ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

INTEGRACIÓN DEL SISTEMA CENTRALIZADO DE SEGURIDAD PARA EL EDIFICIO DE LA CORPORACIÓN GPF

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y CONTROL

QUIMUÑA LLUMIQUINGA PEDRO DIEGO
diegonk1975@gmail.com

DIRECTOR: ING. XAVIER SALAS
xavier.s@ec-mastertronic.com

CO-DIRECTOR: Dr. ANDRÉS ROSALES ACOSTA
androsaco@gmail.com

Quito, Abril 2016

DECLARACIÓN

Yo, Pedro Diego Quimuña Llumiquinga**,** declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Pedro Diego Quimuña Llumiquinga

CI: 1713754768

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Pedro Diego Quimuña Llumiquinga, bajo nuestra supervisión.

ING. XAVIER SALAS

DIRECTOR DEL PROYECTO

DR. ANDRÉS ROSALES

CO-DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a mis padres Elsa y Pedro, que gracias a su gran esfuerzo, consejos y sacrificio me permitieron alcanzar este objetivo planteado en mi vida el de ser un gran profesional y seguir superándome día a día.

A mis hermanos Roberto, Marco y Antonella que con sus consejos y apoyo supieron sembrar en mi la perseverancia, el sacrificio y sobre todo la humildad que nuestros padres nos inculcaron para ser hombres y mujeres de bien.

A mi esposa Norma y mi angelita Annie Scarlett, que con su apoyo me permiten seguir adelante en la culminación de este proyecto

Quiero agradecer a la Corporación GPF, lugar en el que sigo creciendo profesionalmente por haberme permitido realizar este proyecto en sus instalaciones. Finalmente agradezco al Ing. Xavier Salas que con sus conocimientos, consejos y ejemplos fue una guía para la culminación del proyecto.

Pedro Diego Quimuña Llumiquinga

DEDICATORIA

Dedico éste trabajo a mis padres, que con sus bendiciones y concejos siempre estuvieron junto a mí y me dieron la fuerza para superarme cada día más.

A mis hermanos que siempre están en los buenos y malos momentos, por su apoyo incondicional y sus ánimos de ser cada día mejor.

A mi esposa e hija, por las que seguiré luchando por su bienestar

A mis sobrin@s Kiki, Nayeli y Dillan que con sus sonrisas y ocurrencias animaron mi vida.

Pedro Diego Quimuña Llumiquinga

CONTENIDO

RESUMEN

La Corporación GPF cuenta con nuevas instalaciones ubicadas en el sector del Valle de los Chillos, las cuales utilizan tecnología de punta en lo referente a los sistemas de seguridad electrónica. Esto dado que, en la actualidad los sistemas de control de acceso, detección de incendios, circuito cerrado de televisión (CCTV) e intrusión, resultan de esencial importancia para proteger la infraestructura y garantizar la integridad física del personal.

En consecuencia, el objetivo del presente proyecto es integrar los sistemas de detección de Incendio, CCTV e intrusión al sistema de control de acceso utilizando la misma interfaz gráfica y el mismo sistema de navegación.

El sistema de control de acceso es administrado y monitoreado por el medio Software CCURE 9000. Con este software se crea un concentrador virtual de aplicaciones integradas de los sistemas de seguridad antes mencionados. Esto permite visualizar múltiples disposiciones y paneles de vigilancia en una misma estación.

En la actualidad es importante la integración de los sistemas de seguridad para crear un edificio con una infraestructura adecuada. El presente proyecto de titulación se desarrolla para proveer a los operadores de sistemas de seguridad un sistema centralizado, confortable y seguro.

PRESENTACIÓN

En este proyecto se implementa la integración de los sistemas de seguridad Electrónica ya existentes en la Corporación GPF. El sistema consta de la interacción de cuatro subsistemas: control de acceso, detección de incendios, circuito cerrado de televisión (CCTV) e intrusión. Este trabajo tiene como finalidad proveer a la Corporación GPF de un sistema de seguridad muy eficiente y utilizando sistemas y equipos de última tecnología.

Con este objetivo, este trabajo se ha dividido en cinco capítulos que se describen a continuación:

El primer capítulo presenta una introducción general de los conceptos básicos de los sistemas de seguridad electrónica, esquemas y características de los dispositivos que lo conforman.

El segundo capítulo consiste en la implementación de la integración de los sistemas de control de acceso, detección de incendio, circuito cerrado de televisión (CCTV) e intrusión. Presenta las principales conexiones de los dispositivos usados, para integrar estos sistemas a la red del establecimiento. Estos sistemas son de vital importancia para el control y seguridad del personal que conforman la Corporación GPF.

El tercer capítulo muestra las configuraciones necesarias de todos los equipos involucrados, tales como servidores, convertidores de comunicación serial a Ethernet, etc. Además, se presenta el software que integra los sistemas.

El cuarto capítulo reporta los resultados de las pruebas correspondientes al funcionamiento del sistema de integración. Es aquí donde se comprueba la operatividad del sistema.

Finalmente, en el capítulo cinco, se presentan las conclusiones y recomendaciones llegadas al terminar el presente proyecto.

CAPÍTULO 1

MARCO TEÓRICO

1.1 INTRODUCCION

La Corporación GPF, debido a su alto crecimiento con el negocio del retail farmacéutico traslado sus oficinas que se encuentran ubicadas en el centro histórico de Quito, a una edificación totalmente nueva y moderna ubicada en el sector del Valle de Los Chillos.

Conjuntamente con su crecimiento, el personal y sus departamentos también lo han hecho es por eso que sus instalaciones deben contar con un Sistema de Seguridad Electrónico muy eficiente el cual tiene como función principal el facilitar las actividades del personal y precautelar sus bienes muebles e inmuebles, previniéndolas de atracos, robos e incendios.

El edificio de la Corporación GPF, consta de las siguientes áreas:

- Subsuelo 2
- Subsuelo 1
- Planta baja
- Primer piso
- Outlet
- Comedor
- Casa Estudio
- Cancha
- Parqueaderos externos
- Sistemas Operativos

1.2 SISTEMAS DE SEGURIDAD ELECTRÓNICA.

Un sistema de seguridad electrónica es el conjunto de elementos y dispositivos electrónicos que interconectados nos permiten brindar seguridad a una área

determinada. En la actualidad los sistemas de seguridad electrónica son de vital importancia, ya que es el conjunto de acciones enfocadas a la protección, defensa y preservación de las personas y su entorno frente a amenazas externas que atentan contra su integridad. Un Sistema de Seguridad Electrónica debe tener las siguientes características:

- Proveer un ambiente seguro para personas, propiedades y datos.
- Ser Confiable.
- Ser fácil de usar y administrar.
- Ser escalable.
- Permitir Integración.
- Ser auditable.
- Permitir extraer pruebas irrefutables.

1.2.1 SISTEMA DE CONTROL DE ACCESO.

El sistema de control de acceso tiene por objeto impedir el libre acceso del público en general a diversas áreas. Las zonas más sensibles, como las oficinas de directivos, salas de reuniones o los archivos precisan una protección especial. Las necesidades de cada empresa precisan de configuraciones singulares, sobre todo ellas que tienen personal muy diferenciado como administrativo, limpieza y mantenimiento. [1]

Permite gestionar los niveles de accesos a los ocupantes del ambiente y a los visitantes. Según los requerimientos del cliente, también es posible gestionar los horarios de acceso y salida de los ocupantes.

1.2.1.1 Componentes del Sistema.

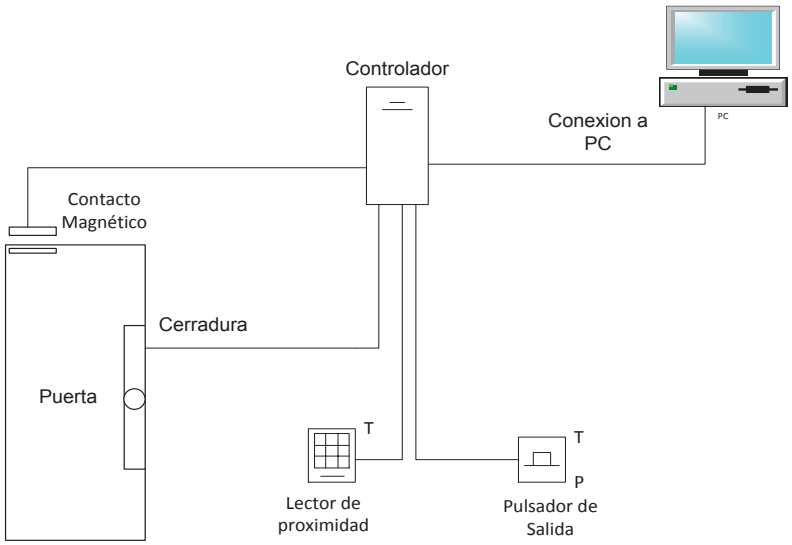


Figura 1. 1 Diagrama general de un sistema de control de accesos.

Los elementos comunes de un sistema de control de acceso son los siguientes Figura 1.1:

- Controlador: Concentra la información y toma las decisiones. Su función es comunicarse con el programa central que concentra toda la información del sistema en general, tanto la información de configuración como la de eventos producidos.

- Dispositivos de identificación: Son aquellos que tiene por objeto identificar a la persona que desea ganar el acceso. Existen diferentes tipos de dispositivos, algunos permiten el acceso más rápido, como las **tarjetas de proximidad** y otros identifican al sujeto con más precisión, como los **lectores biométricos**.

- Dispositivos de entradas: Estos dispositivos comunican al controlador el estado de las otras variables del sistema y le permiten tomar las decisiones con mayor precisión. Por ejemplo los contactos magnéticos **i**ndican si la puerta está abierta o cerrada y el pulsante de salida se utiliza para dar salida a través de la puerta.

- Dispositivos de salida: Son aquellos que ejecutan las acciones ordenadas por el controlador como las de liberar cerraduras, accionar barreras, liberar molinetes, accionar alarmas, etc. Por ejemplo la cerradura es un dispositivo eléctrico que el controlador activará utilizando una de sus salidas si se concede al titular el acceso.

- Red de comunicaciones: Es la red utilizada para que el controlador se comunique con otros controladores y/o con una o más estaciones centrales.

1.2.2 SISTEMA DE DETECCIÓN DE INCENDIOS.

En la actualidad los sistemas de detección de incendio son de vital importancia, Figura 1.2, puesto que alertan frente a incidentes que podrían originar un incendio o explosión y otorgan un aviso temprano y oportuno para poder activar los planes de contingencia, y así proteger a las personas y sus propiedades. Estos sistemas deben permitir:

- Supervisar los dispositivos instalados.
- Señalar el punto exacto de una alarma.
- Integrarse a otros sistemas de seguridad.
- Minimizar falsas alarmas.

Figura 1. 2 Esquema general del sistema de detección de incendios.

1.2.2.1 Componentes del Sistema.

Los componentes de un sistema de detección y alarma de incendios son los siguientes:

- Panel de Control: Es el cerebro del sistema que monitorea y supervisa las inputs o recepciones de información. Monitorea, supervisa y ordena a las outputs o salidas de información del sistema. Los Inputs están compuestos por los dispositivos de iniciación, mientras que los outputs están compuestos por los dispositivos de notificación y control.

- Dispositivos de Iniciación: Son los componentes del sistema que mediante medios manuales o automáticos informan al panel de control de un cambio de estado o condición anormal del sistema. Estos pueden ser: sensores de Humo, sensores de temperatura o estaciones manuales de Incendio.

- Dispositivos de Notificación: Son los componentes del sistema que proveen de medios audibles o visibles de alerta ante la detección de una condición anormal en la estructura a ser protegida. La condición anormal que será detectada dependerá de los dispositivos de iniciación instalados. Estos Pueden ser: luces estroboscópicas, sirenas campanas, luces Incandescentes.

- Dispositivos De Control: Son los dispositivos auxiliares que operarán automáticamente luego de que la condición anormal o cambio de estado de los dispositivos de iniciación. Estos pueden provocar: desactivación de ascensores, liberación de puertas de evacuación, activación de Sistemas de Presurización de Escaleras, activación de Sistemas de administración de humos, activación de sistemas de extinción de incendios.

1.2.3 SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN).

Los sistemas CCTV son una solución efectiva para prevenir y detectar actos delictivos. Estos sistemas permiten dar la alerta de forma instantánea frente a los

actos vandálicos asegurando que las agresiones a las personas como a los bienes se reduzcan sustancialmente. Este sistema debe permitir:

- Tener un registro de eventos, que permita grabar en tiempo real y por detección de movimiento los sucesos del día.
- Monitorear un área extensa con pocas personas y así hacer más segura la vigilancia del área a cubrir.
- Mejorar la efectividad de los empleados y de ésta manera disminuir las pausas en su trabajo.
- Revisar posteriormente las grabaciones y determinar cuáles fueron las razones o las personas culpables en algún incidente y tomar acciones para evitar fallas futuras.
- Encontrar objetos perdidos por accidente en la empresa con solo revisar grabaciones y ver qué pasó con dicho objeto.
- Funcionar como un elemento disuasorio y ayudar a localizar a los culpables.

Figura 1. 3 Esquema general sistema CCTV. [2]

1.2.3.1 Componentes del Sistema.

Los componentes básicos de un sistema de Circuito Cerrado de Televisión son:

Cámara: Las cámaras están conectadas a través de líneas de transmisión a los monitores de TV los cuales nos permiten visualizar y controlar las áreas vigiladas.

Una cámara IP son videocámaras especialmente diseñadas para enviar las señales a través de internet desde un explorador o a través de una red local LAN.
Cableado estructurado: Sistema de cables, conectores y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio. Dependiendo de la categoría de una red, su velocidad varía considerablemente.

Monitor: Los monitores son los dispositivos por los que se muestra la imagen captada por las cámaras. Los mismos que deben ser robustos ya que la mayoría de ellos deben estar trabajando las 24 horas del día.

Grabador (NVR): Es la red troncal de un sistema de seguridad por video con base IP. Utiliza comunicación TCP/IP para tener acceso al hardware conectado en red y controlarlo. Administra la cámara de video, el almacenamiento y los recursos de sensor de su sitio.

1.2.4 SISTEMA DE INTRUSIÓN.

Un sistema de intrusión es el conjunto de dispositivos que aseguran el conocimiento previo de una presencia en un recinto no permitido, y que hace posible una adecuada intervención para lograr la frustración de un delito.

El objetivo del sistema de intrusión es detectar y avisar por medio de señales de alarma a los operadores.

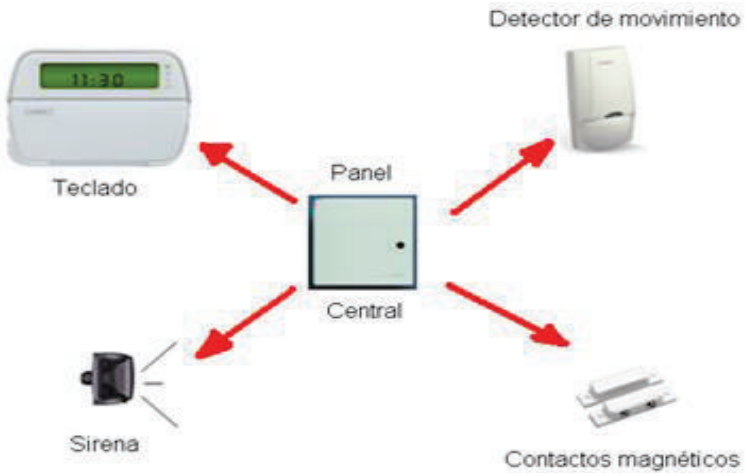


Figura 1. 4 Esquema general del sistema de intrusión.

1.2.4.1 Componentes del Sistema.

El sistema de detección de intrusión recoge y procesa las señales de los detectores conectados, y activa los indicadores y señales de alarma necesarias para el funcionamiento y la intervención. Está compuesto de las siguientes partes:

- Central: Es el corazón del sistema. Recibe y manda información a los detectores a través del bus. Con dicha información puede activar sobre dispositivos de alarma. Se encuentra en el interior de un armario anti-sabotaje para protegerla de posibles agresiones o manipulaciones. Esta central se compone de las siguientes unidades: Alimentación, conexiones para las líneas de detección, microprocesador o sistema de procesamiento similar, salidas para alarma, transmisión a distancia, interfaces para la activación, comunicación.

