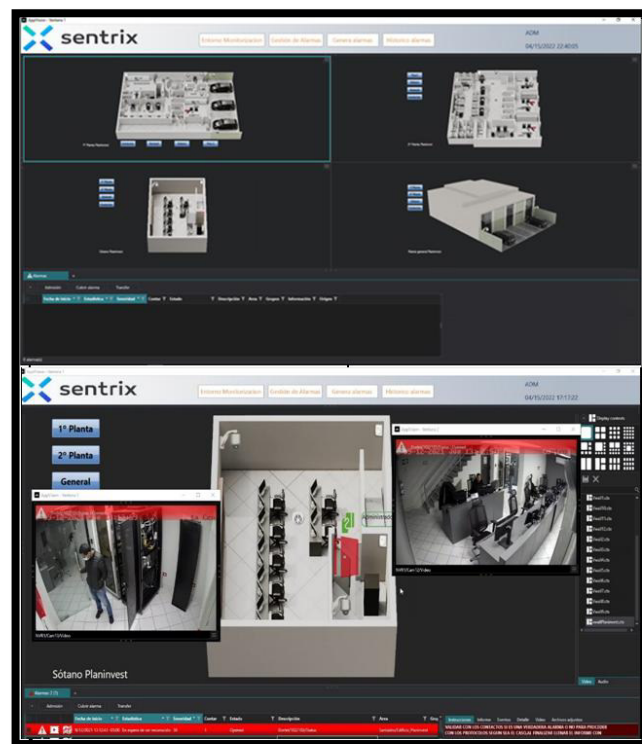


Figura 22 Interfaces de la empresa Planinvest. Fuente. Edición Propia.

En segundo lugar, una plataforma PSIM implementada que integra el sistema de CCTV de la empresa Martinizing, con interfaces específicas para cada sede (Chacarilla, Espinar, Primavera, dasso, planicie y dos de mayo) , en las que se representan los dispositivos mediante iconos gráficos que muestran su

estado (activo, desconectado, en alarma), lo cual permite a los operadores identificar situaciones anómalas en tiempo real (ver Fig. 23 a 25).

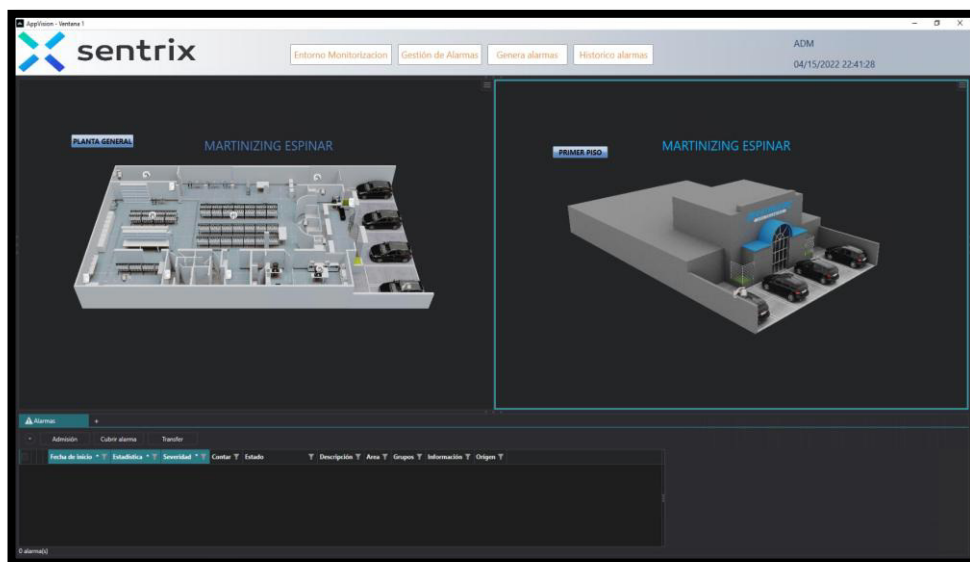


Figura 23. Interfaces de empresa Martinizing Espinar. Fuente. Edición Propia.

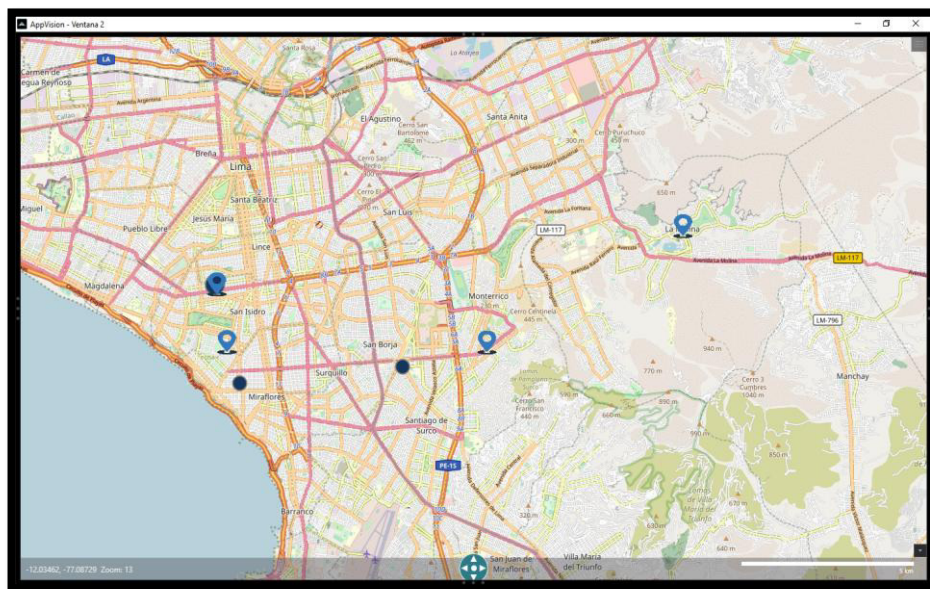


Figura 24 Interfaces de integración empresa Martinizing 6 sedes. Fuente. Edición Propia.



Figura 25 Interfaces de empresa Martinizing primavera. Fuente. Edición Propia.

En tercer lugar, una plataforma PSIM implementada que integra el sistema de CCTV y el sistema de intrusión de la empresa FUCSA. Los dispositivos están representados visualmente mediante iconos que indican su estado (conectado, alarmado, desconectado). Asimismo, se ha implementado la correlación entre eventos de control de acceso y cámaras, lo que permite a los operadores verificar visualmente, en tiempo real, cualquier evento generado desde las puertas (ver Fig. 26).

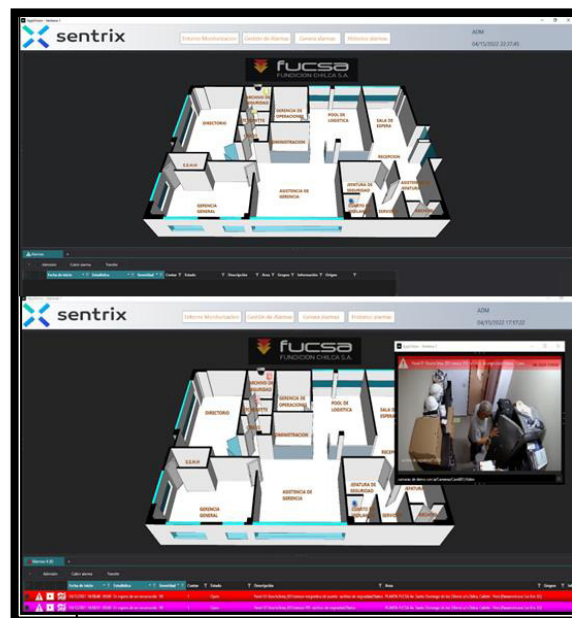


Figura 26 Interfaces de la empresa Fucsa. Fuente. Edición Propia

Por último, se obtuvo una interfaz consolidada que permite gestionar los sistemas de seguridad electrónica de Planinvest, Martinizing y Fucsa desde un centro de monitoreo unificado. Esta vista centralizada muestra las alarmas activas, el estado de todos los dispositivos integrados y permite una respuesta coordinada ante eventos de cualquier sede (ver Fig.27).

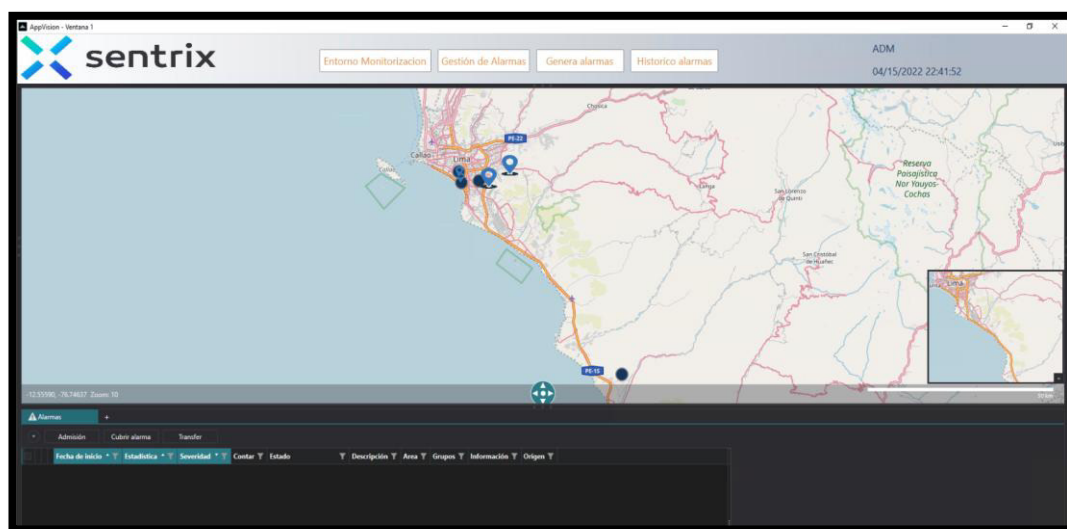


Figura 27 Vista principal de la plataforma PSIM. Fuente. Edición Propia.

CAPITULO IV: DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

La implementación de la plataforma PSIM se realizó utilizando drivers previamente desarrollados por el fabricante PRYSM, lo cual representó una ventaja técnica significativa para el proyecto. Estos drivers, ya utilizados en proyectos anteriores a nivel mundial, estaban diseñados para familias completas de modelos de cámaras y sistemas de control de acceso.

Gracias a ello, fue posible una integración directa sin necesidad de desarrollos adicionales, salvo la validación en campo (particularmente en los paneles Bosch) debido a una actualización reciente en su firmware. Como resultado, se logró una integración confiable y rápida, reduciendo los tiempos de desarrollo y los riesgos de incompatibilidad en comparación con el escenario inicial, donde los sistemas operaban sin comunicación entre sí.

El uso de drivers propietarios (no estándares como ONVIF para cámaras o Wiegand para lectoras) permitió una integración con mayor profundidad funcional en comparación con protocolos genéricos. Esto facilitó el acceso a un mayor número de variables específicas de cada dispositivo, optimizando la supervisión y el control operativo. Por ejemplo, en el sistema de videovigilancia se habilitó la visualización del estado operativo de cada cámara, alertas ante fallas y la generación automática de clips de video vinculados a eventos de control de acceso, todo desde una sola interfaz.

No fue necesario utilizar los softwares propietarios de cada sistema, salvo para tareas administrativas puntuales como la gestión de credenciales o la configuración avanzada de los grabadores. Como resultado, se incrementó la capacidad de monitoreo, pasando de sistemas aislados sin supervisión activa

a una plataforma unificada con control en tiempo real y mayor eficiencia operativa.

Desde el punto de vista operativo, los beneficios fueron claros. La plataforma consolidó todos los sistemas en una única interfaz, eliminando la necesidad de alternar entre múltiples aplicaciones. Los dispositivos fueron representados gráficamente sobre planos reales de las instalaciones, incluyendo su ubicación exacta, nombre descriptivo (empresa, piso, tipo de dispositivo) y su estado (activo, fallando, desconectado). Además, para cada evento relevante, se habilitó la navegación directa al sinóptico correspondiente mediante doble clic en los mensajes de alarmas, mejorando el tiempo de respuesta. Como resultado, se logró reducir significativamente los tiempos de identificación y atención de incidentes, en contraste con el escenario inicial, en el que no existía monitoreo activo y el soporte se limitaba al área de TI, que solo verificaba la operatividad básica de los equipos.

También se implementaron procedimientos operativos predefinidos para ciertos eventos, con instrucciones claras para los operadores. Estos podían añadir comentarios a los incidentes (por ejemplo: “falsa alarma”, “persona sospechosa”) y generar reportes consolidados con métricas clave como activaciones de alarma, fallas de dispositivos o estados de conectividad de los sistemas por empresa. Como resultado, se mejoró la trazabilidad de los eventos y se obtuvieron indicadores cuantitativos de desempeño, lo que antes no era posible debido a la ausencia de un sistema de supervisión común.

Finalmente, si bien se realizaron simulaciones con sistemas de detección de incendios para fines demostrativos y de capacitación, estas no formaron parte de la implementación operativa final, por lo que no fueron consideradas dentro del alcance formal del proyecto. No obstante, dichas simulaciones permitieron mostrar el potencial de la plataforma para integrar sistemas de detección de incendios direccionables en el futuro, los cuales podrían asociarse con cámaras cercanas para verificar en tiempo real si una alarma de incendio es real o falsa (por ejemplo, generada por polvo o partículas en el ambiente). Como resultado, se evidenció la escalabilidad de la solución y su potencial

para integrar nuevos subsistemas de seguridad conforme a las necesidades futuras del grupo empresarial.

4.2 Evaluación Económica

La evaluación económica de la implementación debe entenderse dentro del contexto particular del proyecto. En el presente proyecto, no se partió desde cero, ya que todas las empresas involucradas (Planinvest, Martinizing y Fucsa) contaban previamente con sistemas de videovigilancia y control de accesos operativos los cuales aún contaban con vida útil. Por tanto, la inversión no se destinó a la adquisición de hardware, sino a la centralización e integración de dichos sistemas mediante la plataforma PSIM.

Los principales costos asumidos fueron:

Licencias de software PSIM, en su versión redundante y con el paquete adecuado para soportar el número de cámaras, controles de acceso y funcionalidades requeridas.

Soporte técnico y mantenimiento anual, proporcionado por el fabricante. Este es obligatorio para garantizar el funcionamiento continuo y las actualizaciones del sistema.

Licencias de sistema operativo y servidor redundante. La solución se instaló en un servidor existente que cumplía con los requerimientos mínimos, pero que necesitaba una versión actualizada de Windows Server. El servidor redundante fue provisto por el fabricante como parte de una solución tipo “hardware all-in”. Cabe señalar que los requerimientos técnicos del software PSIM son bastante bajos, incluso puede ejecutarse en una PC de escritorio, aunque es más seguro hacerlo en un servidor con sistema operativo de servidor.

Adecuación inicial del centro de monitoreo, incluyendo la instalación del software cliente en las estaciones de trabajo de los operadores. Esto no generó costos adicionales, ya que las licencias solo son necesarias en el servidor. El software cliente puede instalarse en múltiples estaciones, pero

solo podrán operar simultáneamente aquellas permitidas por las licencias del servidor.

Disponibilidad de drivers. Uno de los factores más relevantes desde el punto de vista económico fue la disponibilidad de drivers ya desarrollados por el fabricante para los modelos de grabadores y sistemas de control de acceso utilizados. Estos drivers, creados en otros proyectos por parte del fabricante del PSIM debido a su alcance global, fueron proporcionados sin costo adicional. Esto representó un ahorro significativo, ya que el desarrollo de un driver personalizado puede superar los 10 mil euros por sistema, dependiendo de la complejidad además del tiempo que puede necesitar de 3 meses a más.

Este ahorro no fue registrado como partida presupuestaria reinvertida, pero permitió mantener el proyecto dentro de un marco de costos razonable. Si se hubiera optado por reemplazar todos los dispositivos por equipos de una sola marca (por ejemplo, Dahua) para luego implementar una solución del mismo fabricante, se habría incurrido en mayores costos de equipos, mano de obra, y tiempo sin los sistemas de seguridad operativos, lo que hubiera puesto en riesgo las instalaciones, especialmente considerando que se tiene proyectado integrar en el futuro a más empresas del grupo empresarial

Además, esta alternativa habría limitado la capacidad de crecimiento tecnológico, al depender de un solo fabricante. En cambio, con PSIM, las empresas pueden adquirir dispositivos de distintos fabricantes que ya cuentan con drivers desarrollados por PRYSM, y en caso contrario, solicitar su desarrollo.

En cuanto a la escalabilidad, la solución instalada permite integrar nuevos fabricantes, dispositivos y funcionalidades mediante la compra progresiva de licencias, sin necesidad de inversiones importantes en hardware ni en el núcleo de la plataforma. Esto permite una evolución gradual en función del crecimiento operativo de las empresas. Además, mientras se mantenga el soporte técnico, todas las actualizaciones del software son gratuitas, ya que PRYSM continúa desarrollando mejoras y nuevas funcionalidades para su plataforma.

CAPITULO V: CONCLUSIONES

El levantamiento de información inicial permitió identificar las tecnologías, fabricantes y modelos de equipos presentes en cada empresa, así como la forma en que eran gestionados sus sistemas de seguridad. Se constató que la gestión era mínima, limitada al soporte del área de TI para verificar la operatividad básica de los dispositivos, sin contar con operadores dedicados al monitoreo ni procedimientos de supervisión en tiempo real. Este diagnóstico evidenció la necesidad de unificar la gestión mediante un centro de monitoreo, y sirvió de base para definir los requerimientos de integración y operatividad.

La preparación e instalación del software AppVision™ y de sus componentes (drivers) estableció la infraestructura tecnológica necesaria para garantizar la comunicación con los sistemas a integrar y permitió iniciar la siguiente etapa sin inconvenientes.

La implementación de la solución PSIM (Physical Security Information Management) en las empresas Planinvest, Martinizing y Fucsa permitió la integración de sistemas heterogéneos de videovigilancia y control de accesos en una sola plataforma, logrando una mejora sustancial en la eficiencia operativa. A diferencia de soluciones tradicionales como los VMS o software limitados al ecosistema de un único fabricante, el PSIM permitió centralizar dispositivos de distintas marcas en una sola interfaz, sin necesidad de reemplazos costosos ni interrupciones del servicio por cambios de equipos. Además, asegura una escalabilidad futura que solo depende de la adquisición de licencias adicionales.

Las pruebas realizadas a los dispositivos integrados validaron la interoperabilidad entre subsistemas, confirmando la confiabilidad de la implementación y reduciendo los riesgos de incompatibilidad. Esta etapa

aseguró que los sistemas pudieran operar de manera coordinada bajo la plataforma PSIM.

La evaluación del entorno de trabajo del operador evidenció beneficios directos en la operación diaria: se redujeron los tiempos de respuesta ante incidentes, se disminuyeron las falsas alarmas gracias a la correlación automática de eventos y se optimizó el trabajo de supervisión mediante el uso de sinópticos interactivos y reportes personalizados.

La capacitación brindada al personal operativo permitió asegurar la correcta adopción de la plataforma, garantizando la continuidad de su operatividad y reduciendo la dependencia de soporte externo inmediato. Asimismo, las simulaciones realizadas evidenciaron el potencial de la plataforma para ampliar su alcance hacia otros subsistemas de seguridad en el futuro.

La solución implementada no solo permitió integrar los sistemas existentes de tres empresas del grupo, sino que también elevó el nivel de control, eficiencia y escalabilidad en la operación diaria. Esto demuestra que un enfoque basado en PSIM es altamente efectivo para organizaciones que buscan evolucionar tecnológicamente sin comprometer sus recursos existentes ni depender de un único proveedor. Además, la arquitectura abierta de la plataforma garantiza que en el futuro no se limite la adopción de soluciones más potentes en hardware, ya que los sistemas podrán ser reemplazados o actualizados sin generar costos adicionales por licencias, más allá de la incorporación de nuevos dispositivos que requieran conectividad mediante drivers

CAPITULO VI: RECOMENDACIONES

Cuando se diseñen soluciones orientadas a la integración de sistemas de seguridad electrónica, una de las alternativas más eficientes es el uso de plataformas PSIM (Physical Security Information Management). Estas permiten tanto la gestión centralizada de sistemas ya existentes como el desarrollo de proyectos desde cero, facilitando un crecimiento tecnológico sin depender de un único fabricante. Esto brinda a las organizaciones la libertad de seleccionar proveedores con mejores tecnologías y costos.

Las plataformas PSIM son altamente adaptables a escenarios diversos y actualmente evolucionan de forma constante, integrando funcionalidades relacionadas con la ciberseguridad y el Internet de las Cosas (IoT). Por ello, se recomienda profundizar en el estudio, comparación y análisis técnico de estas soluciones al momento de plantear una estrategia de integración.

Para una implementación exitosa, es fundamental realizar un levantamiento técnico detallado. Esto incluye identificar las topologías existentes, los modelos de los equipos involucrados y los protocolos de comunicación que utilizan. Esta información resulta clave para elegir el método de integración más económico y viable, ya que en muchos casos se requiere solicitar al fabricante del PSIM drivers específicos o incluso el desarrollo de nuevos, con el fin de permitir la comunicación entre el PSIM y los dispositivos.

En los casos donde sea necesario desarrollar drivers personalizados, actualmente la mayoría de fabricantes de sistemas de seguridad electrónica ofrecen SDKs o APIs que facilitan la integración con terceros. Se recomienda gestionar reuniones técnicas entre los representantes de los distintos fabricantes para evaluar la viabilidad, complejidad y costos de dicho desarrollo. Dependiendo de la complejidad, un driver personalizado puede implicar tiempos prolongados y costos significativos de implementación.

En ese sentido, resulta estratégico elegir plataformas PSIM que ya cuenten con un amplio catálogo de integraciones preexistentes, lo cual reduce significativamente los tiempos de implementación y el presupuesto total del proyecto. Este factor es especialmente relevante en proyectos de mediana o gran escala, donde la optimización de recursos y plazos resulta determinante para su éxito.

Adicionalmente, se recomienda establecer planes de pruebas periódicas que validen la interoperabilidad de los dispositivos integrados frente a cambios de firmware o actualizaciones de drivers, evitando interrupciones en la operación. Del mismo modo, se aconseja recopilar retroalimentación continua de los operadores para optimizar la interfaz gráfica, las alarmas y los reportes de acuerdo con la dinámica de cada empresa, aprovechando que la plataforma puede actualizarse en función de nuevas necesidades. Finalmente, se recomienda implementar programas de capacitación continua y generar manuales internos de operación, a fin de garantizar la transferencia de conocimiento y la sostenibilidad del proyecto a largo plazo.