- Detectores: Son dispositivos que detectan el movimiento de las personas basándose en distintos principios de funcionamiento, ellos envían información a la central a través del bus de detección.

- Equipos de señalización y mando: Las centrales de intrusión a menudo suelen tener los paneles de señalización y mando integrados. Sin embargo, en la mayoría de los casos, el panel de señalización y mando se instalan separados de la central. Por ejemplo si se usa teclados sus funciones son: conmutar el sistema o partes del mismo, reconocimiento y armado de alarmas, probar los dispositivos de alarma y detectores, señalización de los modos de funcionamiento y los sucesos.

- Dispositivos de alarma: Se puede tener alarmas internas y externas. Alarma interna: Su misión es informar y avisar a personas presentes en edificio y disuadir y alertar al servicio de vigilancia. Alarma externa: La finalidad de su instalación es avisar e informar a las cercanías del edificio y disuadir a intrusos.

1.2.5 BENEFICIOS.

Un Sistema de Seguridad Electrónica para ser eficiente debe brindar los siguientes beneficios:

- Mayor seguridad al restringir circulación de personas a sectores no autorizados.
- Registro automático de actividades sospechosas.
- Vigilancia no atendida de áreas críticas.
- Control y supervisión remota de procesos.

1.3 SISTEMA CENTRALIZADO DE SEGURIDAD ELECTRÓNICA.

Un sistema centralizado tiene la capacidad de controlar de manera integrada e inteligente todos los sistemas del edificio por razones de gestión seguridad y ahorro. Estos sistemas permiten garantizar una gestión de la seguridad mucho más integral y coordinada. [3]

1.3.1 TECNOLOGIA IP.

IP es la sigla de Internet Protocol o Protocolo de Internet. Trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.

Las direcciones IP hacen referencia al equipo de origen y llegada en una comunicación a través del protocolo de Internet. Los conmutadores de paquetes (conocidos como switches) y los enrutadores (routers) utilizan las direcciones IP para determinar qué tramo de red usarán para reenviar los datos.

La dirección IP está compuesta por un número que permite identificar jerárquica y lógicamente la interfaz de una computadora u otra máquina que se encuentra conectada a una red y que emplea el protocolo de Internet. [4]

1.3.2 INTEGRACIÓN DE SISTEMAS DE SEGURIDAD.

La Integración de Sistemas permite el control centralizado de todos los sistemas de seguridad, domótica y explotación, mejorando su eficacia y coordinación y optimizando los costes y recursos necesarios. Un Sistema de Seguridad Integral se compone de módulos de subsistemas que responden a las diferentes funciones de seguridad requeridas, pudiendo centralizar subsistemas tales como:

CCTV, control de accesos, sistema anti-intrusión, detección y extinción de incendios, megafonía e interfonía, alarmas técnicas, etc. [5]

Ventajas que ofrece la integración de sistemas:

- Reducción de los tiempos de respuesta ante una emergencia.
- Simplificación de uso y mantenimiento, manejable incluso para personal no especializado.
- Reducción de costes.
- Flexible, adaptable y ampliable.
- Alta fiabilidad e inmunidad frente a pérdidas de información.

La figura 1.5 muestra la integración de cuatro sub sistemas de seguridad que se comunican por medio de el protocolo de comunicación TCP/IP y visualizan bajo la gestión de un software unificado, con el cual se realiza el monitoreo en tiempo real de todos los sistemas de seguridad electrónica de forma centralizada. [6]

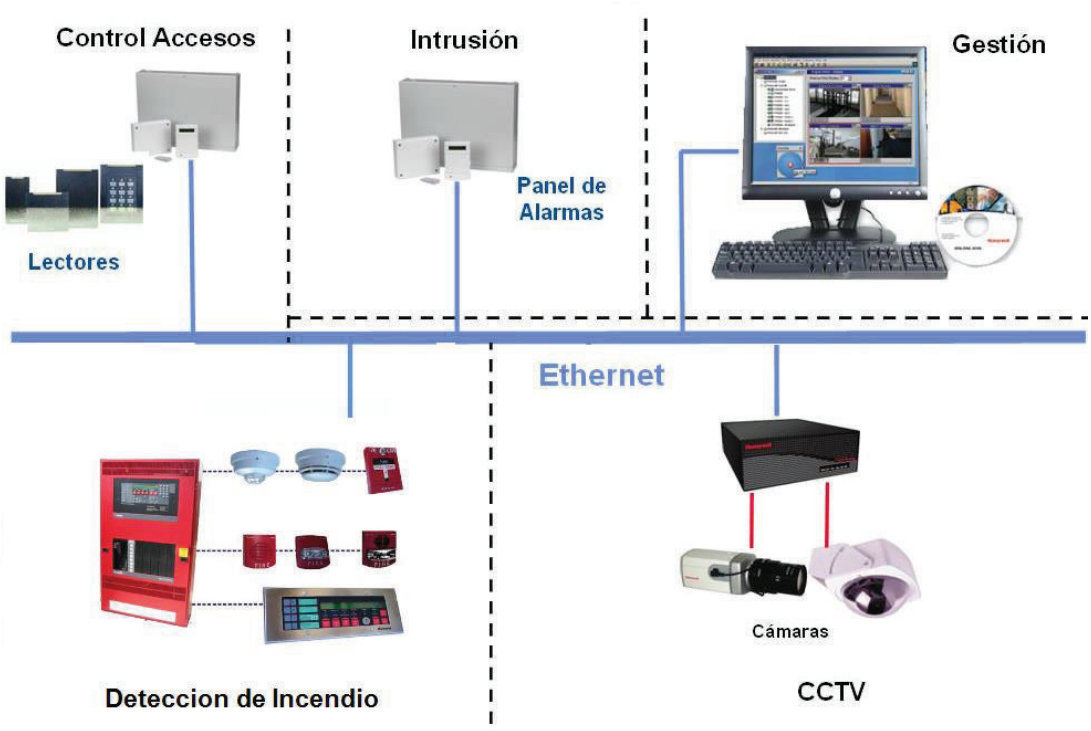


Figura 1.5 Integración de sistemas de seguridad electrónica.

1.4 APLICACIÓN A LA CORPORACIÓN GPF.

El edificio administrativo de la corporación GPF, que actualmente se encuentra en funcionamiento se ha proyectado convertirse en un edificio inteligente. Por lo que es de vital importancia la seguridad del mismo, el sistema de control de accesos estará dirigido por una unidad computarizada central, la cual tendrá un software especialmente diseñado para controlar a más de 100 lectoras de tarjetas y más de 300 puntos de alarmas (pulsadores, contactos magnéticos, etc..), dependiendo de la licencia que adquiera la corporación.

El Sistema de control de accesos para el edificio de la Corporación GPF estará integrado por elementos que brinden alta seguridad de ingreso, tanto por puertas principales como por puertas alternas a diferentes áreas. Con la integración con los demás sistemas de seguridad se ofrece al operador de consola mayor dominio y eficiencia con estos sistemas.

El software de control de acceso que se utiliza es CCURE 9000 (SOFTWARE HOUSE), con lo que se obtiene un sistema completo conectando cada cable de bajada a un puerto de comunicación, módem o servidor del terminal Ethernet.

El circuito cerrado de televisión (CCTV) es una tecnología de video vigilancia diseñada para supervisar una diversidad de ambientes y actividades. Este es un circuito en el que todos sus componentes se encuentran entrelazados en el que incluyen visión nocturna y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras

CAPÍTULO 2

IMPLEMENTACIÓN DEL SISTEMA DE INTEGRACIÓN

El sistema de seguridad de la corporación GPF consta de cuatro sub sistemas que son: control de accesos, detección de incendios, CCTV e intrusión. Estos sistemas están implementados en todas las áreas, como son: subsuelo 2, subsuelo 1, parqueaderos internos, cuarto de seguridad, planta baja lado A y lado B, recepción, primer piso lado A y lado B, outlet, comedor, casa estudio, cancha y parqueaderos. Figura 2.1 y 2.2.

Figura 2.1 Edificio Corporativo (subsuelo 1 y 2, planta baja y primer piso).

Figura 2.2 Edificios exteriores (Outlet, archivo, comedor).

En este capítulo se muestra el hardware necesario para integrar los sistemas de seguridad en un solo software gestor de eventos. Para lo cual es necesario que los sistemas que funcionan independientemente se comuniquen a través del protocolo TCP/IP. Figura 2.3.

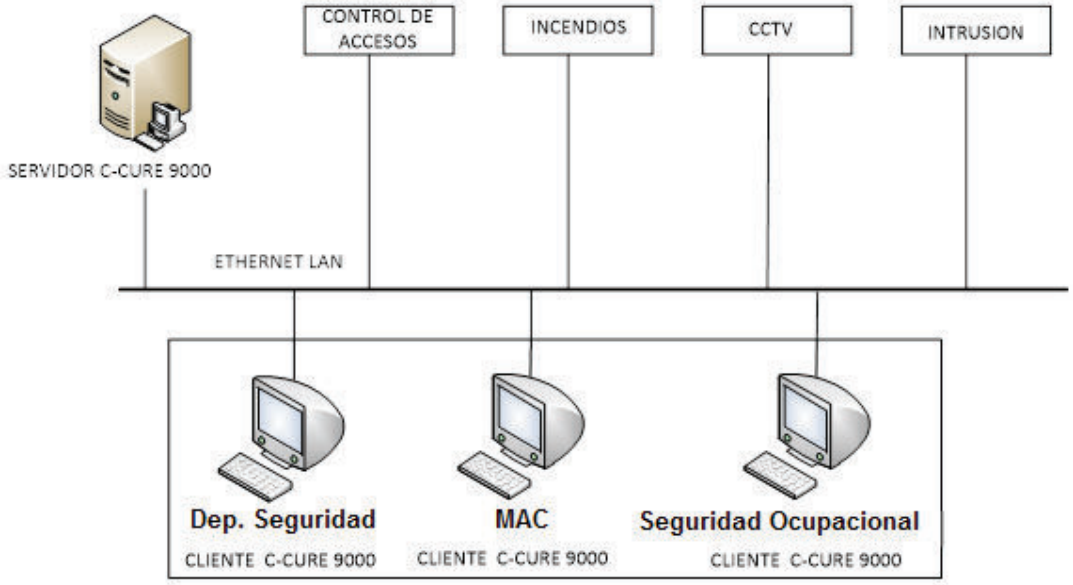


Figura 2.3 Integración de Sistemas de seguridad a la plataforma C-CURE 9000.

2.1 CONTROL DE ACCESO

El sistema de control de accesos del edificio administrativo está basado en una arquitectura distribuida de lectores y controladores de acceso que combinan las técnicas de comunicaciones modernas. Posee un computador central conectado a la red de datos con el software propio del fabricante que servirá para la programación, administración y registro de todos los eventos del sistema de accesos y alarmas.

El sistema está formado principalmente por un servidor, clientes y controladores istar edge. El servidor se encuentra instalado en el cuarto eléctrico de primer piso lado A, los clientes se sitúan en el departamento de seguridad, MAC y seguridad ocupacional, en tanto los controladores están distribuidos en todos los cuartos eléctricos.

Adicional se utiliza la plataforma de control de accesos CCURE 9000 para la programación, administración y monitoreo del sistema. Figura 2.4.

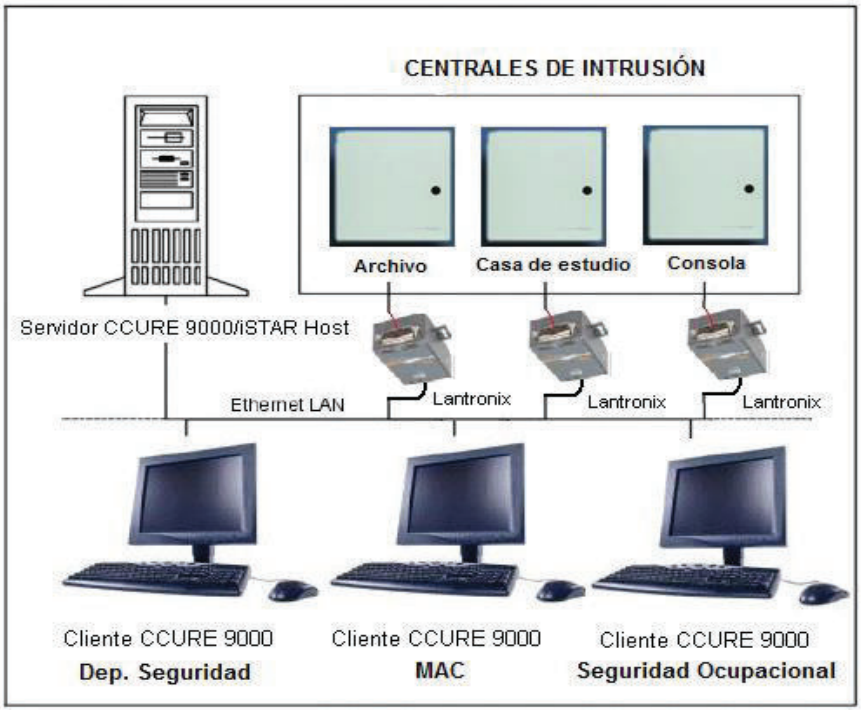


Figura 2.4 Sistema Control de Accesos.

2.1.1 DISPOSITIVOS DEL SISTEMA.

2.1.1.1 Controladora Istar Edge.

Es una controladora de puertas, que se presenta como un dispositivo IP para lectoras (2 o 4 lectoras). Las controladoras Istar Edge poseen entradas y salidas donde se conectan los contactos magnéticos, pulsadores de salida y cerraduras. Además las lectoras se enlazan a los pines disponibles en el controlador o a su vez en las tarjetas RM ubicadas en la puerta. Figura 2.5.

Figura 2.5 Controladora Istar Edge.

En la tabla 2.1 se describe las características de la controladora Istar Edge.

Tabla 2.1 Especificaciones Controladora Istar Edge.

Fuentes de Alimentación	
Requisitos de alimentación	12/24 Vcc, con detección Automática.
Solo placa	400 mA, max. 3.8 A a 12 Vcc, 3.1 A, a 24 Vcc, para la placa mas todos los dispositivos que se conecten.
Respaldo de memoria y reloj	Cuatro pilas AA, ofrecen respaldo automático para la base de datos en la memoria flash.
Memoria del Sistema	64 MB de RAM, 128 MB de Flash EEPROM.
Comunicaciones por Red	Puerto Ethernet tipo 10/100base-T
Tecnología de lectoras admitidas	Proximity, smart card, wiegand.
Corriente disponible para los lectores	12 Vcc, 1.5 A en total (Incluida la potencia auxiliar y para puerto RM).
Comunicaciones por bus RM	Tres puerto RS 485 semiduplex de dos hilos, más dos hilos opcionales para alimentar el dispositivo.
Corriente auxiliar disponibles para las entradas	12 Vcc, dos (cada una de 350mA).
Potencia de salida (con tensión)	12 V o 24 Vcc, 0.75 A (Istar Edge tiene su propia toma de corriente, la tensión de salida es igual que la entrada)
Protección de las tomas, en cada una	Fusible PTC re- armable, 0.75A, supresor de picos de tensión

La controladora Istar Edge requiere alimentación de 12 Voltios, el esquema se muestra en la figura 2.6.

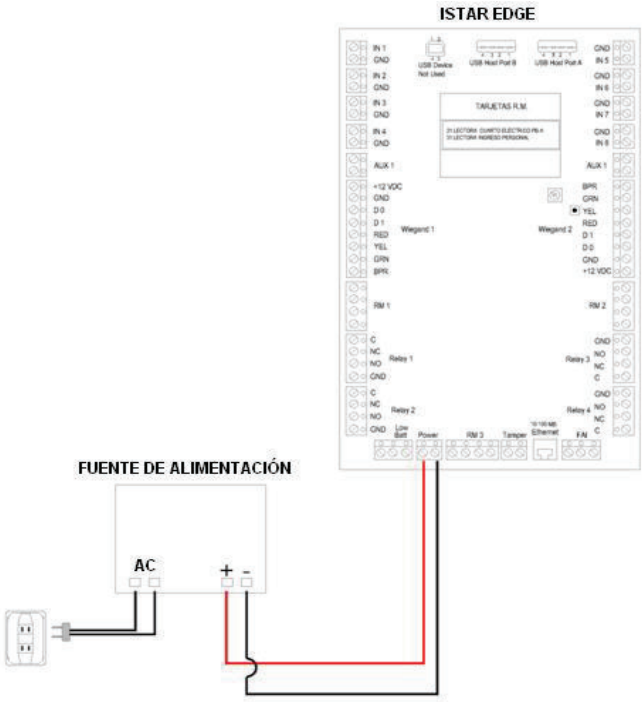


Figura 2.6 Esquema de alimentación de la controladora iSTAR Edge.