CAPITULO VII: BIBLIOGRAFÍA

Bosch Security Systems. (2020). *Video Systems Guidebook*. Bosch GmbH.

Cuppens, N., & Cuppens, F. (2015). *Security Information Management for Integrated Physical and Logical Security*. Springer.

Espillico, F. (2015). *Diseño e implementación de un sistema integral de seguridad, controlado y monitoreado en forma local y remota mediante las redes de comunicación para las agencias de Caja Rural – Los Andes S.A.* [Tesis de licenciatura, Universidad Nacional del Altiplano]. Repositorio Institucional.

Honeywell. (2019). *Intrusion Detection System Overview*. Honeywell Security Group.

Microsoft. (2020). *What is a software development kit (SDK)?* <https://learn.microsoft.com/en-us/windows/uwp/get-started/what-is-a-sdk>

Modbus Organization. (2012). *Modbus Messaging on TCP/IP Implementation Guide v1.0b*. <https://modbus.org>

Nilsson, J. (2012). *Security integration: The rise of PSIM platforms*. *Security Technology Executive*, 22(3), 14–17.

OPC Foundation. (2021). *What is OPC?* <https://opcfoundation.org>

Pappalardo, A. (2013). *A framework for threat recognition in physical security information management* [Tesis doctoral, Università degli Studi di Napoli Federico II]. FedOA. http://www.fedoa.unina.it/9120/1/Pappalardo_Alfio_25.pdf

Pérez, J. (2016). *Diseño de un sistema de seguridad electrónica con monitoreo centralizado para protección de una instalación minera* [Tesis de licenciatura, Universidad Nacional de Ingeniería]. Repositorio Institucional.

Prysm Software. (2021). *AppVision™ User Guide v4.6*. PRYSM SAS.

Red Hat. (2022). *What is an API?* <https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces>

CAPITULO IX: ANEXOS

Anexo A – Etapa 1: Planificación y Levantamiento de Información

Sistemas de seguridad electrónica empresa Planinvest.

La empresa Planinvest dispone de un sistema de videovigilancia (CCTV) y un sistema de control de accesos. Sin embargo, actualmente no cuenta con un operador dedicado al monitoreo continuo de estos sistemas.

La gestión se encuentra a cargo del área de TI, cuya labor se limita principalmente a verificar que los equipos se encuentren encendidos, conectados y operativos desde el punto de vista básico. No se realiza supervisión activa de las cámaras, ni se efectúa un seguimiento en tiempo real de los eventos o alarmas que puedan generarse. Asimismo, no existen procedimientos operativos definidos para la atención de incidentes, ni una centralización de información que permita analizar eventos de manera ordenada.

Esta condición representa una gestión pasiva del sistema, orientada únicamente a mantener la infraestructura funcionando, sin explotar las capacidades de seguridad que ofrecen estos subsistemas.

La empresa Planinvest cuenta con los siguientes sistemas:

Un sistema de CCTV analógico con un DVR del fabricante Hikvision de 16 canales, de los cuales utiliza 12. Se recopiló la información necesaria para su integración. (Ver Cuadro A1).

Cuadro A1 Sistema de CCTV empresa Planinvest.

Empresa (Coordenadas geográficas)	Lugar	Tipo de sistema	Puerto	Número	Fabricante	Modelo	IP	Usuario/Contraseña	Canales de grabador	Nombre de la cámara	Ubicación	Estado
PLANINVEST (- 12.09225, - 77.04605)	San Isidro	CCTV	tcp port	3xxxx	HIKVISION	DS- 7216HQHI- F2/N	XXX.XXX.X.XXX	XXXXX/XXXXX	Cam01	Calle 2	Según planos	Operativo
			udo port	3xxx					Cam02	...	...	Libre
			http port	8xx					Cam03	Recepción 1	Según planos	Operativo
									Cam04	Recepción 2	Según planos	Operativo
									Cam05	Sala de espera	Según planos	Operativo
									Cam06	Salón	Según planos	Operativo
									Cam07	Oficina 1	Según planos	Operativo
									Cam08	oficina 2	Según planos	Operativo
									Cam09	Escalera	Según planos	Operativo
			rtsp	5xx					Cam10	Administración 1	Según planos	Operativo
									Cam11	Administración 2	Según planos	Operativo
									Cam12	Control Center	Según planos	Operativo
									Cam13	Calle 2	Según planos	Operativo
									Cam14	-----	-----	Libre
									Cam15	-----	-----	Libre
									Cam16	-----	-----	Libre

Fuente. Elaboración propia.

Un sistema de control de acceso marca Dorlet, bajo topología cliente-servidor. El software utilizado es DASSNET SERVER. Se cuenta con una controladora utilizando una de las dos entradas de lectoras para controlar el acceso a la data center. (Ver Cuadro A2).

Cuadro A2 Sistema de control de acceso empresa Planinvest.

Empresa (Coordenadas geográficas)	Lugar	Tipo de sistema	Puerto	Número	Fabricante	Modelo	IP	Usuario/Contraseña	Nombre de lectora	Número de device ID	Ubicación	Estado
PLANINVEST (-12.09225, -77.044051)	San Isidro	Control de acceso	tcp port	8xxx	DORLET	DASSNET SERVER 2.4.20	Local host	XXXXX/XXXXX	Lector_1_51	103	Puerta Data Center	Operativo
									Lector_2_51	203	-----	Libre

Fuente. Elaboración propia

Sistema de detección de incendios mediante un panel de intrusión modelo VISTA-48LA/64SP del fabricante Honeywell, con tres lazos que conectan detectores de humo convencionales. Al no existir driver para este panel, se evaluó el desarrollo con el fabricante PRYSM. Sin embargo, por los costos y el tiempo requerido, se decidió simular el sistema para fines de capacitación y modo demo. (Ver Cuadro A3).

Cuadro A3 Sistema de detección de incendios empresa Planinvest

Empresa (Coordenadas geográficas)	Lugar	Tipo de sistema	Cantidad de sensores	Piso	Nombre de variable	Nota
PLANINVEST (-12.09225, -77.044051)	San Isidro	Sistema de detección de incendio	Sensor 01	Piso 01	Oficina	Sistema simulado
			Sensor 02	Piso 01	Área de usos múltiples	
			Sensor 03	Piso 01	Almacén	
			Sensor 04	Piso 02	Hall	
			Sensor 05	Sótano	Sala de monitoreo	

Fuente. Elaboración propia

Sistema de intrusión de la empresa Verisure. Debido a que PRYSM no cuenta con driver para este panel y no es factible obtener SDK del fabricante, se descartó la integración. Se simuló el sistema para capacitación en modo demo. (Ver Cuadro A4).

Cuadro A4 Sistema de intrusión empresa Planinvest.

Empresa (Coordenadas geográficas)	Lugar	Tipo de sistema	Cantidad de sensores	Piso	Nombre de variable	Nota
PLANINVEST (-12.09225, - 77.044051)	San Isidro	Sistema de intrusión	PIR 01	Piso 01	PIR área de usos múltiples	Sistema simulado
			PIR 02	Piso 01	PIR almacén	
			PIR 03	Piso 02	PIR hall	
			PIR 04	Sótano	PIR sala de monitoreo	
			PIR 05	Sótano	PIR data center	

Fuente. Elaboración propia

Sistemas de seguridad electrónica empresa Martinizing.

Dispone únicamente de un sistema de CCTV en sus distintas sedes. No cuenta con operadores que monitoreen las cámaras de manera constante. El área de TI es la responsable de revisar que los equipos funcionen, sin embargo, no realiza supervisión operativa ni atiende las alarmas en el momento en que ocurren.

Para esta empresa se integran los sistemas de CCTV de seis sucursales en Lima:

- Chacarilla: DVR de 8 canales (8 usados)
- Espinar: DVR de 8 canales (6 usados)
- Primavera: DVR de 4 canales (1 usado)
- Dasso: DVR de 4 canales (1 usado)
- Planicie: DVR de 4 canales (1 usado)
- Dos de Mayo: DVR de 4 canales (1 usado)

Se recopiló información necesaria para la integración (ver Cuadro A5).

Cuadro A5 Sistema de CCTV empresa Martinizing

Empresa	Coordenadas geográficas)	Tipo de sistema	Puerto	Número	Fabricante	Modelo	IP	Usuario/Contraseña	Canales del grabador	Nombre de la cámara	Ubicación	Estado
MARTINIZING	Chacarilla (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	NOVA	NV-DVR3108E	192.xxx.	admin/xxxxx	Cam01	Estac. 2	Según planos	Operativo
			udp port	3xxxx					Cam02	Lavado		Operativo
			http port	8xx					Cam03	Estac 1		Operativo
			rstp	5xx					Cam04	Recepción		Operativo
									Cam05	Cajas		Operativo
									Cam06-08	Sin nombre		Operativo
MARTINIZING	Espinar (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	DAHUA	DH-XVR4108HS	192.xxx.	admin/xxxxx	Cam01,02,08			Libre
			udp port	3xxxx					Cam03	Lavado	Según planos	Operativo
			http port	8xx					Cam04	Recepción		Operativo
			rstp	5xx					Cam05-07	Sin nombre		Operativo
MARTINIZING	Primavera (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	DAHUA	DHI-HCVR5104H	192.xxx.	admin/xxxxx	Cam01-03			Libre
			rstp	5xx					Cam04	Primavera	Según planos	Operativo
MARTINIZING	Dasso (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	DAHUA	DHI-HCVR5104H	192.xxx.	admin/xxxxx	Cam01	Dasso	Según planos	Operativo
			udp port	3xxxx					Cam02-04			Libre
MARTINIZING	Planicie (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	DAHUA	DHI-HCVR5104H	192.xxx.	admin/xxxxx	Cam01	Planicie	Según planos	Operativo
			udp port	3xxxx					Cam02-04			Libre
MARTINIZING	Dos de mayo (1x.xx, 7x.x)	CCTV	tcp port	3xxxx	DAHUA	DH-XVR4104HS	192.xxx.	admin/xxxxx	Cam01,03-04			Libre
			udp port	3xxxx					Cam02	Dos de mayo	Según planos	Operativo

Fuente. Elaboración propia.

Sistemas de seguridad electrónica empresa FUCSA.

La Dispone de un sistema de CCTV y un sistema de detección de intrusión. No cuenta con operadores encargados del monitoreo en tiempo real. La responsabilidad recae en el área de TI, que, solo valida el estado funcional de los equipos, pero no gestiona directamente las cámaras ni las alarmas generadas durante el día a día.

La empresa FUCSA cuenta con cámaras analógicas con visión nocturna, y un sistema de intrusión con un sensor magnético, un sensor PIR con doble tecnología (infrarrojo y microondas Doppler) y un pulsador de emergencia en la sala de control. (Ver Figura A1)

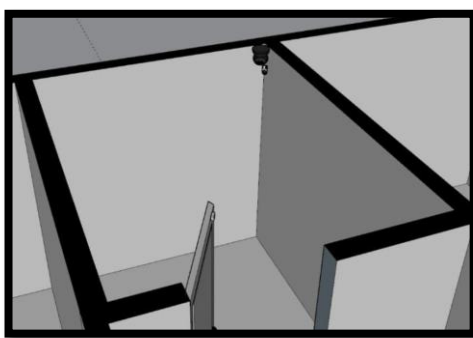


Figura A1 Cámara, PIR y sensor magnético. Fuente. Edición Propia.