2.1.1.2 Lectoras.

La función de una lectora es leer la información almacenada en una tarjeta, una vez que el sistema identifica el titular de la misma, el controlador decide si la persona está autorizada o no a ingresar en un área específica. Esta validación puede estar basada en autoridad, horarios o la combinación de ambas. Figura 2.7.

Figura 2.7 Lectora HID utilizada en el Edificio Corporativo.

Los lectores de proximidad HID instalados, tienen un rango de lectura de 5 a 10 cm, totalmente a prueba de agua y sus formatos de salida son de 26 bits. Las lectoras se conectan al grupo de bornes correspondientes a wiegand 1 y wiegand 2 o a las tarjetas RM colocadas en la puerta del tablero de la controladora iSTAR. Ver conexión en Figura 2.8.

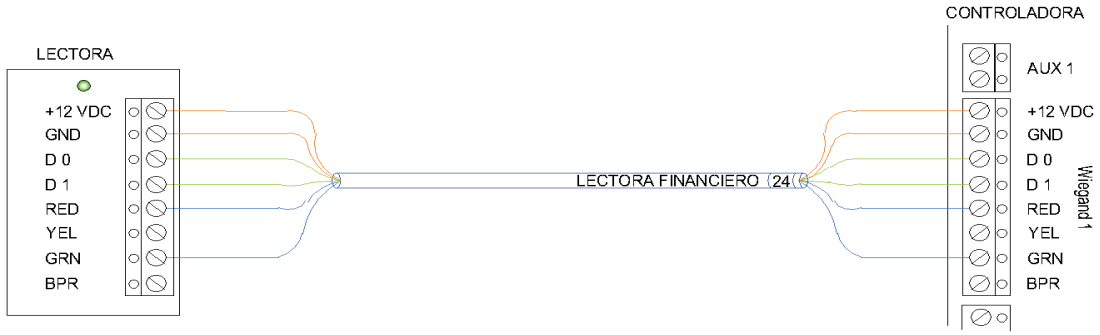


Figura 2.8 Conexión LECTORA HID.

2.1.1.3 Protocolo Wiegand. [7]

El protocolo Wiegand es una forma de comunicación que fue definida e introducida al mercado por la empresa HID®, hace ya más de 15 años, es esencialmente unidireccional y permite el traspaso de datos entre una lectora y una controladora

El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes de lectores por que permite la transmisión de información a través de un par de cobre acompañado por la alimentación para el dispositivo de lectura sin afectar por ello a los datos.

Como todo protocolo de comunicaciones, Wiegand consta de dos partes fundamentales: una parte describe el modo en que físicamente se transmite la información digital y la otra parte la forma de interpretar numéricamente dicha información.

Sistema de transmisión:

La transmisión de datos Wiegand usa tres hilos. La línea para enviar los unos lógicos o DATA 1, la línea para hacer lo propio con los ceros lógicos o DATA 0 y la línea de masa de referencia de ambos o GND. Los niveles que se usan son Bajo, a nivel GND, o Alto a +5V o VCC. En estado de reposo, o sea sin transmitir, la línea de GND es exactamente lo que es GND y siempre está en nivel bajo y las líneas DATA 1 y DATA 0 están en nivel alto, a nivel de +5V o VCC.

Para transmitir un Bit 1 se envía un pulso a Bajo, normalmente de 50 µseg (microsegundos) por la línea DATA 0, mientras ahora es DATA 1 la que permanece en Alto. Figura 2.9

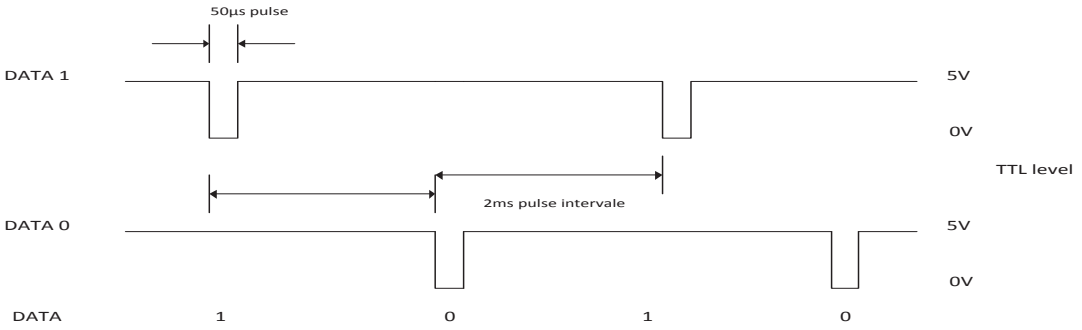


Figura 2.9 Transmisión de bits.

Interpretación de los Datos:

El código Wiegand 26 está compuesto por 26 bits y la interpretación del mismo es la siguiente:

- El primer Bit, B0, es la Paridad Par de los primeros 12 bits transmitidos (B1:12)
- Los 8 siguientes, B1:B8 son un Byte, un entero de 8 bits, al que llaman Facility Code y representa un número que va desde 0 hasta 255
- Los 16 siguientes: B9:B24 son dos Bytes, un entero de 16 bits, al que llaman User Code, que pueden valer entre 0 y 65535
- El ultimo bit, B25, es la paridad impar de los últimos 12 bits transmitidos (B13:24)

2.1.1.4 Pulsante de salida.

El pulsante sirve para dar salida a través de la puerta. En algunas puertas (Cuartos eléctricos y Consola de seguridad), solo se requiere el pulsante de salida y un lector de tarjetas en el exterior. Figura 2.10.

Figura 2. 10 Pulsantes de salida.

2.1.1.5 Contactos Magnéticos.

Los contactos magnéticos constan de dos piezas colocadas una en el marco de la puerta y otra en la hoja de apertura. Su funcionamiento se basa en unas laminillas finas que por la acción de la atracción del campo magnético formado por un imán, cierran el circuito. Al abrir la puerta, separa el imán de las láminas y estas, al separarse, abren el circuito produciendo la señal eléctrica que indicará si la puerta fue abierta. Figura 2.11.

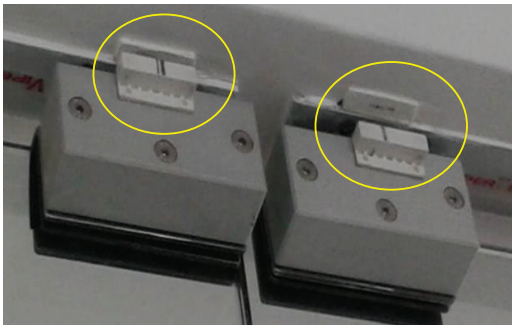


Figura 2. 91 Contactos magnéticos.

Los contactos magnéticos van conectados a los Inputs o entradas del iSTAR Edge. Figura 2.12.

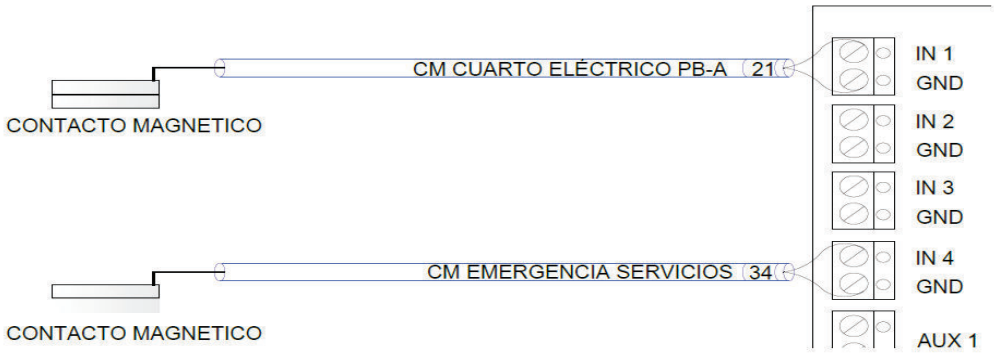


Figura 2.102 Conexión Contacto Magnético en el iSTAR Edge.

2.1.1.6 Cerraduras y Picaportes.

Las cerraduras y los picaportes son dispositivos que el controlador activará utilizando una de sus salidas si se concede al titular el acceso.

Una cerradura electromagnética se compone de dos partes: una placa hecha por un material magnético y una placa metálica rodeada por una bobina. Cuando corriente eléctrica es pasada por la bobina, la placa metálica es magnetizada y atrae fuertemente a la placa del material magnético cerrando así la puerta. Figura 2.13.

Figura 2.113 Cerradura (Cuartos Eléctricos).

El picaporte eléctrico consiste en dos piezas: una pieza que contiene un perno el cual se extiende o se contrae (se instala en el marco de la puerta) y un recibidor

de este perno (se instala en la puerta). Cuando el perno se extiende entra en el recibidor impidiendo así que la puerta se pueda abrir. Figura 2.14.

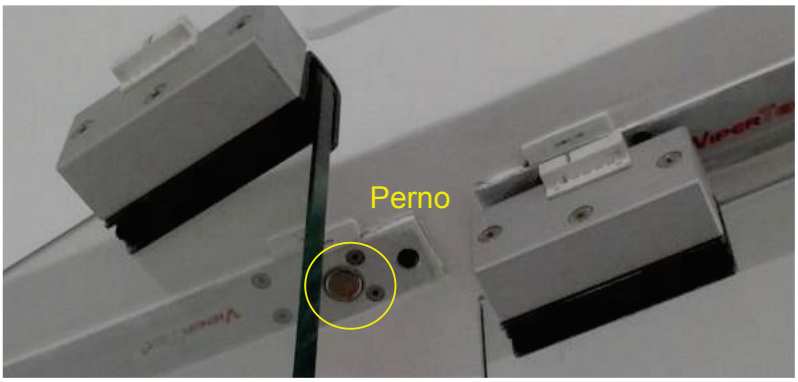


Figura 2. 124 Picaporte (Oficinas).

La conexión de la cerradura a la controladora se muestra en la Figura 2.15

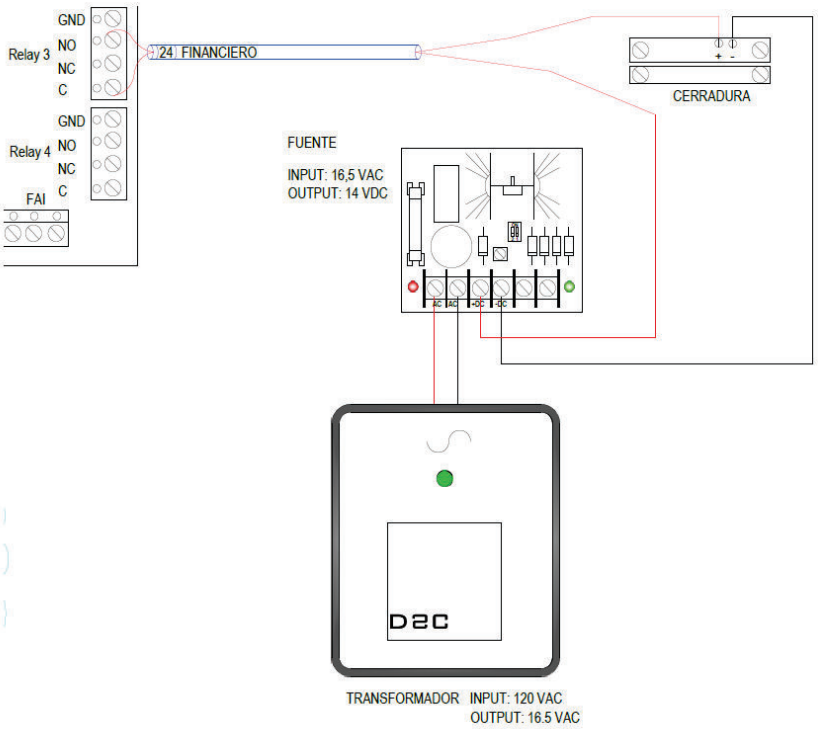


Figura 2. 13 Conexión de cerraduras o picaportes al relé del iSTAR Edge.

2.1.1.7 Tarjeta de proximidad HID.

Tarjeta de proximidad es el nombre genérico dado a la tarjeta inteligente “sin contacto” que se utiliza para el acceso seguro. La tarjeta de proximidad funciona

entre 5 y 10 cm. Cuentan con una salida wiegand 26 y usa la Interfaz 26/Ethernet, la cual se encarga de transmitir los datos que entrega el lector a una PC mediante Ethernet. De esta manera los datos provistos por el lector serán visualizados en la PC.

Figura 2. 14 Tarjeta HID.

En resumen, la figura 2.17 muestra el esquema general del sistema.

Figura 2. 157 Esquema general del sistema de control de accesos.

2.1.2 UBICACIÓN DE LAS CONTROLADORAS EN LOS CUARTOS ELÉCTRICOS.

El Edificio de la Corporación GPF dispone de dos ductos verticales, que sirven de medio de transporte del cableado, uno al lado sur denominado **DE_A** y uno al lado norte denominado **DE_B**. Además existe un ducto vertical **DE-S2** que interconecta Subsuelo 2 con Subsuelo 1. Figura 2.18.

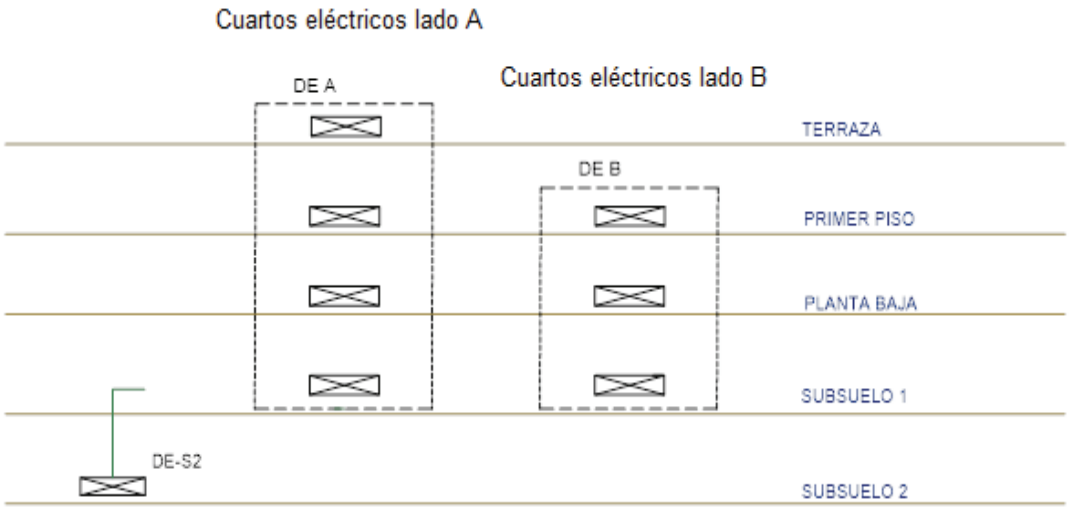


Figura 2.168 Ductos eléctricos del edificio principal.

La tabla 2.2 muestra la ubicación de las controladoras en los cuartos eléctricos.

Tabla 2. 2 Tableros de control de acceso ubicados en los cuartos eléctricos.

Cuarto Eléctrico A	Cuarto Eléctrico B	Ubicación
P1-A-01	P1-B-01, P1-B-02	Primer piso.
PB-A-01, PB-A-02, PB-A-03	PB-B-01, PB-B-02	Planta baja.
SUB-1-01, SUB-1-02, SUB-1-03	LIBRE.	Subsuelo 1.
SUB-02-01		Subsuelo 2, Bodega MAC

La figura 2.19 ilustra la posición de las controladoras en los cuartos eléctricos.

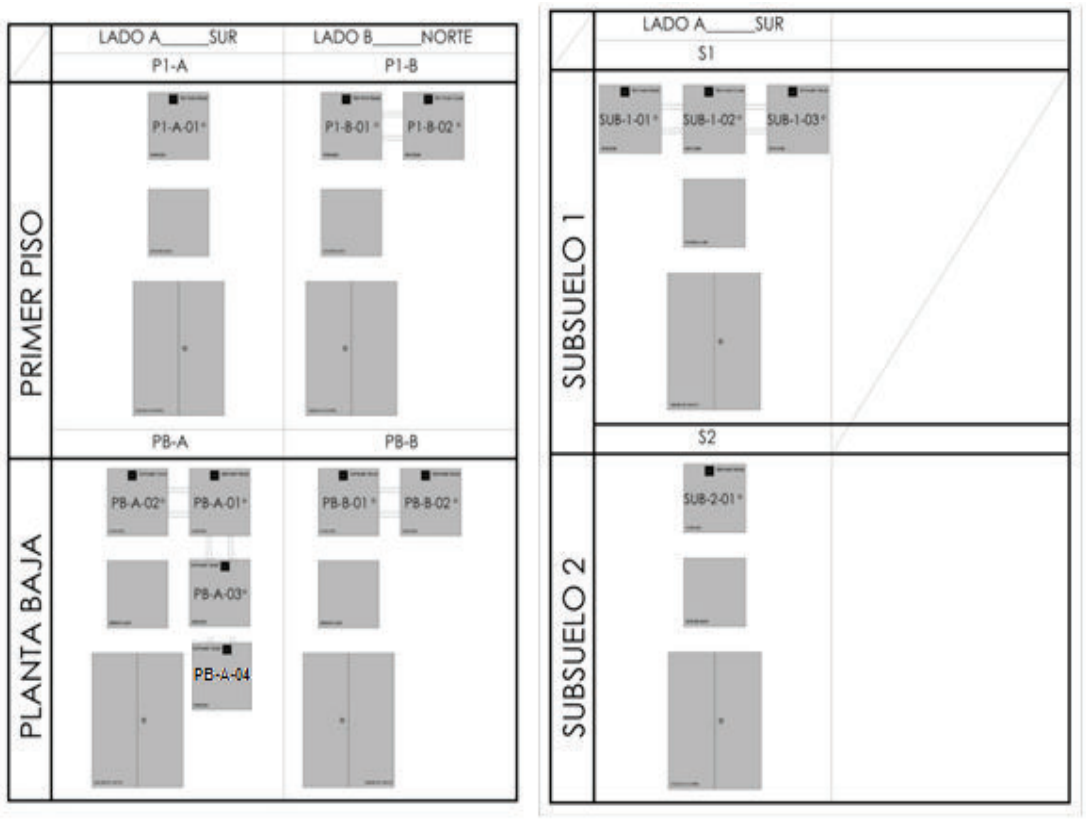


Figura 2.17 Ubicación de tableros en los cuartos eléctricos.

Cada controladora permite habilitar y deshabilitar las puertas. En la tabla 2.3 se observa las puertas correspondientes a las plantas de primer piso y planta baja. En la tabla 2.4 las de subsuelos.

Tabla 2.3 Puertas correspondientes a tableros de primer piso y planta baja.

	Ubicación	Puerta #
P1-A-01	Cuarto eléctrico piso 1A	43
	Gerencia General	35
	Fybeca/Sana Sana	42
P1-B-01	Auditoría interna/manejo de riesgos	39
	Cuarto eléctrico piso 1B	38
	Asesoría Legal-Abi-OKI-DOKI	36
	Responsabilidad corporativa	37
P1-B-02	Desarrollo organizacional	41
	Planeación y finanzas	40
PB-A-01	Cuarto eléctrico planta baja A	21
	Financiero	24

PB-A-02	Gerencia de servicios	17
PB-A-03	Ingreso GS-MAC-TEC	19
	MAC	16
	Tecnología	18
	Terraza PB	23
PB-B-01	Cuarto eléctrico planta baja B	25
PB-B-02	Oficinas Marketing	26
	Selección de Personal	20
	Servicios al personal	22
	Marketing	27

Tabla 2. 4 Puertas correspondientes a tableros de subsuelo 1 y 2.

	Ubicación	Puerta #
SUB-1-01	Consola de seguridad	5
	Contabilidad-nomina-archivo	3
	Cuarto eléctrico subsuelo 1 A	2
	Seguridad	4
SUB-1-02	Bodega UPS	8
	Concentrador de fibra óptica	9
	Contac center	10
	Tableros eléctricos	7
SUB-1-03	Parqueaderos ejecutivos	6
SUB-02-01	Acceso posterior subsuelo 2	1
	Archivo	2

La controladora de sistemas operativos se encuentra ubicado en las instalaciones de sistemas operativos en el área de laboratorio. La tabla 2.5 muestra sus puertas correspondientes.

Tabla 2. 5 Puertas correspondientes a sistemas operativos.

SISTEMAS OPERATIVOS	Puerta #
Data center	1
Centro de computo	2
Sistemas operativos	3

2.1.3 LISTADO DE EQUIPOS INSTALADOS.

En la tabla 2.6 se indica el número de dispositivos conectados en el Edificio Corporativo para el sistema control de accesos.

Tabla 2.6 Equipos instalados.

DESCRIPCION	LECTORA	CHAPAS	CONTAC.M	PULSANTES
SUBSUELO 2	3	3	3	0
SUBSUELO 1	10	12	17	5
PLANTA BAJA	15	23	25	2
PRIMER PISO	9	14	18	2
CENTRO DE CÓMPUTO	3	2	2	2
ARCHIVO	1	1	1	0
TOTAL	**41**	**55**	**66**	**11**

2.2 DETECCIÓN DE INCENDIO.

El sistema de detección de incendio del edificio administrativo, supervisa todos los dispositivos instalados en las oficinas, envía una alarma a la central ubicada en el cuarto de seguridad a través de los detectores de humo, calor y las estaciones manuales ayudando así a proteger sus instalaciones de los daños que serían provocados por el humo o el fuego. Se producirá una alarma de incendios cuando se activen:

- Dos o más detectores de humo o calor, ó
- Una estación manual

2.2.1 DISPOSITIVOS DEL SISTEMA.

2.2.1.1 Central de Incendio.

Consiste en tarjetas de control diseñadas exclusivamente para la detección de incendios. Ésta central supervisa los detectores de humo, temperatura y estaciones manuales instaladas. La central se comunica con cada punto, es decir, en caso de una activación, la central sabe exactamente cuál fue el punto (detector, estación manual) que se ha activado, puesto que los dispositivos del

sistema poseen un número de programación único que los diferencia de los demás elementos. La central de incendios posee dos bahías. En cada bahía se colocan las tarjetas de control usadas en este sistema. Figura 2.20.

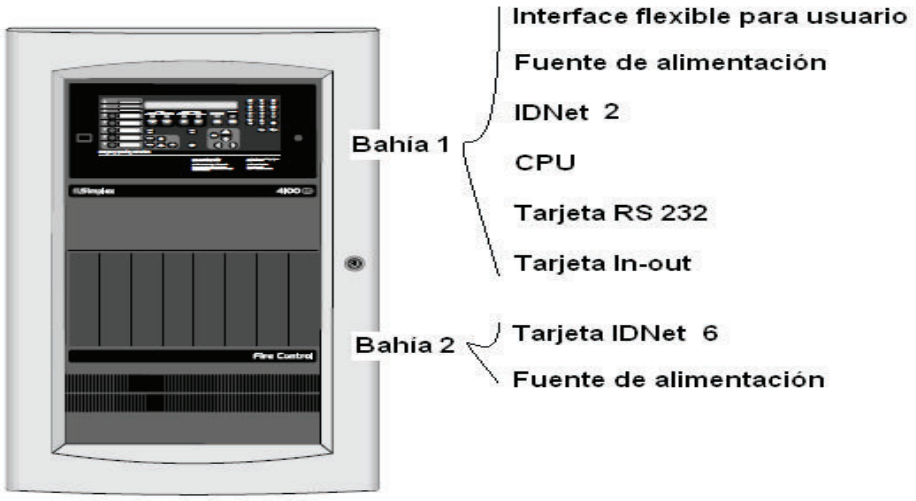


Figura 2. 20 Central de detección de incendios del edificio corporativo.

Además la comunicación IDNet[1] se realiza a través de la tarjeta 2 y 6 y corresponden a los dispositivos que se muestran a continuación:

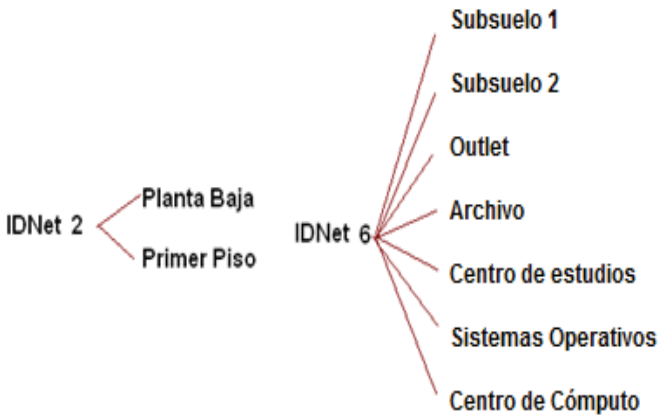


Figura 2. 18 Distribución de los dispositivos direccionables en las tarjetas IDNET.

2.2.1.2 Sensores.

En las instalaciones de la Corporación GPF se encuentran instalados sensores fotoeléctricos y térmicos de la marca Simplex.

[1] Comunicaciones direccionables de los paneles de detección de Incendios marca Simplex

2.2.1.2.1 Sensor de Humo Fotoeléctrico

Los sensores de humo fotoeléctrico utilizan una fuente de luz infrarroja pulsada y un receptor de fotodiodo de silicio para proporcionar una detección de humo de alimentación eléctrica baja coherente y precisa. Tienen siete niveles de sensibilidad disponibles para cada sensor individual, con un rango de 0.2% a 3.7 % por pie de oscuridad de humo. La sensibilidad se selecciona y se monitorea en el panel de control de la alarma de incendio. El cabezal del sensor brinda una entrada de humo de 360º para lograr una respuesta óptima ante el humo desde cualquier dirección. [7]. Figura 2.22

Figura 2. 19 Sensor de humo fotoeléctrico.

2.2.1.2.2 Detectores de Temperatura

Los detectores de temperatura responden a la energía calorífica transportada por convección y se sitúan en el techo. La respuesta se produce cuando el elemento de detección alcanza una temperatura fija determinada o cuando se llega a una velocidad especifica de cambio de temperatura. Figura 2.23.

Figura 2. 20 Sensor de calor.

2.2.1.3 Estaciones Manuales.

La estación manual instalada posee un módulo individual direccionable que monitorea en forma continua el estado y comunica los cambios al panel de control conectado a través de cableado de comunicaciones IDNet. Las estaciones manuales del edificio corporativo son de doble acción (operación con rompimiento de cristal). Figura 2.24.

Figura 2. 21 Estación Manual.

2.2.1.4 Luces Estroboscópicas.

La luz estroboscópica es una fuente luminosa que emite una serie de destellos muy breves en rápida sucesión. Puede dar solo una advertencia temprana de un incendio o un incidente potencialmente peligroso. Este dispositivo no detecta humo, monóxido de carbono, gas, calor o llama. No puede prevenir ni extinguir incendios. La luz estroboscópica se instala y ubica donde los residentes con problemas de audición puedan verla. No tiene medios de detección propios. Figura 2.25.

Figura 2. 22 Luz Estroboscópica/Audible

2.2.2 INTERFAZ DE COMUNICACIÓN.

El panel de detección de incendios posee una tarjeta RS 232 que se utiliza para transmitir datos seriales de este sistema al lantronix UDS 1100 (convertidor serial a Ethernet). El lantronix UDS 1100 va a comunicarse con el servidor de control de acceso por medio del protocolo TCP/IP y así tener comunicación entre ambos sistemas. Con el fin de gestionar en una sola interfaz gráfica el control y monitoreo de estos sistemas de seguridad. Figura 2.26.

Figura 2. 23 Interfaz de comunicación entre sistemas.

2.2.2.1 Tarjeta RS 232.

La tarjeta instalada es 4100-6038 Interface RS-232, marca simplex. Se debe realizar el siguiente procedimiento para configurar el hardware de este sistema:

- Configurar los jumpers de la tarjeta RS 232 (figura 2.27) como indica la tabla 2.7.

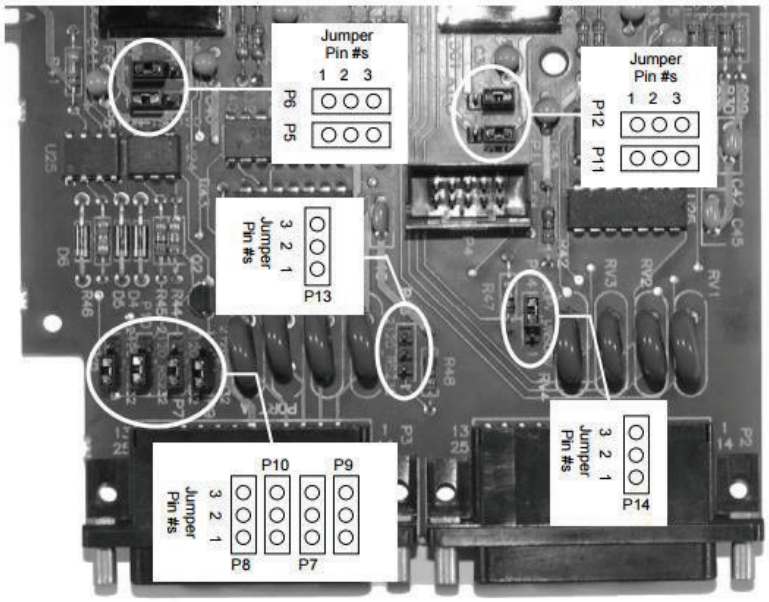


Figura 2.27 Tarjeta RS 232 del panel de detección de incendios.

Tabla 2.7 Configuración de Jumper para comunicación RS 232.

	If Connected to Port A							If Connected to Port B		
	P5	**P6**	**P7**	**P8**	**P9**	**P10**	**P13**	**P11**	**P12**	**P14**
2120 DC COMM (Port A Only)	2-3	2-3	2-3	2-3	2-3	2-3	2-3	N/A	N/A	N/A
2120 Master/Slave Modems, FSK-Type (Port A Only)	2-3	2-3	1-2	1-2	1-2	1-2	None	N/A	N/A	N/A
Service Modem (Port A Only)	1-2	1-2	1-2	1-2	1-2	1-2	None	N/A	N/A	N/A
2120 Comm Standard Modem (Port A Only)	2-3	2-3	1-2	1-2	1-2	1-2	2-3	N/A	N/A	N/A
DC Printer -- Supervised	1-2	1-2	1-2	1-2	1-2	1-2	None	1-2	1-2	2-3
DC Printer -- Unsupervised	1-2	1-2	1-2	1-2	1-2	1-2	1-2	1-2	1-2	1-2
AC Printer, CRT, 3rd Party Computer, GCC, Alert Central -- Supervised	2-3	2-3	1-2	1-2	1-2	1-2	None	2-3	2-3	2-3
AC Printer, CRT -- Unsupervised	2-3	2-3	1-2	1-2	1-2	1-2	1-2	2-3	2-3	1-2

- Configurar los switches.

La tarjeta RS 232 tiene una dirección única, tanto físicamente como en la programación. Su dirección es 004. Ver figura 2.27. Ajustar el switch SW1 en la tarjeta como muestra la figura 2.29.