Sistema de CCTV analógico de 4 canales marca Dahua (ver cuadro A6).

Cuadro A6 Sistema de CCTV empresa Fucsa

Empres a (Coorde nadas geográfi cas)	Lu gar	Tipo de siste ma	Pue rto	Núm ero	Fabric ante	Modelo	IP	Usuario/Co ntraseña	Can ales del grab ador	Nom bre de la cáma ra	Ubica ción	Esta do
FUCSA (- 12.5679 68, - 76.6351 32)	Chi lca	CCT V	tcp port	3xxx	DAHU A	DH- XVR51 04HS-I3	177.xxx. xx.xxx	Admin/xxxx	Cam 01	Archi vos gener ales	Según plano s	Oper ativo
			udp port	3xxx					Cam 02	Sin uso		Libre
			http port	8xx					Cam 03	Sin uso		Libre
			rtsp	5xx					Cam 04	Sin uso		Libre

Fuente. Elaboración propia

Sistema de intrusión marca Bosch serie B. Incluye: sensor magnético en puerta, un PIR de doble tecnología y un pulsador de emergencia (ver Cuadro A7).

Cuadro A7 Sistema de intrusión empresa Fucsa

Empresa (Coordenadas geográficas)	Lugar	Tipo de sistema	Puerto	Número	Fabricante	Modelo	IP	Usuario/Contraseña	Input del panel	Tipo de dispositivo	Ubicación	Estado
FUCSA (-12.567968, -76.635132)	Chilca	Sistema de intrusión	tcp port	7xxx	BOSCH	BG5112	172.xxx.xx.xxx	admin/XXXXX	Poi nt 01	Sensor PIR	Archivado de seguridad	Operativo
									Poi nt 02	Sensor magnético	Puerta de archivo de seguridad	Operativo
									Poi nt 03	Pulsador de emergencia	Cuarto de vigilancia	Operativo

Fuente. Elaboración propia

Requerimientos del cliente para el desarrollo de la interfaz del monitoreo.

Mediante lluvia de ideas y reuniones con el jefe de sistemas y el área usuaria de operaciones de Planinvest, se definieron las siguientes funcionalidades para la interfaz del operador:

- Un mapa donde se aprecie todas las empresas con coordenadas geográficas.
- Matriz de cámaras por cliente.
- Barra donde se muestre las alarmas.
- Planos 3D por cada cliente.
- Colocar el logo de la empresa Planinvest.
- Mostrar la fachada y todos los pisos existentes de las empresas.

- Relacionar sistemas.
- Workflow.
- Acceso directo a históricos.

Integración de sistema de CCTV.

Fabricantes Dahua y Hikvision: Se cuenta con drivers desarrollados que permiten integrar todas las funcionalidades. La implementación se basó en la documentación técnica proporcionada por PRYSM.

Integración de sistema de Control de acceso.

Fabricante Dorlet: Se cuenta con driver para comunicación con el servidor y visualización de eventos desde DASSNET. La implementación se basó en la documentación oficial de PRYSM.

Integración del sistema de intrusión.

Fabricante Bosch: Se cuenta con driver para las series B y G. Este se conecta directamente con los paneles para obtener información y permitir su gestión. Debido a que es un driver recientemente desarrollado, se implementó con soporte directo del fabricante.

Anexo B – Etapa 2: preparación e instalación del software AppVision

Instalación del software PSIM.

Se trabajó con el fabricante PRYSM y su software PSIM AppVision. Se procedió con la instalación de los sistemas operativos Windows 10 Pro para las computadoras destinadas a los operadores y Windows Server 2016 para el servidor principal.

Las PC y los sistemas operativos cumplan con los requisitos mínimos especificados en el AppVision – Configuration Manual v4.7. (Ver Fig. B1).

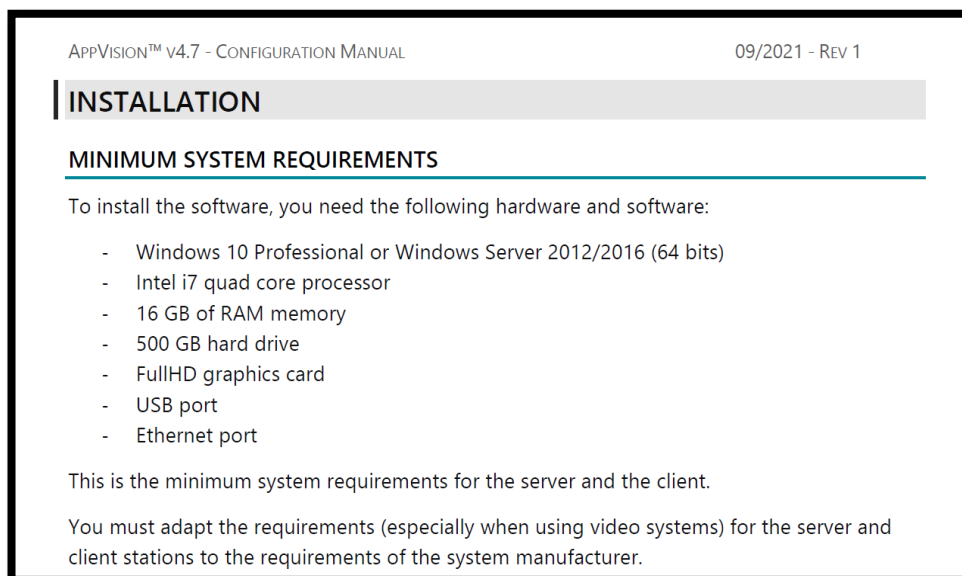


Figura B1 Requisitos mínimos de hardware. Fuente. AppVision v4.7 Configuration Manual.

Configuración de parámetros de red.

Se asignaron las direcciones IP de acuerdo con el cuadro definido por el área de sistemas de la empresa Planinvest (ver Tabla B1).

Cuadro B1 Distribución de IP para el proyecto

Nombre	IP	Gateway	Máscara	DNS
Operador 01	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Operador 02	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Operador 03	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Operador 04	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Operador 05	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Servidor principal	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX
Servidor redundante	172.XX.X.XX	172.XX.X.XX	255.255.255.0	172.XX.X.XX

Fuente. Elaboración propia

La PC cliente también funcionó como servidor redundante. Para su configuración, se accedió a las propiedades de Ethernet y se asignaron los parámetros definidos en la Tabla B1. (Ver Fig. B2).

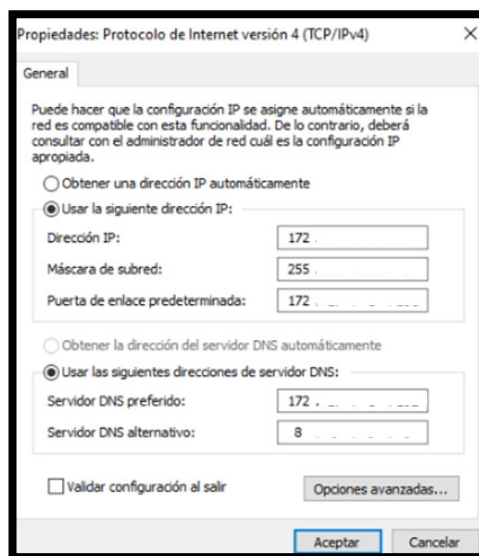


Figura B2 Parámetros de red PC cliente servidor redundante. Fuente. Edición Propia.

En el caso del servidor principal, se repitió el procedimiento ingresando a las propiedades de Ethernet y asignando las direcciones IP correspondientes (ver Fig. B3)

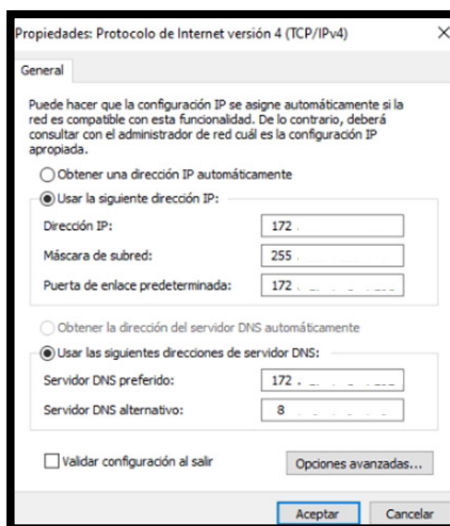


Figura B3 Parámetros de red PC servidor principal. Fuente. Edición Propia.

Instalación del aplicativo servidor.

Con los sistemas operativos y las tarjetas de red correctamente configurados, se inició la instalación del aplicativo en el servidor principal y el redundante (procedimiento idéntico para ambos).

En cada servidor, se copió la carpeta Setup AppVision 4.7 al escritorio, se descomprimió y se ejecutó como administrador el archivo setupClientServer.exe (ver Fig. B4).

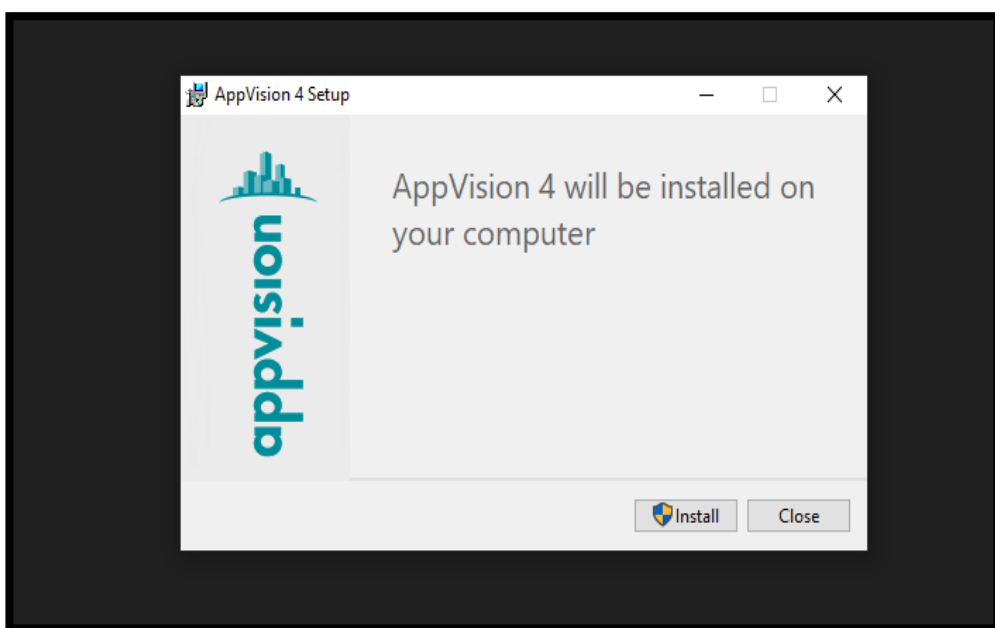


Figura B4 Instalación de servidor AppVision. Fuente. Edición Propia.

Al finalizar la instalación, se crearon tres accesos directos en el escritorio:

- AppVision configurator: para el desarrollo de la plataforma de los operadores.
- AppVision client: para que operadores y desarrolladores accedan a la plataforma.
- AppVision server: para iniciar el servicio del servidor de AppVision.

Ver Fig. B5



Figura B5 Accesos directos AppVSION. Fuente. Edición Propia.

Instalación de las licencias.