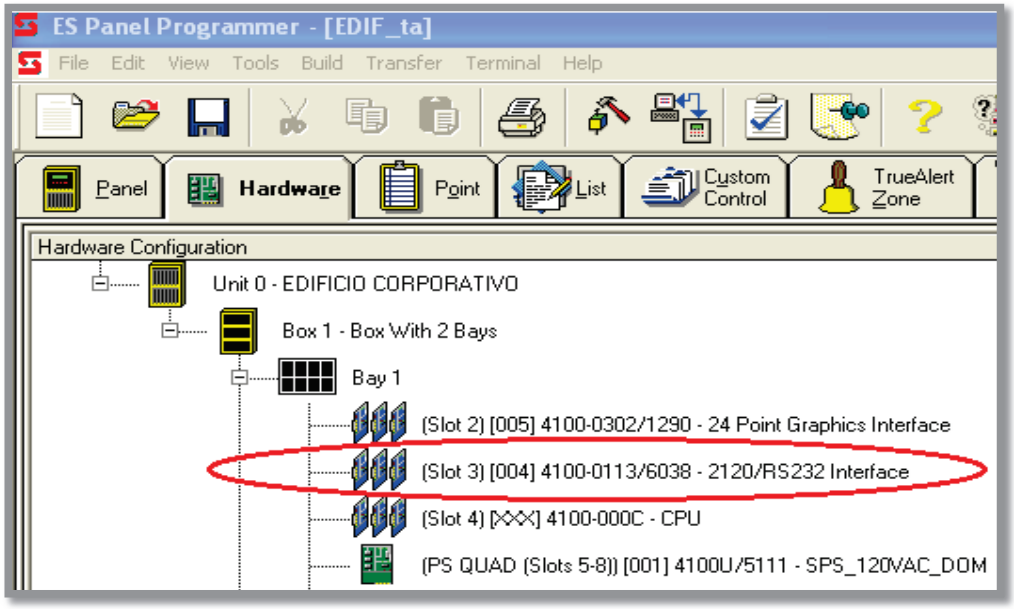
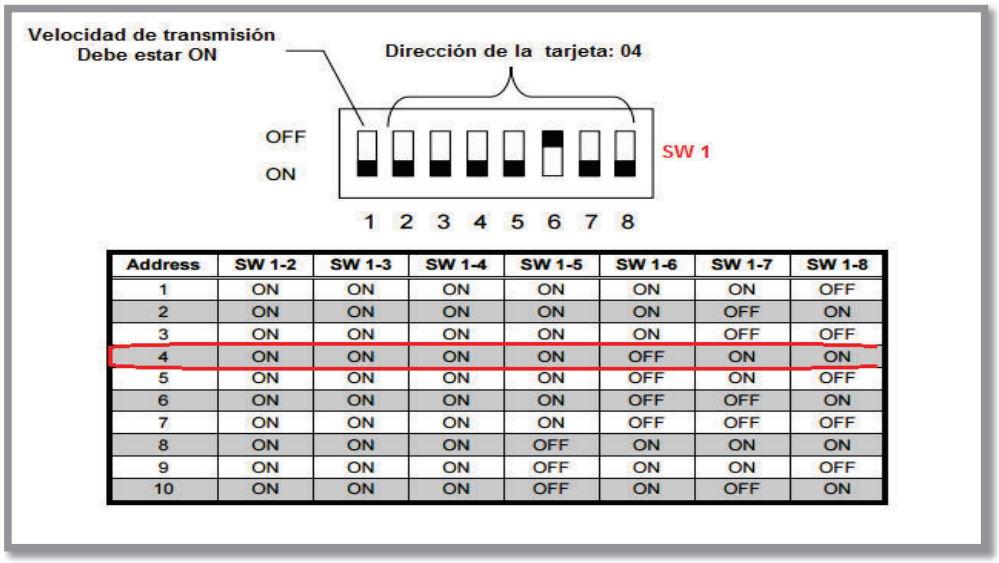


Figura 2. 24 Dirección tarjeta RS 232.

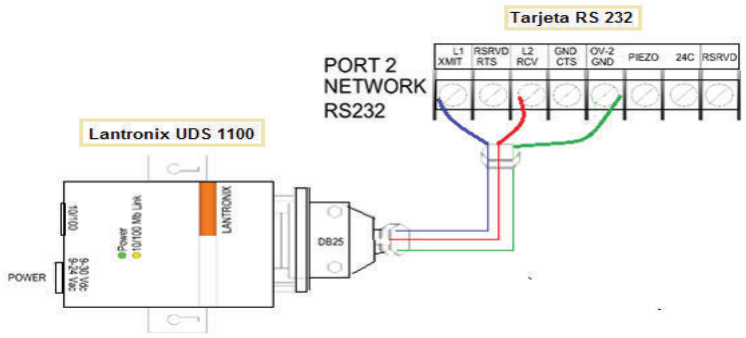


Address	SW 1-2	SW 1-3	SW 1-4	SW 1-5	SW 1-6	SW 1-7	SW 1-8
1	ON	ON	ON	ON	ON	ON	OFF
2	ON	ON	ON	ON	ON	OFF	ON
3	ON	ON	ON	ON	ON	OFF	OFF
4	ON	ON	ON	ON	OFF	ON	ON
5	ON	ON	ON	ON	OFF	ON	OFF
6	ON	ON	ON	ON	OFF	OFF	ON
7	ON	ON	ON	ON	OFF	OFF	OFF
8	ON	ON	ON	OFF	ON	ON	ON
9	ON	ON	ON	OFF	ON	ON	OFF
10	ON	ON	ON	OFF	ON	OFF	ON

Figura 2. 25 Ajustes SW1 sobre la tarjeta RS 232.

2.2.2.2 Lantronix UDS 1100.

El Lantronix UDS 1100 es el dispositivo que permite la comunicación entre la central de detección de incendios (puerto serial) y el servidor de control de acceso por medio de la red Ethernet y usando protocolos de la familia IP (TCP y UDP). Realizar las conexiones como muestra la figura 2.30.



DB25 (LANTRONIX)		CENTRAL DE DETECCION DE INCENDIO 4100 ES
PIN 2	RX	XMIT
PIN3	TX	RCV
PIN7	GND	GND

Figura 2. 30 Conexión Lantronix UDS 1100 con tarjeta RS 232 de central de detección de incendio.

2.2.3 UBICACIÓN.

La central de detección de incendios se ubica en la consola de seguridad y el servidor de control de acceso (CCURE 9000) en el cuarto eléctrico de primer piso lado A. Se comunican mediante Ethernet.

2.2.4 LISTADO DE EQUIPOS INSTALADOS.

En la tabla 2.8 se indica el número de dispositivos instalados en el Edificio Corporativo para el sistema de detección de incendios.

Tabla 2. 8 Dispositivos instalados en el sistema de detección de incendio.

DESCRIPCION	SEN. FOTOE	SEN. TERMICO	EST. MANUAL	LUZ ESTROB	LAM. EMERG
SUBSUELO 2	6	0	2	2	6
SUBSUELO 1	26	17	3	5	23
PLANTA BAJA	75	2	7	17	29

PRIMER PISO	65	0	6	13	22
COMEDOR	0	10	2	2	7
ENFERMERIA	2	4	1	1	3
OUTLET	5	0	1	1	2
GIMNASIO	4	0	2	1	6
SISTEMAS OPERATIVOS	5	0	1	1	0
CENTRO DE CÓMPUTO	2	0	1	1	0
TOTAL	**190**	**33**	**26**	**44**	**98**

2.3 CIRCUITO CERRADO DE TELEVISIÓN CCTV.

El sistema CCTV está formado principalmente por un servidor, clientes y cámaras IP colocadas en áreas específicas del edificio corporativo. Figura 2.31.

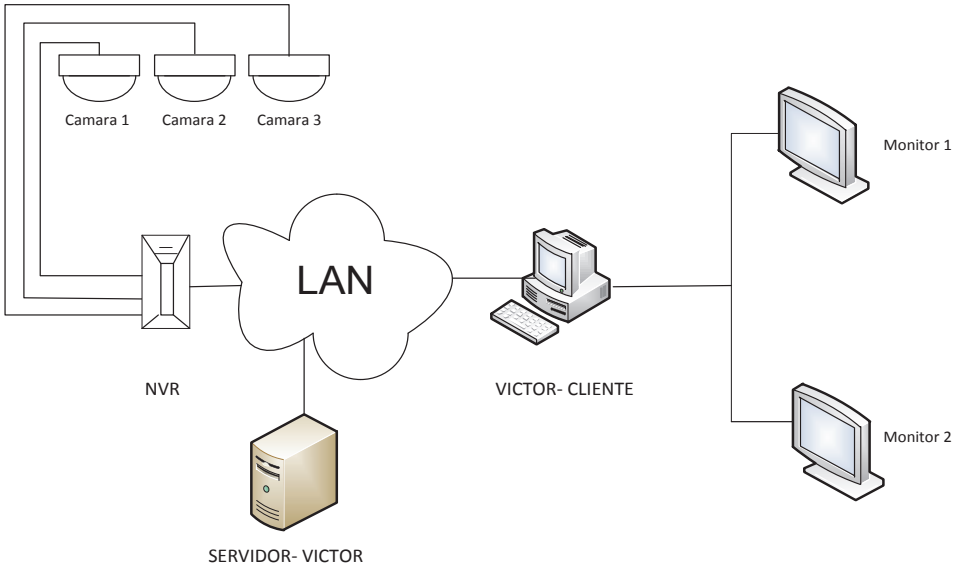


Figura 2. 26 Esquema general del sistema CCTV.

El servidor se encuentra instalado en el cuarto eléctrico de primer piso lado A, los clientes se sitúan en el departamento de seguridad. Adicional se utiliza la plataforma de video VICTOR para la administración y monitoreo independiente del sistema.

VICTOR, es un sistema de administracion unificado de video que permite usar a los usuarios camaras IP y ofrece una solucion para administrar el video con NVR.

2.3.1 DISPOSITIVOS DEL SISTEMA.

2.3.1.1 NVR.

El equipo NVR (Network Video Recorder) administra las cámaras de video y su almacenamiento. El administrador del sitio victor brinda un único punto de acceso a los usuarios y utiliza la funcionalidad de base de datos de SQL Server para brindar autenticación a los clientes, además de permitir un control y una administración centralizados de varias plataformas de grabación en la red.

2.3.1.2 Cámaras Interiores.

Son cámaras IP tipo domo de marca American Dynamics. Tienen una resolución de 2 MP, las cuales funcionan con Switch PoE (Power over Ethernet), de 12 Vdc o 24 VAC. La tecnología Switch PoE describe un sistema para transferir de forma segura potencia eléctrica junto con datos, a dispositivos remotos sobre un cableado categoría 6A, en una red Ethernet sin necesidad de modificar el cableado existente.

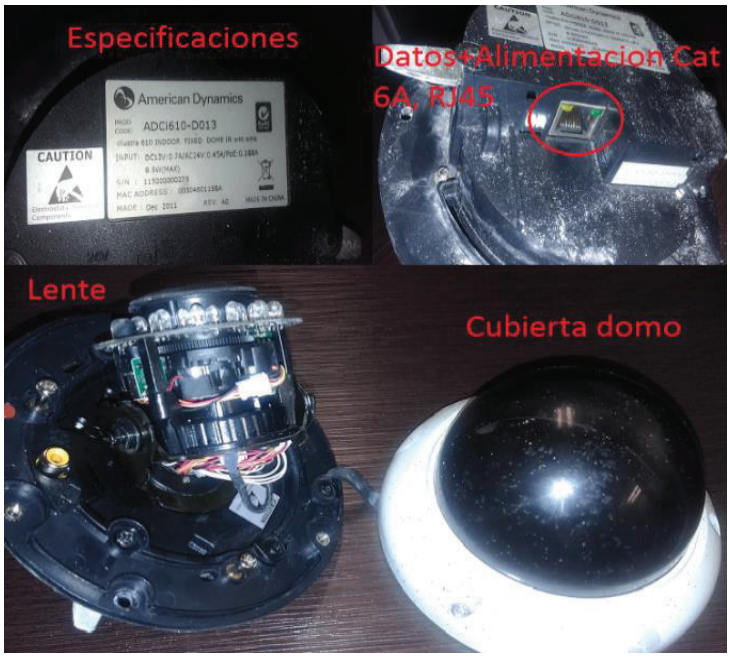


Figura 2.27 Cámara ADCi610-D013 American Dynamics.

La tabla 2.9 muestra las características técnicas de las cámaras interiores.

Tabla 2. 9 Especificaciones técnicas Cámara Domo IP para interiores [8].

Tipo de modelo	**Cámara domo vari-focal para interiores con modo día/noche**
N° de modelo	ADCi610f-D013
Sistema óptico	
Distancia Focal	Vari-focal 3~9 mm
Especificaciones de red	
Compresor de Video	H.264/M-JPEG
Resolución	1800 x 1600
Protocolo de red	TCP/IP, HTTP, NTP, FTP
Fuentes de alimentación	
Requisito de alimentación	PoE IEEE 802.3af clase 0, DC 12 V:0.7 A/ AC 24 V: 0.45A/PoE:0.188A: 8.5 W (MAX)
Consumo de energía	9 W(MAX)
Entorno	
Temperatura de funcionamiento	de -10 °C a 50 °C
Dimensiones	Ø 135 x H 120 mm
Peso	870 g
Mecanismo	
Conectores	Red: conector RJ45/ 10 Base/100 Base-TX

2.3.1.3 Cámaras Exteriores.

Los detalles de las cámaras instaladas se muestran en la tabla 2.10.

Tabla 2. 10 Características técnicas de las cámaras exteriores.

Tipo de modelo	**Cámara SpeedDomo 35X**
N° de modelo	ADVEIPSD35N
Sistema óptico	
Distancia Focal	3.4 a 119 mm
Especificaciones de red	
Compresor de Video	H264/M-JPEG, MPEG-4
Resolución	540 TVL

Tabla 2. 11: Especificaciones Cámaras SpeedDomo Exteriores

Protocolo de red	**TCP/IP, SMTP, FTP**
Fuentes de alimentación	
Requisito de alimentación	PoE IEEE 802.3af clase 0, DC 12 V / AC V 24 /PoE: 12.95 W
Consumo de energía	11 W
Entorno	
Temperatura de funcionamiento	de -10 °C a 50 °C
Dimensiones	Ø 120 x H 205 mm
Peso	1,09K g
Mecanismo	
Conectores	Red: conector RJ45/ 10 Base/100 Base-TX

2.3.2 INTERFAZ DE COMUNICACIÓN.

El sistema CCTV no requiere ningún convertidor ni hardware adicional, esto debido a que todos sus dispositivos se comunican a través de Ethernet. Este sistema se puede comunicar con el servidor de control de acceso sin ningún problema. El grabador de video y las cámaras poseen una dirección IP estática.

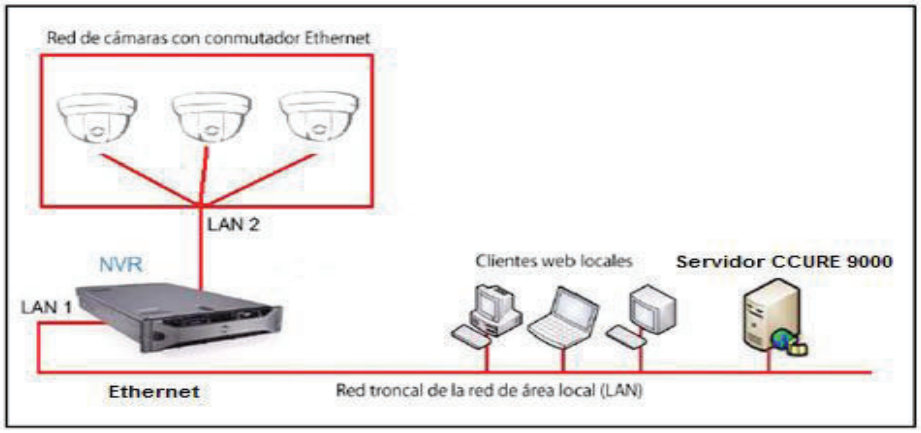


Figura 2. 28 Esquema del sistema CCTV.

2.3.3 DISTRIBUCIÓN DE CÁMARAS.

Una vez realizada la selección y el montaje de las cámaras IP se procede a asignarles un nombre, una dirección IP y la ubicación de las mismas en la edificación como se observa en la Tabla 2.12.

Tabla 2. 12 Direcciones IP de las cámaras del edificio administrativo.

N.	DESCRIPCION	CAMARA	UBICACIÓN	DIRECCION IP
1	PRIMER PISO	CAM-PP-PTZ-1	Exterior frontal	172.22.36.101
2	PLANTA BAJA	CAM-PB-PTZ-2	Exteriores puerta posterior edificio	172.22.36.102
3	SUBSUELO 2	CAM-S2-2	Exteriores de archivo	172.22.36.103
4		CAM-S2-3	Externa lagunas	172.22.36.104
5		CAM-S2-1	Archivo	172.22.36.105
6	SUBSUELO 1	CAM-S1-2	Parqueaderos ejecutivos	172.22.36.106
7		CAM-S1-1	Puerta parqueaderos ejecutivos	172.22.36.107
8		CAM-S1-3	Contabilidad gradas-archivo	172.22.36.108
9		CAM-S1-5	Puerta posterior contac center-contabilidad	172.22.36.110
10		CAM-S1-4	Seguridad-parqueaderos ejecutivos	172.22.36.111
28		CAM-S1-6	Cámara salida auditorio	172.22.36.112
11	PLANTA BAJA	CAM-PB-1	Pasillo gerencia Servicios Corporativos	172.22.36.113
12		CAM-PB-2	Pasillo tecnología	172.22.36.114
13		CAM-PB-4	Puerta terraza-financiero	172.22.36.115
14		CAM-PB-3	Baños planta baja	172.22.36.116
15		CAM-PB-6	Ingreso principal	172.22.36.117
16		CAM-PB-5	Baño proveedores-servicios al personal	172.22.36.118
17		CAM-PB-7	Comercialización	172.22.36.119
18	PRIMER PISO	CAM-PP-1	Gerencia general	172.22.36.120
19		CAM-PP-2	Escaleras unidad de negocio	172.22.36.121
20		CAM-PP-4	Recepción	172.22.36.122
21		CAM-PP-3	Asuntos responsabilidad corporativa	172.22.36.123
22		CAM-PP-5	Pasillo auditoria-do-finanzas	172.22.36.124
23	OUTLET	CAM-OUT-2	Caja Oki-Doki	172.22.36.125
24		CAM-OUT-1	Ingreso Oki-Doki-produbanco	172.22.36.126
25	COMEDOR	CAM-CD-1	Comedor	172.22.36.127
27	ENFERMERIA	CAM-EN-1	Enfermería	172.22.36.128
26	SIS. OPERATIVOS	CAM-SIS-1	Sistemas Operativos	172.21.9.200

En las figuras 2.34, 2.35, 2.36, 2.37, se observa la cobertura de cada cámara instalada.

Figura 2.29 Cámaras del edificio corporativo_1.

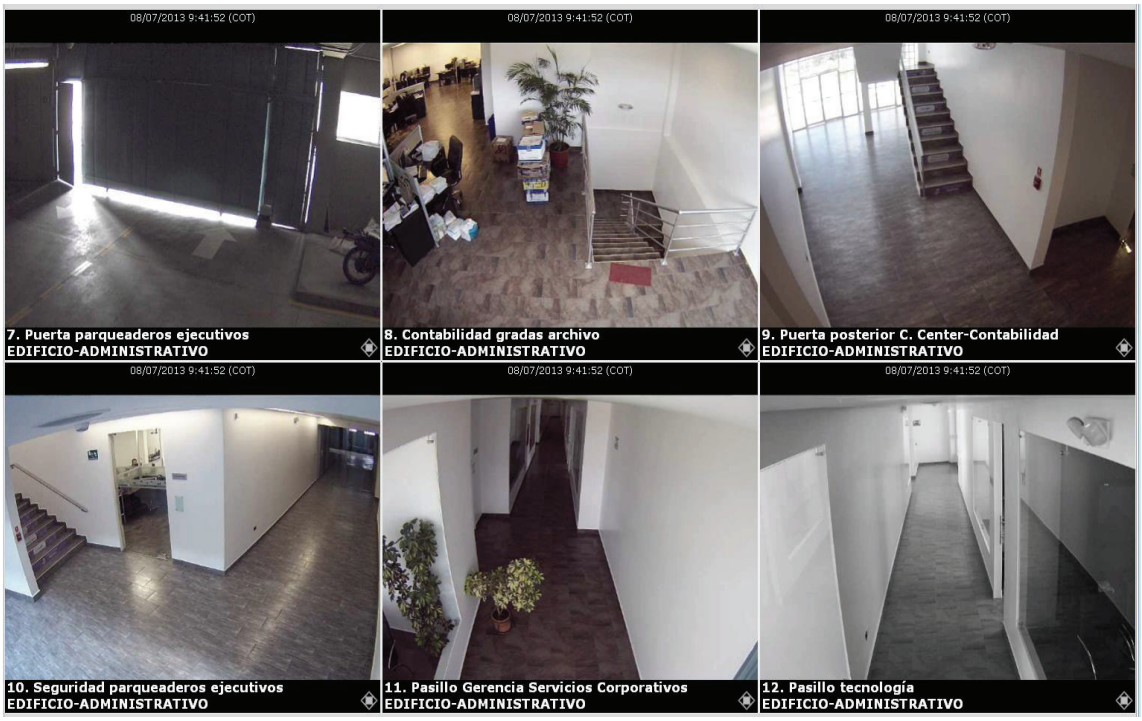


Figura 2.30 Cámaras del edificio corporativo_2.

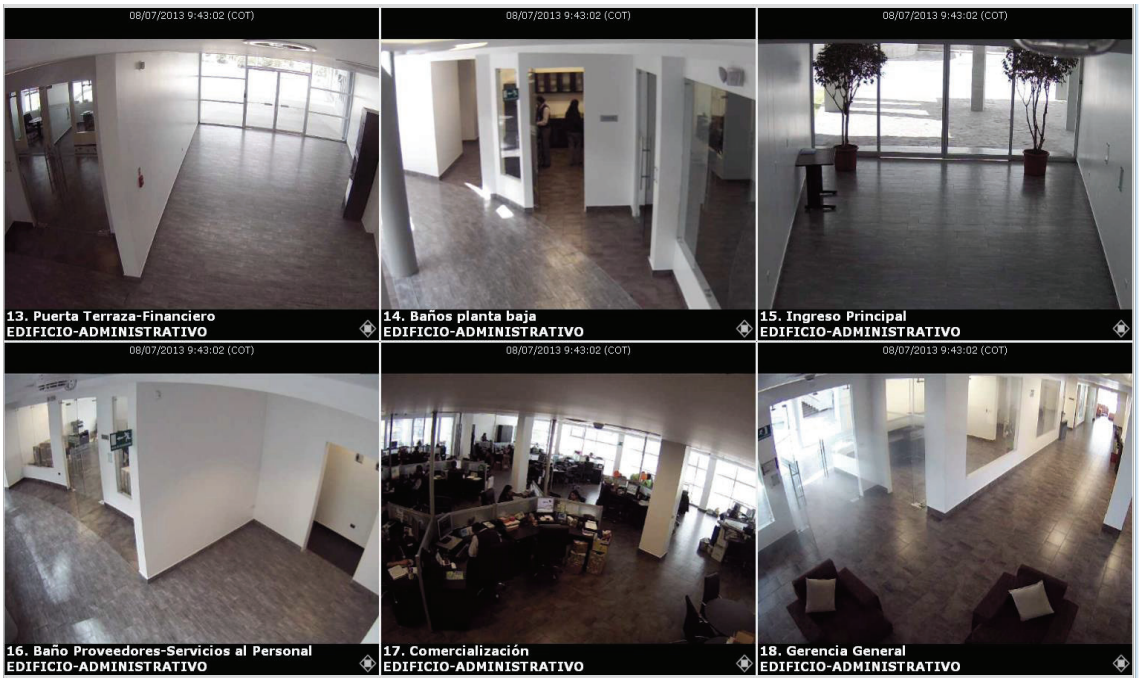


Figura 2.31 Cámaras del edificio corporativo_3.

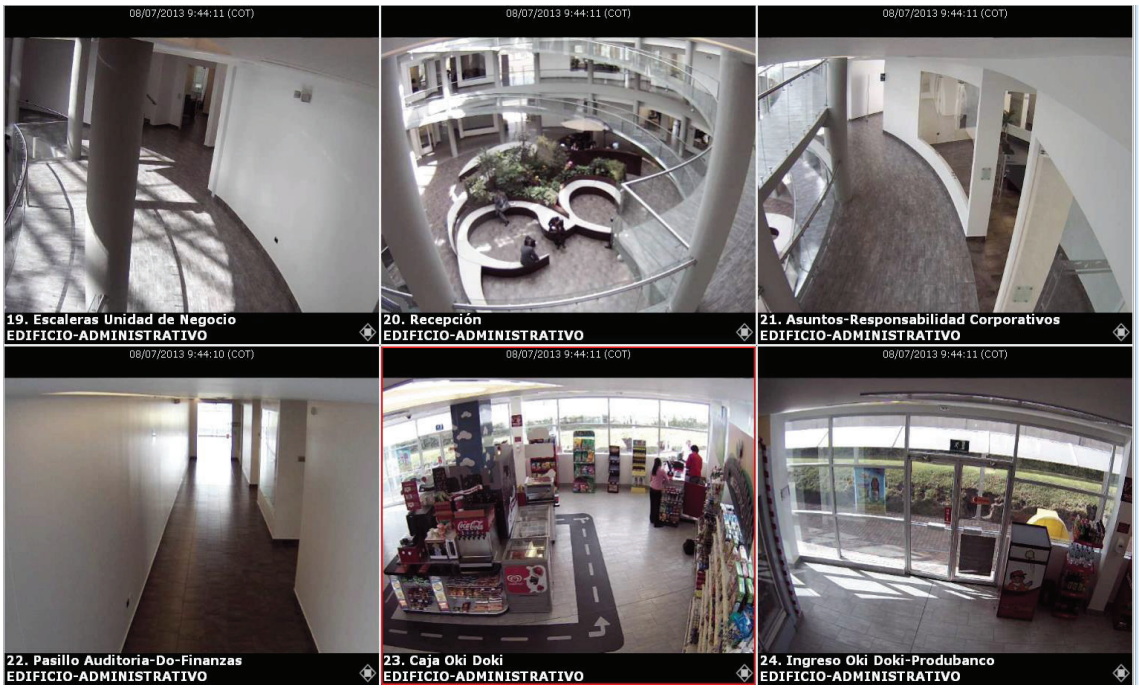


Figura 2.37 Cámaras del edificio corporativo_4.

2.4 SISTEMA DE INTRUSIÓN.

El sistema está formado por tres centrales de intrusión ubicadas en consola de seguridad, archivo y casa de estudio respectivamente. Utilizan convertidores de comunicación serial a Ethernet (lantronix UDS 1100) para que puedan comunicarse con el servidor del sistema de control de accesos (integrador) a través del protocolo TCP/IP y de ésta manera se pueda monitorear los eventos a través de la plataforma CCURE 9000.

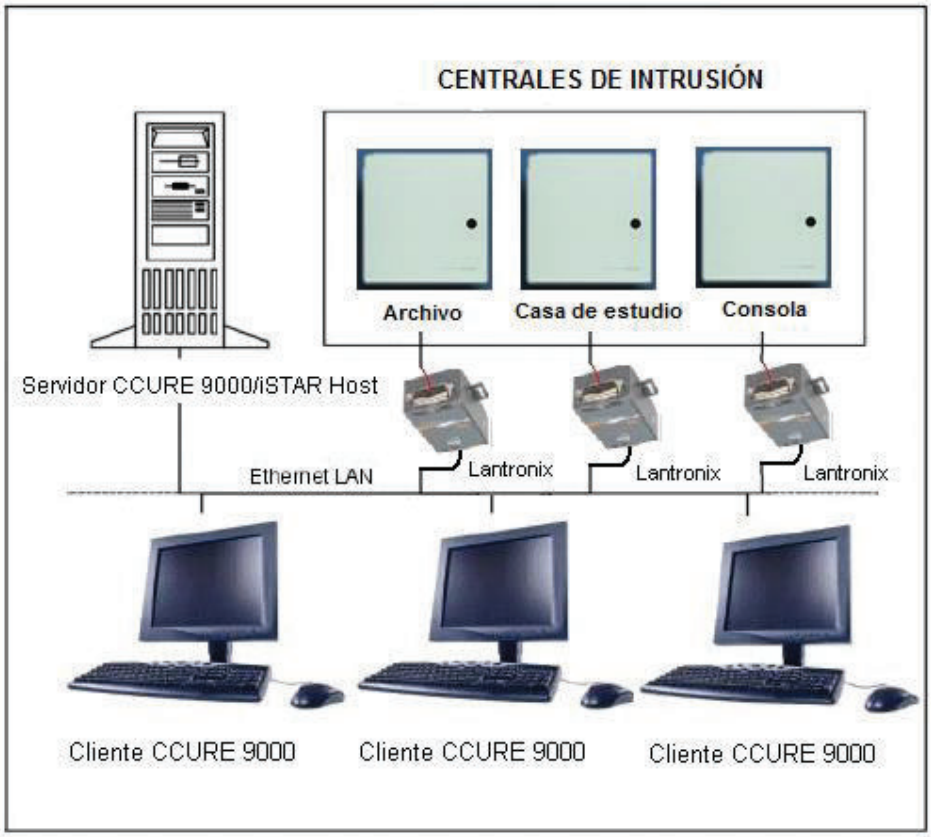


Figura 2.38 Diagrama general del sistema contra intrusión.

2.4.1 DISPOSITIVOS DEL SISTEMA.

2.4.1.1 Central DSC PC 1864.

La Central de alarmas utilizada es la PC1864 (figura 2.38), sus características se muestran en la tabla 2.13.

Figura 2.32 Central de alarmas PC1864.

Tabla 2. 13 Características central PC 1864.

Zonas en la tarjeta	**8**
Zonas cableadas	64(7xPC5108)
Teclados	8
Particiones	8
Códigos de usuario	94 + Código maestro
Memoria de eventos	500 eventos
Transformador Necesario	16,5 VCA/40 VA
Batería Necesaria	4 Ah/7 Ah/14AHr
Salida de sirena	12 Vcc/700mA
Modulo Compatible	Expansor de zonas PC5108 (30 mA)

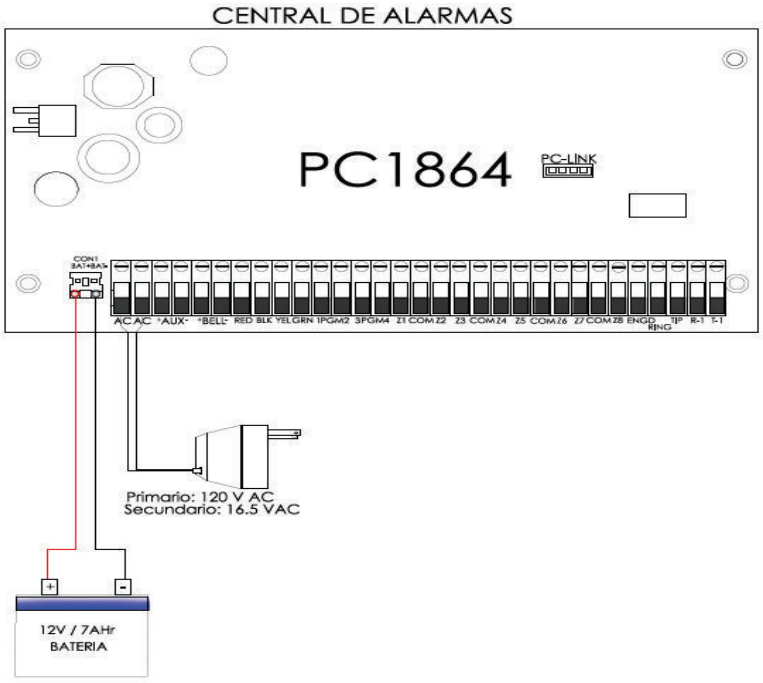


Figura 2.33 Central de Alarmas PC 1864.

La Central de alarmas PC 1864 es alimentada por 16 V de corriente alterna, este voltaje se obtiene mediante un transformador cuyo primario 110 V. Se conecta a una batería (12V / 7AHr) la cual permite tener energizada la central en caso de corte eléctrica. Figura 2.40.

La conexión de comunicación entre la central y todos los módulos se realiza con las borneras de 4 hilos (rojo, negro, amarillo y verde), siendo:

- RED(rojo): Positivo
- BLK(negro): Negativo
- YEL(amarillo) y GRN(verde): Comunicación

Los 4 terminales KEYBUS en todos los módulos deben estar conectados en los 4 terminales KEYBUS del panel de control principal.

2.4.1.2 Sensores de Movimiento.

Los detectores detectan el movimiento en las áreas cubiertas por sus sensores de seguridad (Sensores volumétricos). Los detectores de movimiento transmiten

señales de radio de alta frecuencia. Cuando un objeto tiene una temperatura diferente a la del medio y se encuentra dentro del campo de captación del sensor, la radiación calórica del objeto será captada por los lentes del elemento sensorial ocasionando el accionamiento del sensor. Figura 2.41.

Figura 2.341 Detector de movimiento.

2.4.1.3 Sirenas.

Se puede tener alarmas internas y externas. Alarma interna: Su misión es informar y avisar a las personas presentes en el edificio además de disuadir y alertar al servicio de vigilancia. Alarma externa: La finalidad de su instalación es avisar e informar a las cercanías del edificio y disuadir a intrusos.