Con las licencias recibidas, se accedió al AppVision configurator (ver Fig. 13), se inició sesión con el usuario ADM y la contraseña 123 (ver Fig. 14), y se ingresó al menú Licencia > Activación de la licencia. Se seleccionó el archivo proporcionado y se activó. (Ver Fig.B6, B7 y B8).

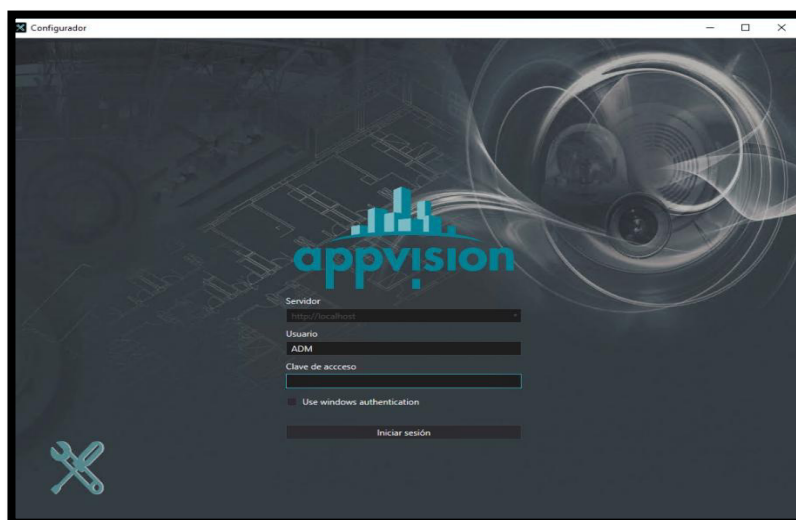


Figura B6 Ventana de acceso al aplicativo “Configurador” de AppVision. Fuente. Edición Propia.



Figura B7 **Ventana principal del aplicativo “Configurador” de AppVision.** Fuente. Edición Propia.

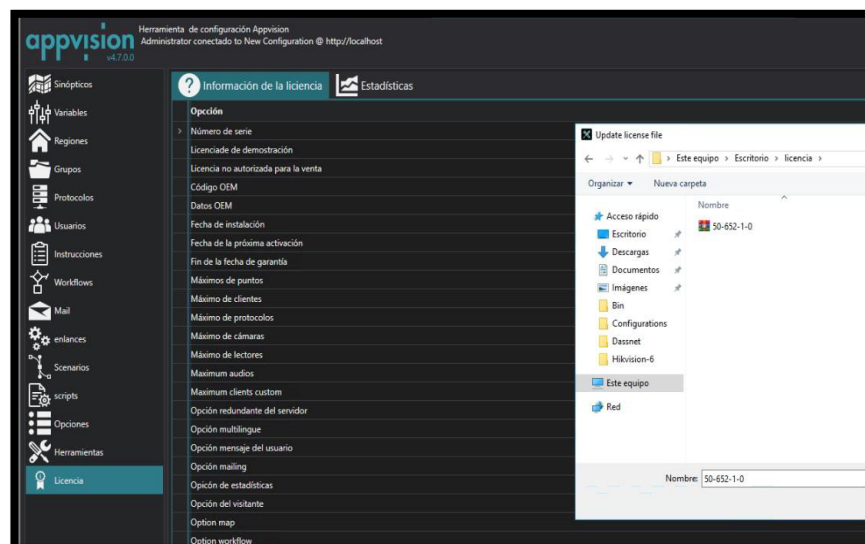


Figura B8 **Licenciamiento del servidor.** Fuente. Edición Propia.

Posteriormente, se reinició el servidor y se verificó que las funcionalidades adquiridas estuvieran habilitadas, como:

- 2500 variables simultáneas.
- clientes concurrentes.
- 8 protocolos máximos.
- 1512 variables de tipo cámara.
- Redundancia de servidor.
- Envío de mensajes y workflow.

Ver Fig. B9

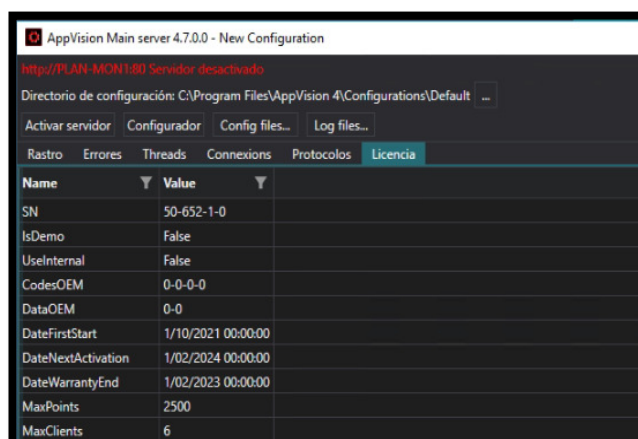


Figura B9 Parámetros de la licencia del servidor AppVision. Fuente. Edición Propia.

Con ambas licencias cargadas, se activaron los servidores desde la opción Activar servidor, ejecutando por defecto el proyecto Default (ver Fig. B10).

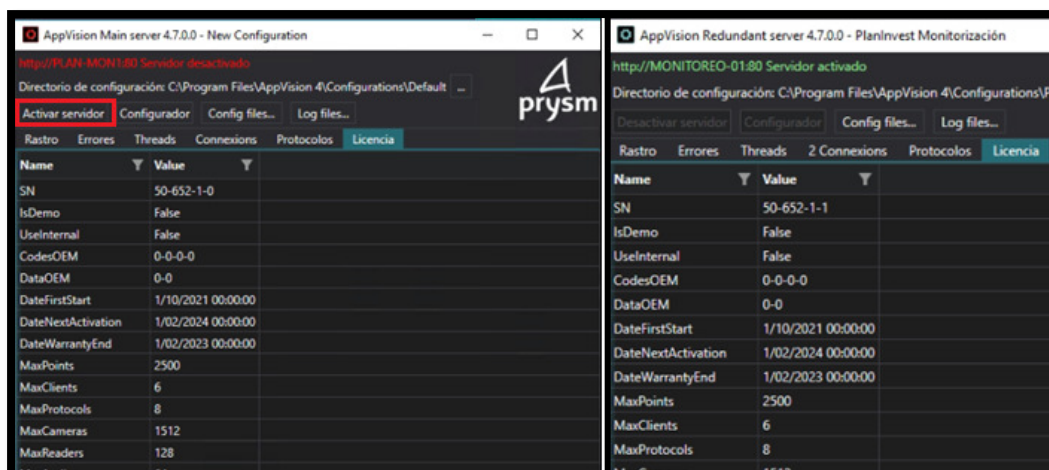


Figura B10 Activación de Servidor AppVision. Fuente. Edición Propia.

Configuración de la redundancia.

La redundancia se implementó siguiendo el manual AppVision 4.6 Apo Backup Redundancy.

Configuración de la redundancia en el servidor principal.

En el servidor principal, desde el AppVision configurator, se accedió a Opciones > Redundant server, ingresando las direcciones IP del servidor principal (URL main server) y del redundante (URL redundant server). (Ver Fig. B11 y B12).

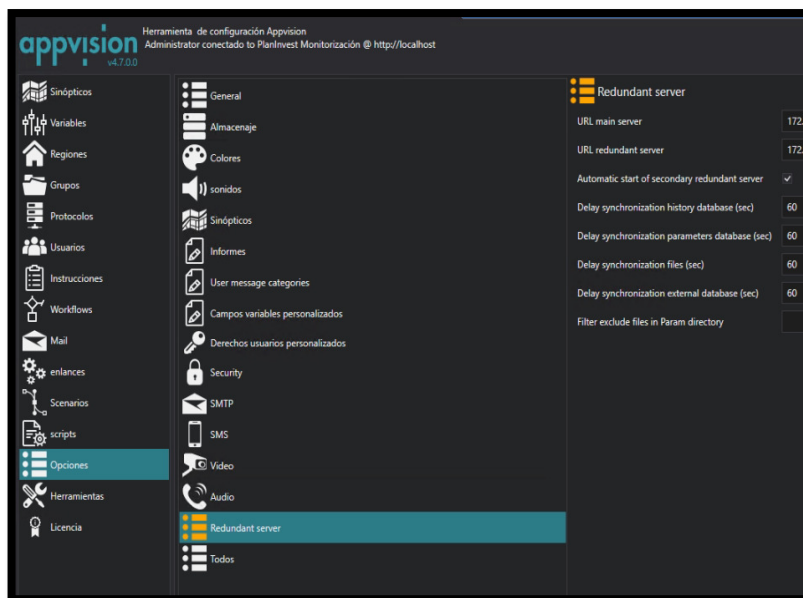


Figura B11 Configuración de redundancia servidor principal. Fuente. Edición Propia.

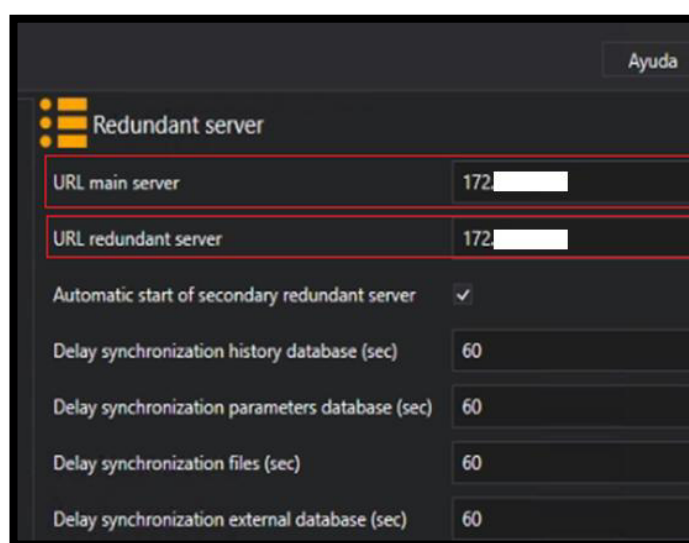


Figura B12 Configuración de redundancia. Fuente. Edición Propia.

Instalación AppVision en estaciones de monitoreo.

En las PCs de los operadores se instaló el cliente AppVision para acceder al servidor y cargar la interfaz del operador (ver Fig. B13).

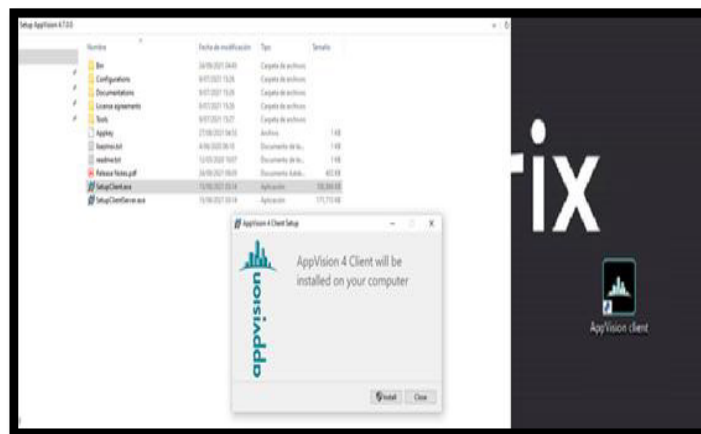


Figura B13 Instalación de AppVision cliente. Fuente. Edición Propia.

Instalación de drivers según fabricante a integrar.

Se descargaron los drivers desde la plataforma de soporte PRYSM (ver Fig. B14).