2.4.1.4 Teclado.

Se utiliza para configurar, activar o desactivar el sistema. Tiene botones con funciones especiales como: emergencia médica, intrusión, fuego, etc.

Figura 2.42 Teclado Alfanumérico.

2.4.2 INTERFAZ DE COMUNICACIÓN.

Las central de intrusión poseen tarjetas IT-100 que se utilizan para transmitir datos seriales de estas centrales a cada lantronix UDS 1100 (convertidor serial a Ethernet) conectado a ellas.

El lantronix UDS 1100 permite comunicarse con el servidor de control de acceso por medio del protocolo TCP/IP posibilitando la comunicación entre ambos sistemas; con el fin de gestionar en una sola interfaz gráfica el control y monitoreo de estos sistemas de seguridad. Figura 2.43.

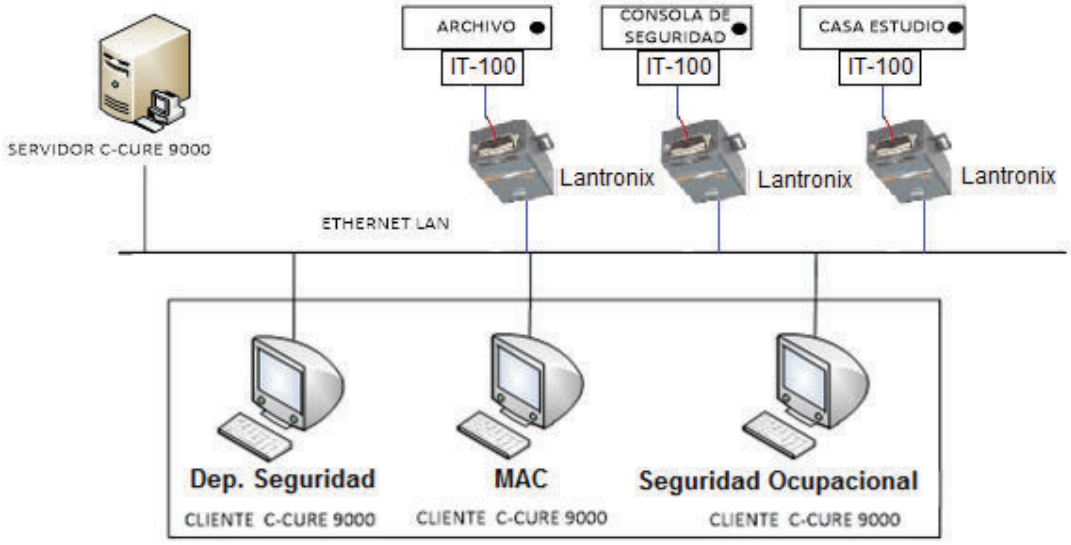


Figura 2.35 Diagrama General Sistema Contra Intrusión C-CURE 9000.

2.4.2.1 Tarjeta IT-100.

La tarjeta IT-100 es un módulo de integración. Posee una interfaz bidireccional RS-232. La conexión de KEYBUS de 4 hilos es utilizada por el panel para comunicarse con este módulo.

- RED(rojo): Positivo
- BLK(negro): Negativo
- YEL(amarillo) y GRN(verde): Comunicación

El Modulo de Integración IT-100 tiene un terminal DB-9, en el que se conecta el RX, TX y GND. Figura 2.44.

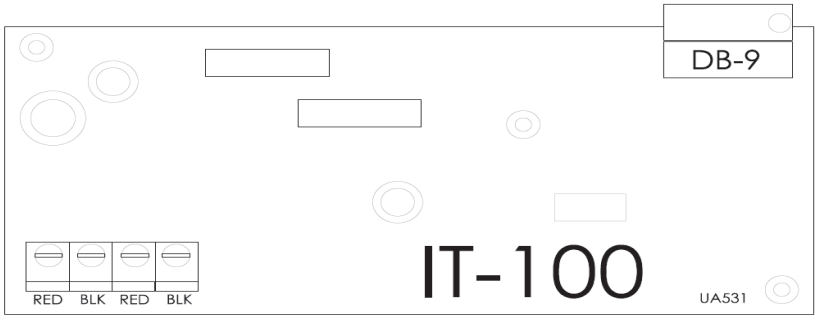


Figura 2. 36 Módulo de Integración IT-100.

Conectar el DB9 del módulo IT-100 con el conector DB25 del lantronix UDS 1100 como muestra en la tabla 2.14 y la figura 2.45.

Tabla 2. 14 Conexión terminales del módulo IT-100 y lantronix UDS 1100.

IT-100 (DB9)	LANTRONIX (DB25)
Rx: 2	Tx: 2
Tx: 3	Rx: 3
GND: 5	GND: 7

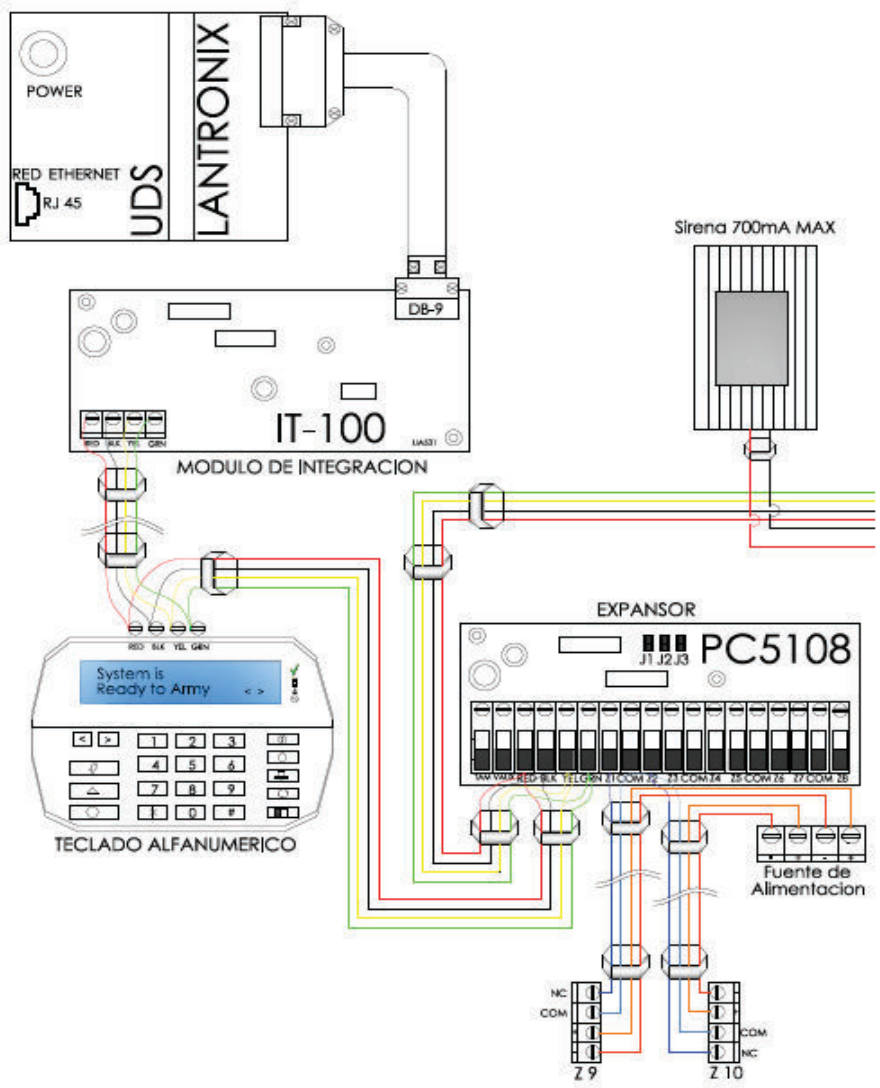


Figura 2. 37 Conexión módulo IT-100 con lantronix UDS 1100.

2.4.2.2 Lantronix.

Lantronix es un conversor de RS232 a Ethernet, el cual permite llevar y gestionar los datos a distancia para dispositivos no conectados actualmente a una red. Figura 2.46.

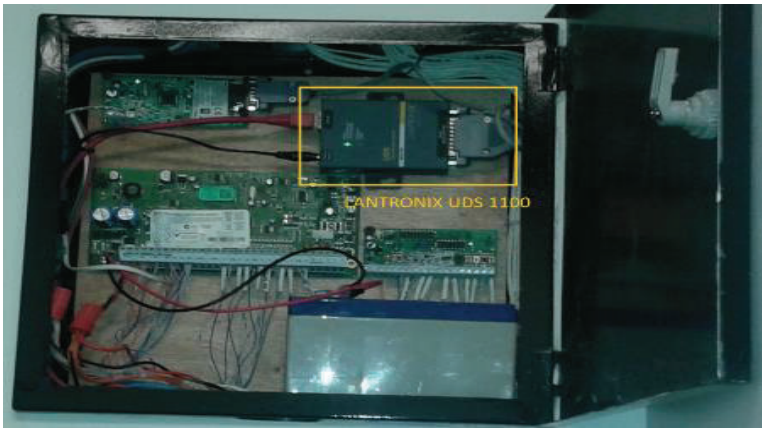


Figura 2.38 Central de alarmas PC1864-Lantronix UDS 1100.

2.4.3 UBICACIÓN DE LAS CENTRALES DE INTRUSIÓN.

Las centrales de intrusión se encuentran ubicadas en consola de seguridad, archivo y caso de estudio. Cada central posee una tarjeta IT-100 y un dispositivo lantronix UDS 1100 para la comunicación entre el sistema de intrusión y el servidor de control de acceso.

2.4.4 LISTADO DE EQUIPOS INSTALADOS.

El listado de equipos instalados se muestra en la tabla 2.15.

Tabla 2. 15 Equipos instalados sistema de intrusión.

DESCRIPCION	SENSOR	CONTACTO MAGNÉTICO	SIRENA
COMEDOR	4	4	0
OUTLET	2	3	1
ARCHIVO	3	1	0
CASA ESTUDIO	2	2	1
SUBSUELO 2	1	3	0
SUBSUELO 1	11	9	0
PLANTA BAJA	19	7	1
PRIMER PISO	9	5	1
PLANTA + 8.00	0	1	0
TOTAL	51	35	4

CAPÍTULO 3

PROGRAMACIÓN DEL SISTEMA DE INTEGRACIÓN

3.1 CCURE 9000.

CCURE 9000 es un sistema de administración de eventos y de seguridad flexible. Es orientado a objetos que cuenta con una variedad de interfaces adaptables para el mantenimiento del sistema y para supervisar los emplazamientos que desee proteger.

Ofrece una amplia capacidad de administración de información utilizando Microsoft SQL Server y Microsoft .NET Framework V4.0. Su arquitectura distribuida servidor-cliente es capaz de admitir una gran gama de los clientes, controladores y dispositivos de entrada, incluidos varios lectores de tarjetas y cámaras. Con CCURE 9000, un equipo puede actuar tanto como servidor como cliente. Figura 3.1.

- UN SERVIDOR: realiza las funciones básicas de CCURE 9000 y a él pueden acceder varios usuarios. El servidor de CCURE actúa también como host para los controladores de iSTAR Edge y para los paneles DSC, etc.
- UN CLIENTE: realiza las funciones administrativas y de supervisión para un único usuario.

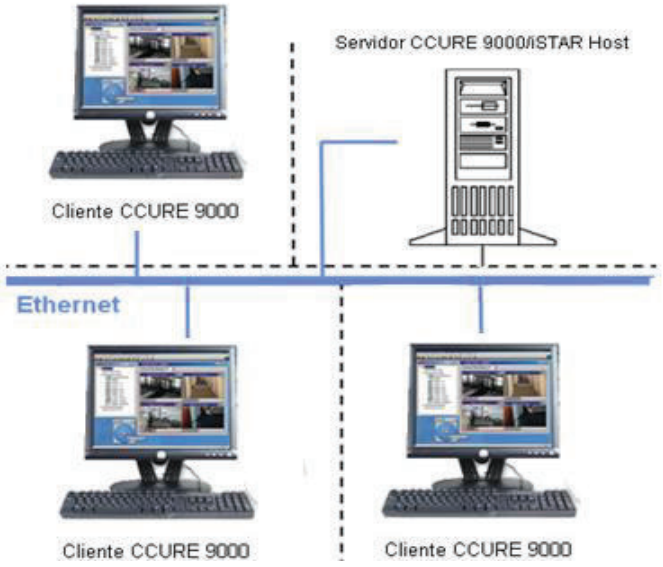


Figura 3.1 Servidores y clientes CCURE 9000.

El servidor de CCURE 9000 y sus clientes son normalmente equipos independientes conectados a través del protocolo de conexión de red TCP/IP.

3.1.2 REQUERIMIENTOS DEL SISTEMA.

El departamento de redes de la Corporación GPF proporcionó un equipo administrador para instalar la plataforma CCURE 9000, en base a los requerimientos que a continuación se detalla:

- **Sistema Operativo**
  - Windows 7 o Windows Server 2008 R2 (Sistema operativo 64 bits).
  - Windows Server 2003, Windows XP.
- **RAM**

  - Debe disponer, como mínimo, de 2 GB de espacio libre en la unidad

- **TRAJETA DE ADAPTADOR**
  - De 24 bits o 32 bits de video en color para los mapas de alta resolución, incluyendo fotografías.

3.1.3 APLICACIÓN DE ADMINISTRACIÓN.

Una vez instalado el software CCURE 9000 se puede acceder tanto a la aplicación de administración como a la de monitoreo de este programa. A continuación se muestra las principales operaciones que se puede hacer desde la aplicación de administración (Figura 3.2):

- Configurar los objetos de seguridad del sistema, por ejemplo: controladores, paneles, puertas y lectores, días festivos, horarios, eventos del sistema y activadores, hardware de vídeo de CCURE y de terceros, y conmutadores CCTV.
- Configurar particiones, las áreas iSTAR, las zonas de intrusión y los comandos de teclado.
- Configurar las rondas de vídeo.
- Configurar los registros de personal, los operadores, y los privilegios de operador.
- Mostrar, importar y exportar los registros de personal y otros datos del sistema.
- Configurar los eventos de respuesta a: entradas, alarmas de vídeo, fallos de comunicación, configurar los eventos para activar acciones, por ejemplo: activar salidas y control de CCTV, activar otros eventos.
- Configurar los diseños de aplicación (supervisión).
- Utilizar las vistas dinámicas para ver los datos de configuración y estados del sistema.
- Mostrar, importar y exportar imágenes.
- Informar sobre datos históricos y de configuración y videoclips.

Figura 3.2 Aplicación de administración.

3.1.4 ESTACIÓN DE SUPERVISIÓN.

La estación de supervisión permite supervisar eventos, actividades, estados de los dispositivos y accesos de seguridad. Sus principales actividades son:

- Utilizar las vistas dinámicas para ver los datos de configuración y el estado del sistema.
- Mostrar, importar y exportar imágenes.
- Informar sobre datos históricos y de configuración y videoclips.

Inicie la estación de supervisión de la siguiente manera:

- Haga doble click en el icono de escritorio de la estación de supervisión o clic en Inicio> todos los programas> Software House> CCURE 9000> estación de supervisión.

La pantalla que se abre (figura 3.3), es sólo una de las varias maneras posibles de configurar el diseño de la aplicación de supervisión desde la aplicación de administración.