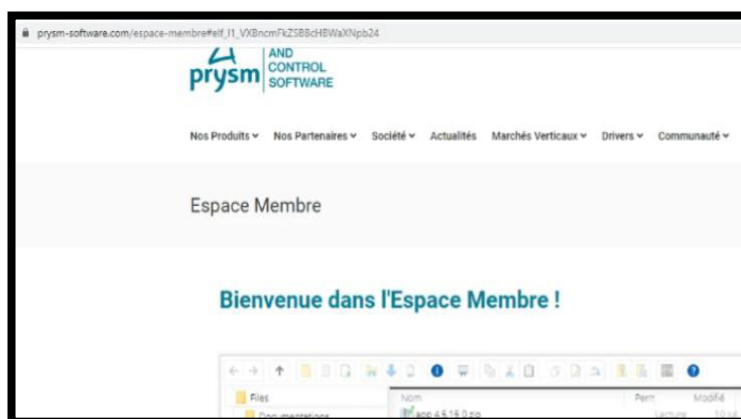


Figura B14 Plataforma PRYSM de soporte. Fuente. Edición Propia.

Integración HIKVISION.

Para integrar los equipos de este fabricante, como primer paso se instalan todos los archivos necesarios para su funcionamiento, siguiendo los pasos detallados en la documentación *HIKVISION supervision with AppVision* (ver Fig. 22). Todos los archivos se copian en la carpeta C:\Program Files (x86)\AppVision 4.0\Bin para que el driver funcione correctamente (ver Fig.B15 y B16).

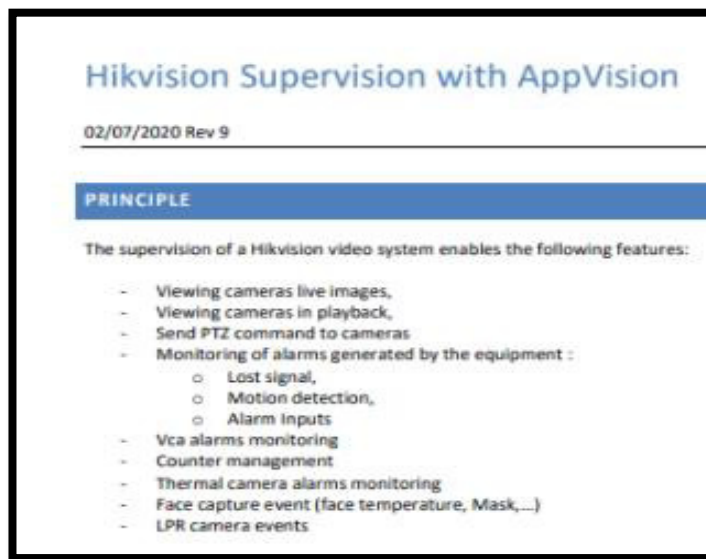


Figura B15 Manual para la integración de equipos Hikvision. Fuente. Manual Hikvision supervisión with App Visión.

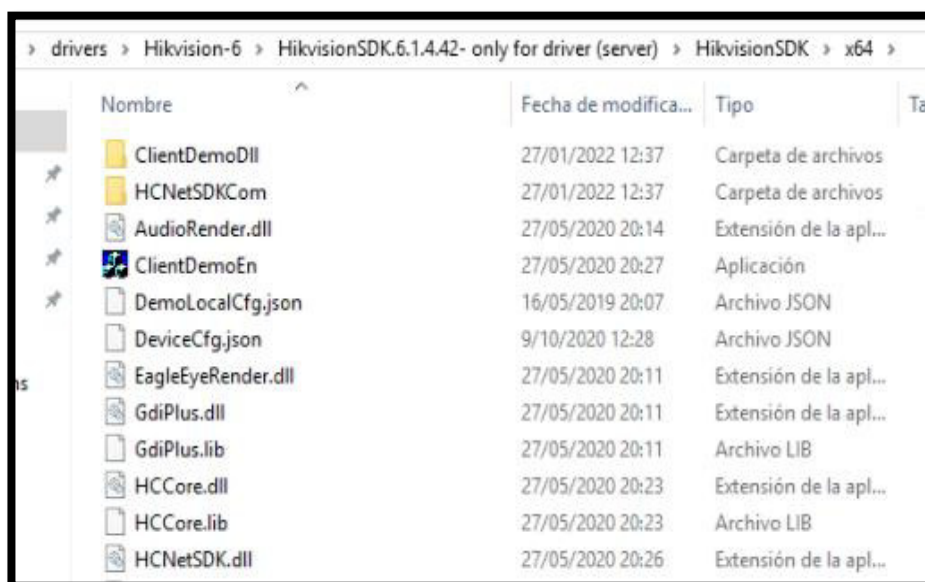


Figura B16 Archivos para la integración con Hikvision. Fuente. Edición Propia.

Integración DAHUA.

Para integrar los equipos de este fabricante, como primer paso se instalan todos los archivos necesarios para su funcionamiento, siguiendo los pasos detallados en la documentación DAHUA NVR SUPERVISION (ver Fig. 24). Todos los archivos se copian en la carpeta C:\Program Files (x86)\AppVision 4.0\Bin para que el driver funcione correctamente. (Ver Fig. B17 y B18).

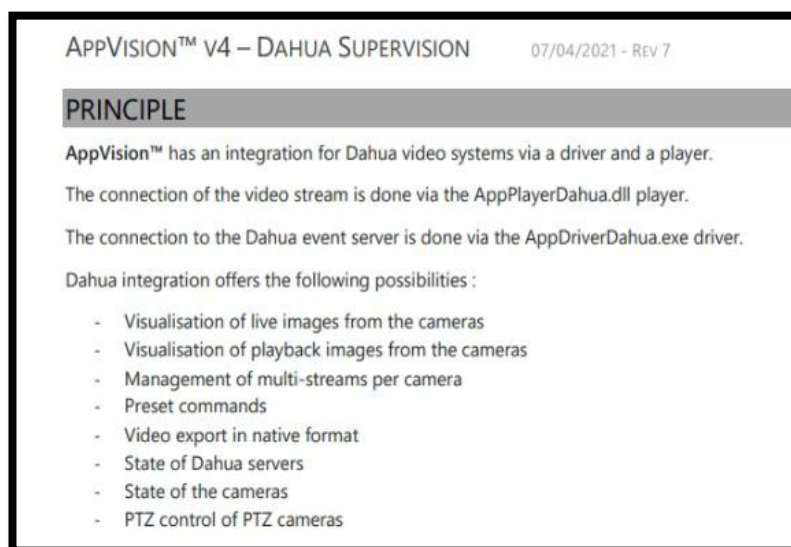


Figura B17 Manual para la integración de equipos Dahua. Fuente. Manual AppVision v4-Dahua supervisión.

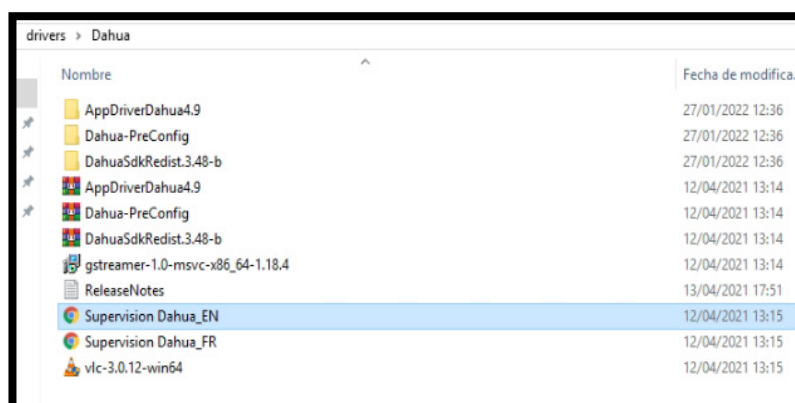


Figura B18 Archivos para la integración con Dahua. Fuente. Edición Propia.

Integración Bosch.

Para integrar los equipos de este fabricante, como primer paso se instalan todos los archivos necesarios para su funcionamiento. Todos los archivos se copian en la carpeta C:\Program Files (x86)\AppVision 4.0\Bin para que el driver funcione correctamente (ver Fig. B19).

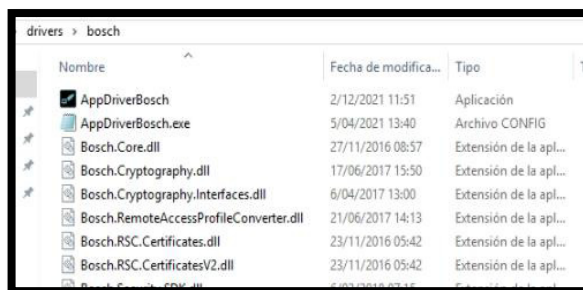


Figura B19 Documentos para la integración con Bosch. Fuente. Edición Propia.

Integración Dorlet

Para integrar los equipos de este fabricante, como primer paso se instalan todos los archivos necesarios para su funcionamiento, siguiendo los pasos detallados en la documentación *DORLET supervision* (ver Fig. 27). Todos los archivos se copian en la carpeta C:\Program Files (x86)\AppVision 4.0\Bin para que el driver funcione correctamente. (Ver Fig. B20 y B21).



Figura B20 Manual para la integración de equipos Dorlet. Fuente. Manual Dorlet supervisión.

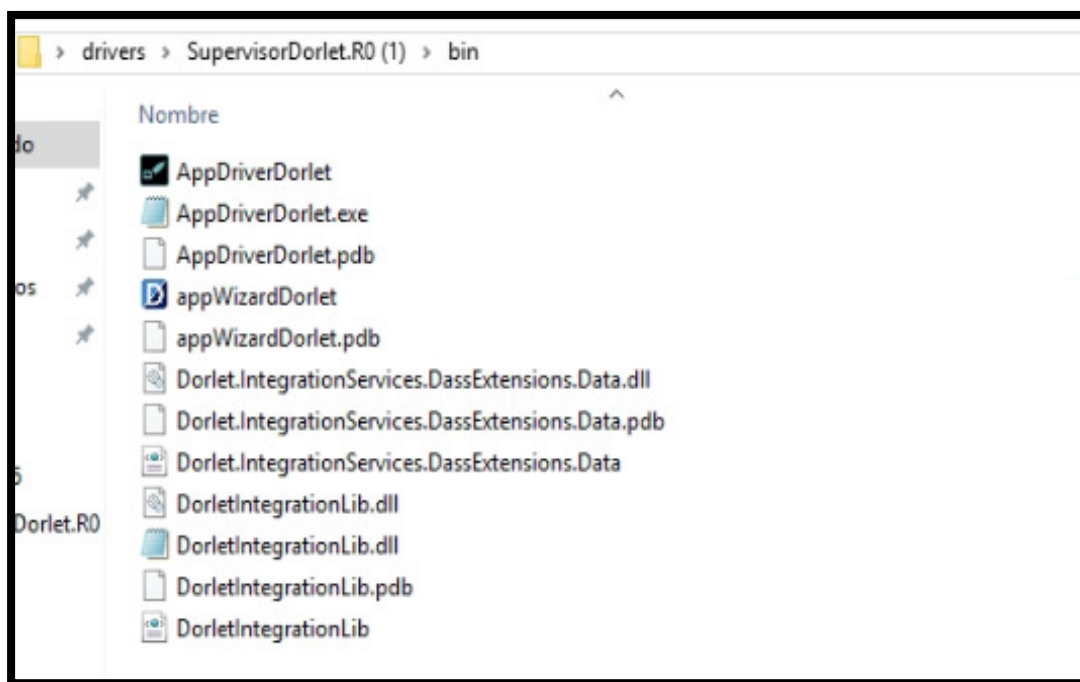


Figura B21 Archivos para la integración con Dorlet. Fuente. Edición Propia.

Anexo C – Etapa 3: Diseño e Implementación

Creación del proyecto

Una vez instalada, configurada y licenciada la plataforma de integración, se procedió a crear la carpeta del proyecto, asignándole el nombre de “Planinvest”. Posteriormente, se copiaron las carpetas “Histo” y “Param” desde el proyecto “Default”, con la finalidad de iniciar correctamente la estructura base de configuración. Este procedimiento fue realizado debido a que es una recomendación directa del fabricante PRYSM para asegurar que el proyecto herede los parámetros iniciales necesarios y evitar errores durante la etapa de parametrización.

Creación de sinópticos

Empresa Planinvest

Se desarrollaron sinópticos por piso (1°, 2° y sótano), uno de la fachada y uno de contactos de emergencia, integrando botones de navegación entre los diferentes sinópticos creados para la empresa Planinvest (ver Fig. C1).

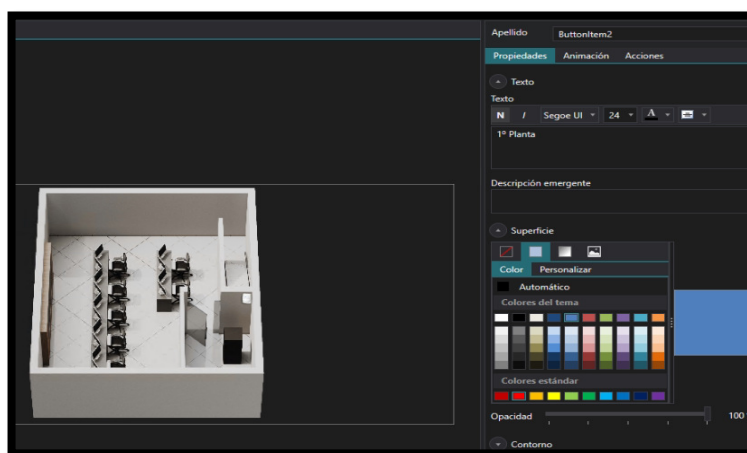


Figura C1 Creación de sinópticos y botones empresa Planinvest. Fuente. Edición Propia.

Empresa Martinizing Chacarilla

Se crearon sinópticos de planta y fachada para el local de Chacarilla, con sus respectivos botones de navegación (ver Fig. C2).



Figura C2 inóptico y botones. Fuente. Edición Propia.

Empresa Martinizing Espinar

Se desarrollaron sinópticos de planta y fachada para el local de Espinar, con botones de navegación (ver Fig. C3).



Figura C3 Sinóptico y botones para local Espinar. Fuente. Edición Propia.

Empresa FUCSA

Se creó un único sinóptico para el ambiente “Archivo” (ver Fig. C4).

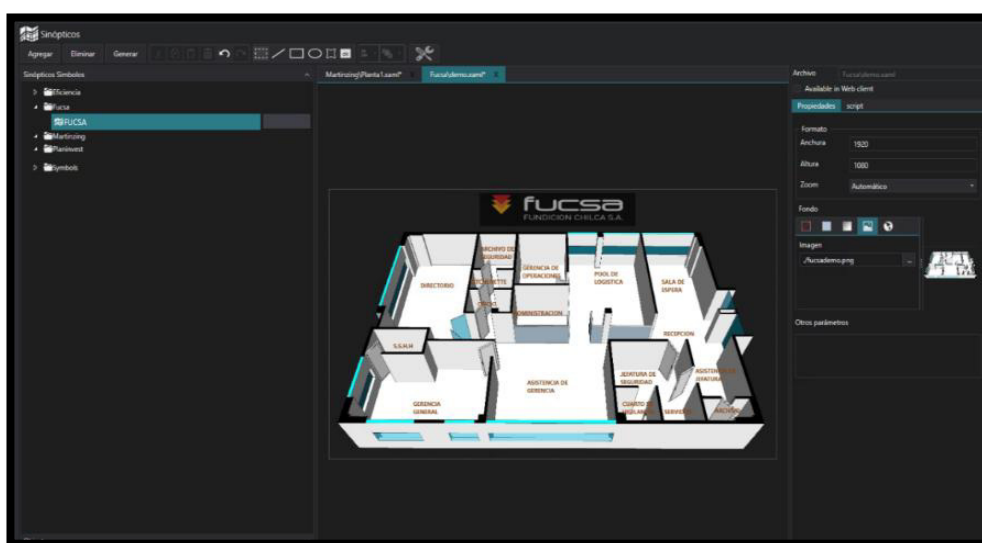


Figura C4 Creación de sinóptico y botones. Fuente. Edición Propia.

Sinóptico histórico de alarmas

Se implementó un sinóptico para acceso rápido al registro de alarmas y eventos (ver Fig. C5).

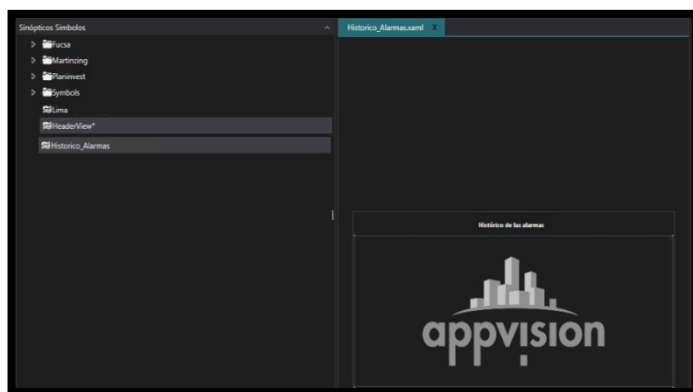


Figura C5 Creación de sinóptico “Histórico Alarmas”. Fuente. Edición Propia.

Sinóptico principal y ubicación geográfica

Se generó un mapa principal con OpenStreetMap para ubicar todos los locales con coordenadas geográficas. Incluye programación de animaciones (estado normal en azul y en alarma parpadeo rojo) y enlaces directos a sinópticos o videos según corresponda (ver Fig. C6).

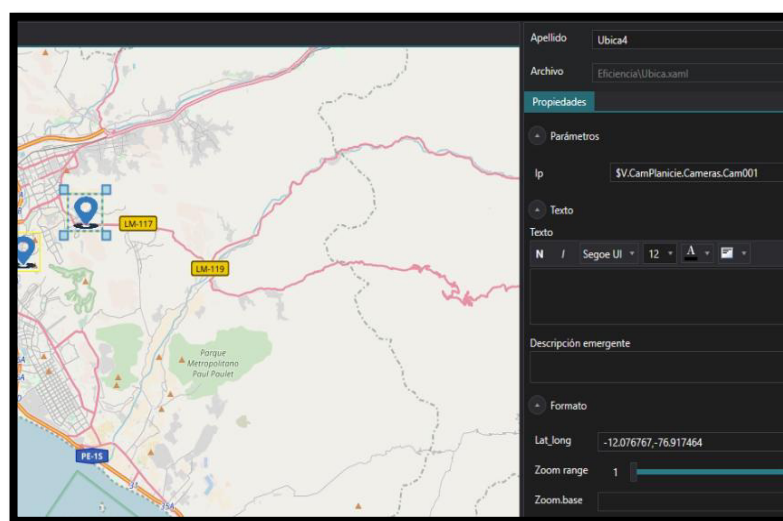


Figura C6 Ubicación geográfica de símbolo. Fuente. Edición Propia.

Sinóptico HeaderView

Cabecera fija en la interfaz, con logo, botones de navegación, generador de alarmas y visor de histórico. Incluye visor de usuario en línea y hora actual (ver Fig. C7).

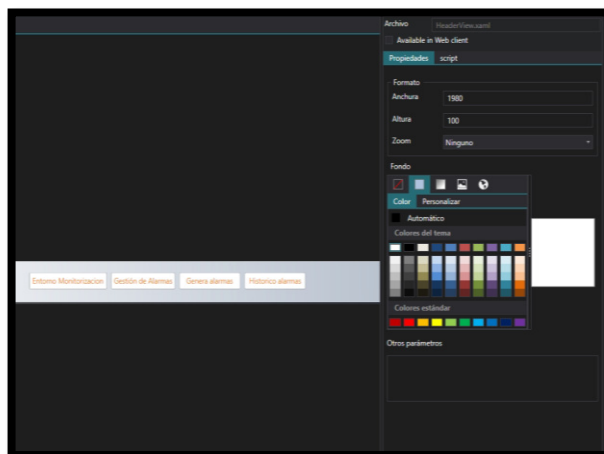


Figura C7 Creación de botones en sinóptico “HeaderView”. Fuente. Edición Propia.

Creación de símbolos

CCTV

Símbolo de cámara con menú contextual para visualización de video (ver Fig. C8).

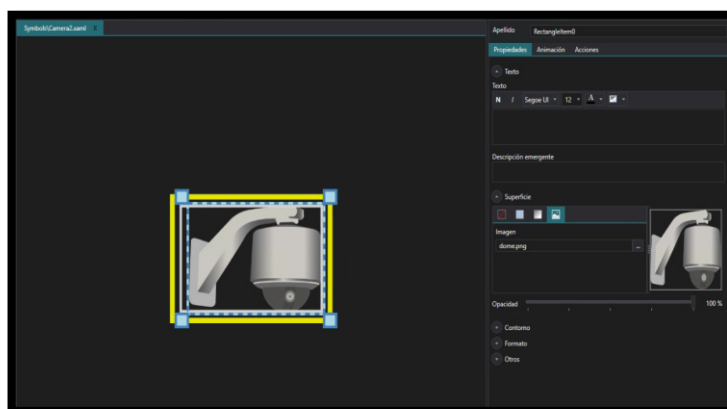


Figura C8 Creación de símbolo de CCTV en AppVision. Fuente. Edición Propia.

Intrusión

Símbolos de sensor PIR, sensor magnético y pulsador de emergencia, con animaciones para estados de alarma y reposo (ver Fig. C9 y C10).

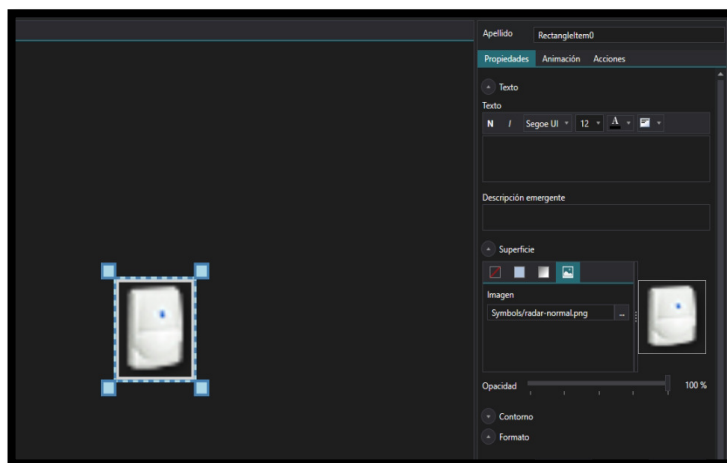


Figura C9 Creación de símbolo de PIR en AppVision. Fuente. Edición Propia.

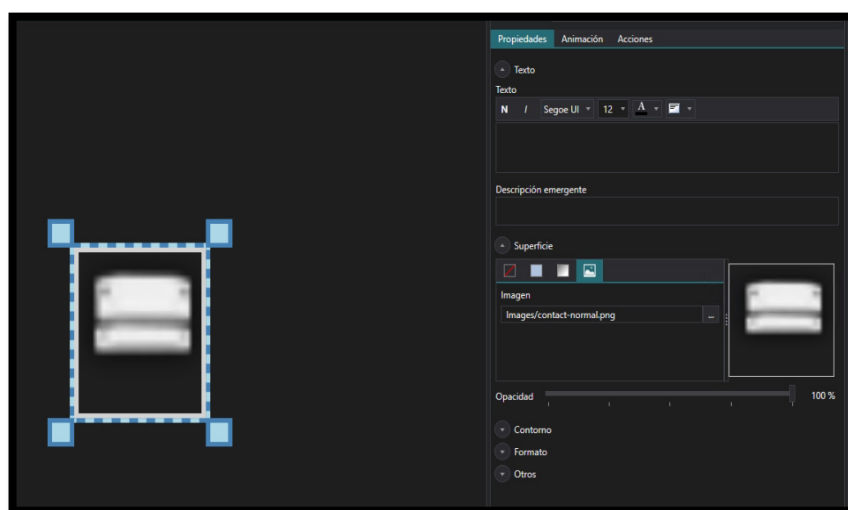


Figura C10 Creación de símbolo del sensor magnético Bosch en AppVision. Fuente. Edición Propia.

Control de acceso

Símbolo para lector Dorlet con animaciones y menú de acciones (ver Fig. C11).

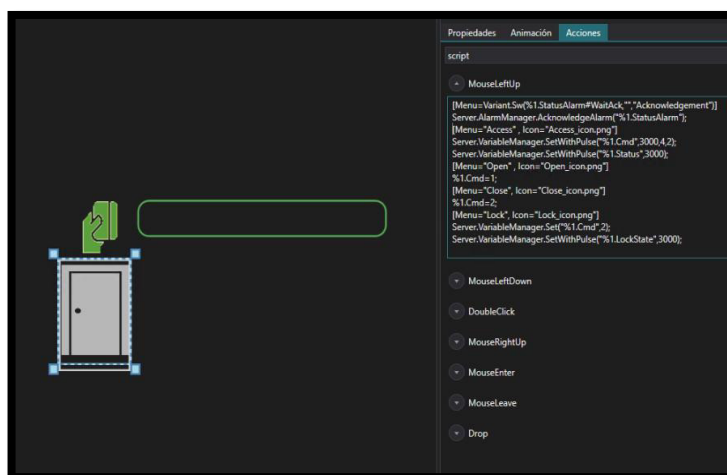


Figura C11 Programación de acciones del símbolo control de acceso Dorlet en AppVision. Fuente. Edición Propia.

Detección de incendios

Símbolo con animaciones típicas del sistema (ver Fig. C12).

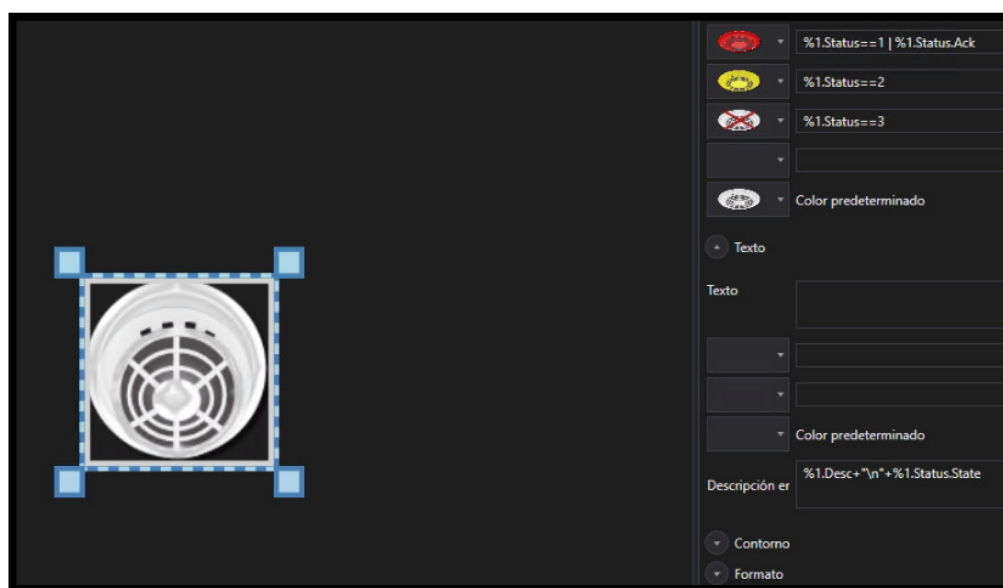


Figura C12 Programación de animaciones del sistema de detección de incendios en AppVision. Fuente. Edición Propia.

Creación de protocolos

Se configuraron protocolos para Hikvision, Dorlet, CamDasso, CamPlanicie, CamFucsa y Bosch (ver Fig. C13).

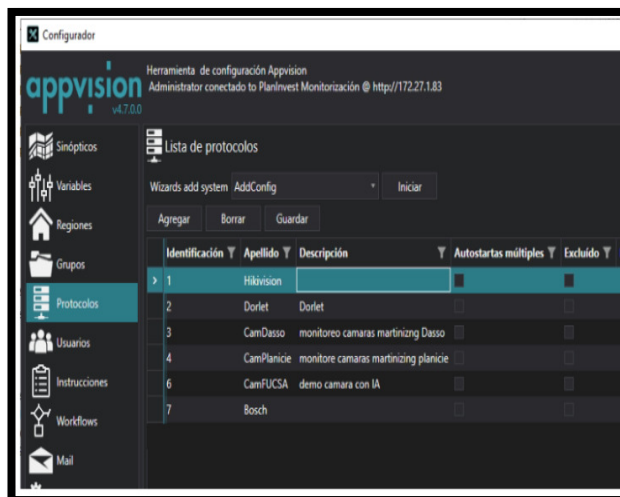


Figura C13 Listado de protocolos creados para la integración. Fuente. Edición Propia.

Creación de variables, asignación de símbolos y protocolos

Empresa Planinvest

CCTV: 1 grabador de 16 canales (ver Fig. C14).

Control de acceso: 1 controladora con 1 puerta activa (ver Fig. C15).

Incendios: 5 detectores simulados (ver Fig. C16).

Identificación	Apellido	Descripción	Tipo	Area	Sinóp
1006	NVR1.Cam001	Cam01	Nódulo	Sanlsidro/Edificio_Planinvest	Fucsa
1014	NVR1.Cam002	Cam02	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1021	NVR1.Cam003	Cam03	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1028	NVR1.Cam004	Cam04	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1035	NVR1.Cam005	Cam05	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1042	NVR1.Cam006	Cam06	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1049	NVR1.Cam007	Cam07	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1056	NVR1.Cam008	Cam08	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1063	NVR1.Cam009	Cam09	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1070	NVR1.Cam010	Cam10	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1077	NVR1.Cam011	Cam11	Nódulo	Sanlsidro/Edificio_Planinvest	Planin
1084	NVR1.Cam012	Cam12	Nódulo	Sanlsidro/Edificio_Planinvest	Planin

Figura C14 Variables para integrar grabador de 16 canales de Hikvision. Fuente. Edición Propia.

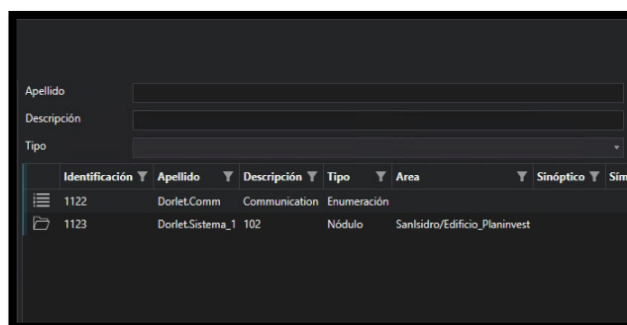


Figura C15 Variables para integrar servidor de control de acceso con una controladora Dorlet. Fuente. Edición Propia.

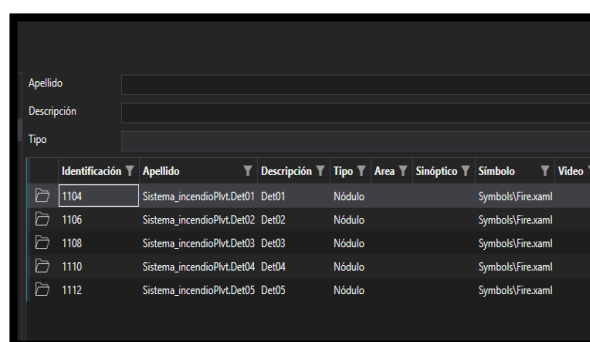


Figura C16 Asignación de símbolo variables sistema de incendio. Fuente. Edición Propia.

Empresa Martinizing

CCTV: 6 grabadores (ver Fig. C17).

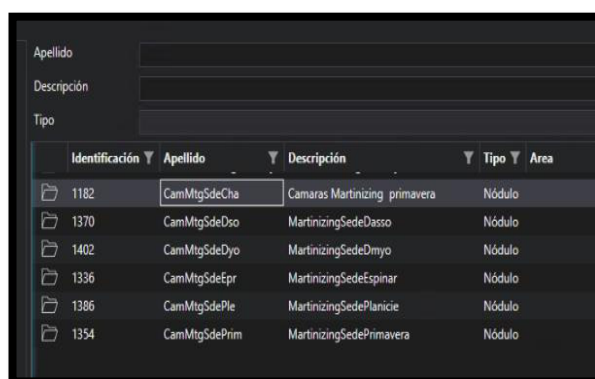


Figura C17 Asignación de símbolo y protocolo para integrar Dahua. Fuente. Edición Propia.

Empresa FUCSA

CCTV: 1 grabador (ver Fig. C18).

Apellido

Descripción

Tipo

	Identificación ▼	Apellido ▼	Descripción ▼	Tipo ▼	Area ▼	Sinóptico ▼	Símbolo
📁	1678	CamFUCSA.Cameras	Cameras	Nódulo			
☰	1700	CamFUCSA.Comm	Comm	Enumeración			
☰	1701	CamFUCSA.Event	Event	Enumeración			
📁	1702	CamFUCSA.ExternalAlarms	ExternalAlarms	Nódulo			
☰	1705	CamFUCSA.otro	analítica	Enumeración			
abc	1706	CamFUCSA.Trace	Trace	texto			

Figura C18 Asignación de símbolo y protocolo para integrar Dahua.
Fuente. Edición Propia.

Intrusión: Variables importadas de Prysm (ver Fig.C19).

Apellido

Descripción

Tipo

	Identificación ▼	Apellido ▼	Descripción ▼	Tipo ▼	Area ▼	Sinóptico ▼	Símbolo ▼
📁	1637	PA001.Area_001	Area_001	Nódulo			
📁	1644	PA001.Cmd	Cmd	Nódulo			
📁	1651	PA001.Output_001	Output_001	Nódulo			
📁	1646	PA001.Panel_Info	Panel_Info	Nódulo			

Figura C19 Asignación de símbolo y protocolo para integrar Bosch.
Fuente. Edición Propia.