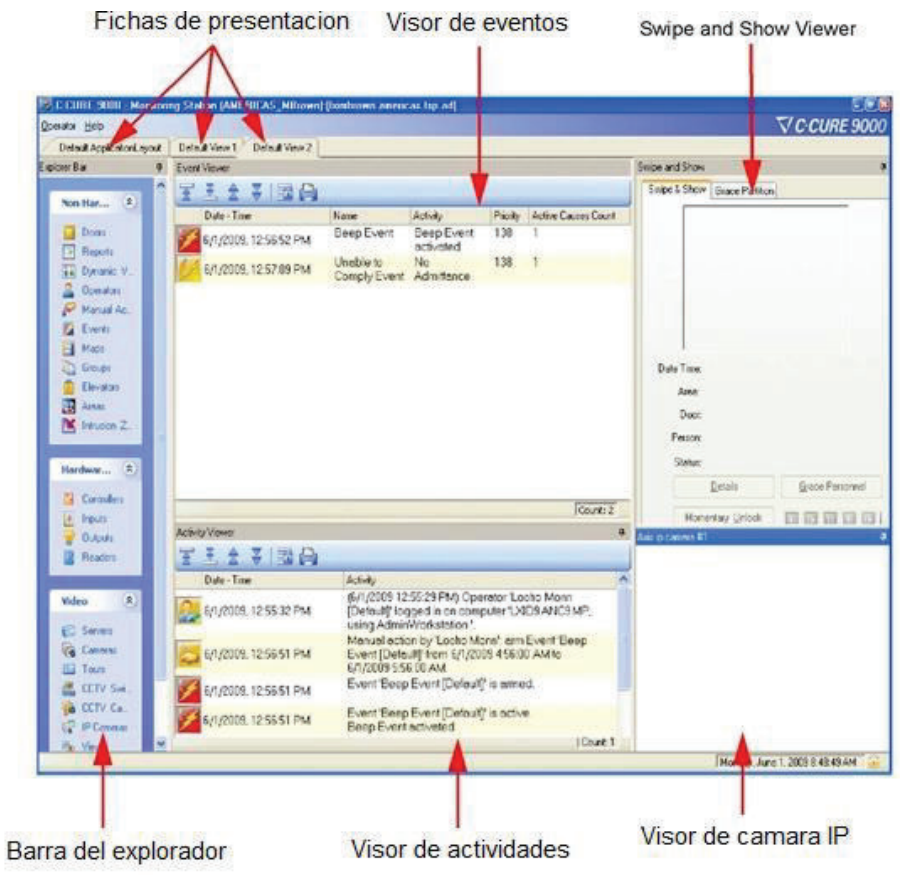


Figura 3.3 Aplicación de administración.

3.2 CONFIGURACIÓN DEL SISTEMA CONTROL DE ACCESO.

El sistema de control de acceso posee controladoras que basan su funcionamiento en el protocolo TCP/IP. Esta característica permite una instalación rápida en la red Ethernet del edificio corporativo. El departamento de sistemas asigna direcciones IP para el servidor y controladores. Ver tabla 3.1, 3.2 y figura 3.5.

Tabla 3. 1 Datos del Servidor de CCURE 9000.

Servidor:	**CCURE**
Nombre Host:	UIOCCURE
Usuario:	Administrator
Dirección IP	172.22.50.20

A continuación se realiza la configuracion de lectura de tarjeta para el Sistema Control de Acceso. Figura 3.4

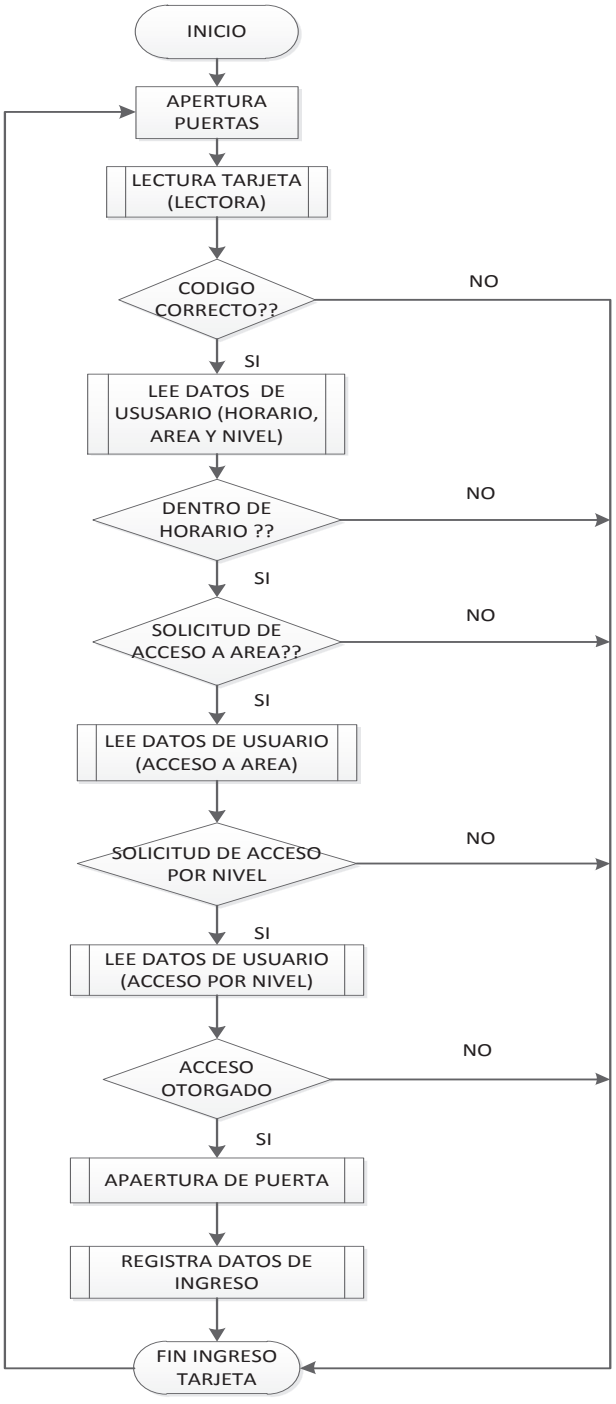


Figura 3.4 Lectura de Tarjeta.

Tabla 3. 2 Asignación de direcciones IP a controladoras Istar Edge.

PISO	TARJETA iSTAR	IP	PUERTAS
ARCHIVO	Master ARCHIVO	172.22.50.26	Archivo nuevo
SUBSUELO 2	Master SUB-2-01	172.22.36.162	Acceso Posterior Sub 2
			Bodega Sistemas
SUBSUELO 1	Master SUB-1-01	172.22.36.154	Consola de Seguridad
			Contabilidad
			Ducto Eléctrico Lado A
			Seguridad
	Esclavo 1 SUB-1-02	172.22.36.155	Bodega UPS
			Concentrador de Fibra Óptica
			Contact Center
			Tableros Eléctricos
	Esclavo 2 SUB-1-03	172.22.36.156	Parqueadero Ejecutivos
PLANTA BAJA PB "LADO B"	Esclavo 1 PB-B-01	172.22.36.157	Ducto Eléctrico PB-B
			Oficinas Marketing
			Selección de Personal
			Servicios al Personal
	Master PB-B-02	172.22.36.158	Marketing
PLANTA BAJA\ PB "LADO A"	Master PB-A-01	172.22.36.151	Control asistencia ingreso
			ducto eléctrico planta baja A
			Servicio a domicilio
			Tecnología puerta posterior
	Esclavo 1 PB-A-02	172.22.36.152	Gerencia General
			Ingreso Gerencia Servicios
			MAC
			Tecnología
	Esclavo 2 PB-A-03	172.22.36.153	Adquisiciones
			Subgerencia SC
			Terraza Planta Baja
	Esclavo 3 PB-A-04	172.22.36.150	Control Asistencia Salida
PRIMER PISO P1 "LADO B"	Master P1-B-01	172.22.36.160	Auditoria Interna/Manejo de Riesgos
			Ducto Eléctrico Piso 1 B
			Legal, ABF
			Responsabilidad Corporativa
	Esclavo 1 P1-B-02	172.22.36.161	Desarrollo Organizacional
			Planeación y Finanzas
PRIMER PISO P1 "LADO A"	Master P1-A-01	172.22.36.159	Ducto Eléctrico Piso 1 A
			Gerencia General
			UN Fybeca / UN Sana Sana

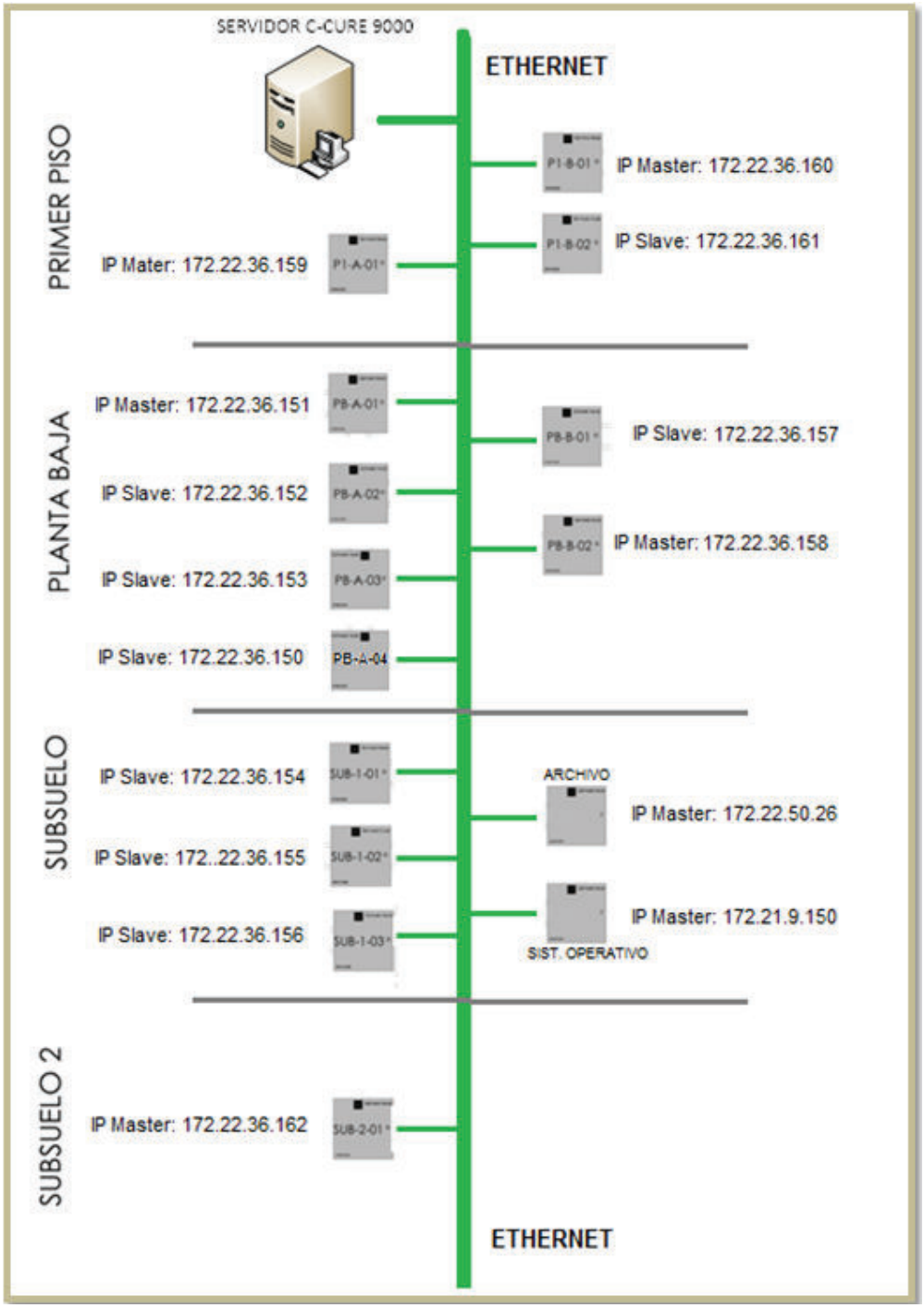


Figura 3.5 Arquitectura de las controladoras Istar Edge.

El sistema tiene la estructura servidor-cliente. El servidor realiza las funciones básicas de la plataforma de control de accesos y a él pueden acceder varios

usuarios. El servidor de CCURE 9000 actúa como host[2] para los controladores, en cambio el cliente realiza las funciones administrativas y de supervisión para un único usuario.

3.2.1 CONFIGURACIÓN DE LAS CONTROLADORAS.

Los controladores se comunican con el host de CCURE 9000 mediante protocolo TCP/IP. Los puertos integrados son Ethernet; por lo tanto, debe conectar físicamente los controladores con una LAN Ethernet. Para especificar las direcciones IP se utiliza el programa ICU.exe. Seguir el siguiente procedimiento:

- Doble click sobre ICU.exe. Al abrir se despliega la imagen de la figura 3.5, donde se muestra el nombre y dirección MAC de la controladora. En esta ventana se selecciona si la controladora es master (maestro) o slave (esclavo).

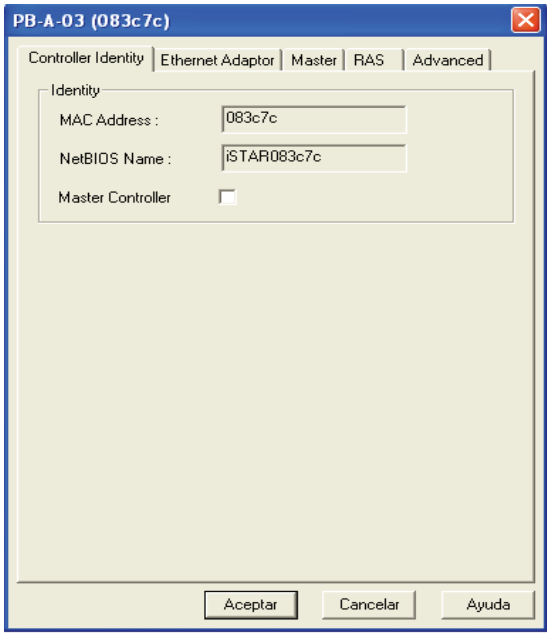


Figura 3.6 Configuración de la controladora.

- Colocar la dirección IP, máscara y gateway asignados por el departamento de sistemas de la corporación GPF. Además solicitar las direcciones del servidor DNS primario, secundario y el sufijo DNS (gfybeca.int). Adicional,

[2] Host o anfitrión es un ordenador que funciona como el punto de inicio y final de la transferencia de datos. Comúnmente descrito como el lugar donde reside un sitio web.

si está configurando una controladora esclava debe poner la dirección IP del maestro. Figura 3.7.

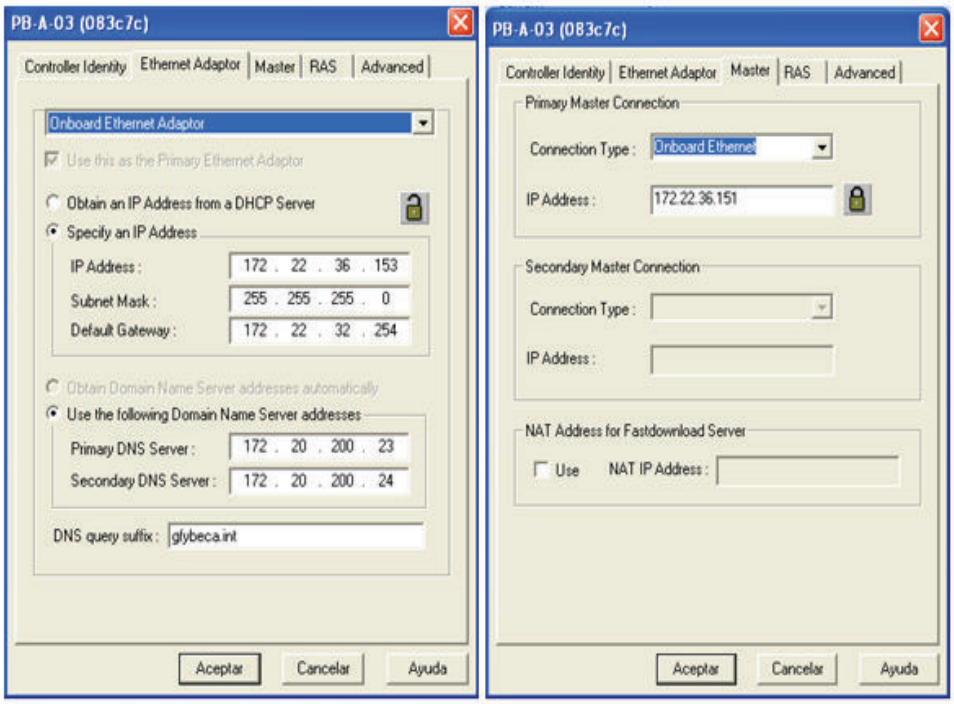


Figura 3.7 Configuración de las controladoras Istar Edge desde ICU.

3.2.2 CREACIÓN DE LAS CONTROLADORAS.

Para crear las controladoras en la plataforma CCURE 9000 es necesario primero crear el clúster[3] y dentro de éste crear las controladoras. Para mejorar la seguridad de la instalación se creó grupos de clúster en cada cuarto eléctrico. Cada clúster atiende a un controlador master, el cual gestiona la comunicación primaria entre el servidor y los demás controladores dentro de ese clúster. El controlador master comunica todos los sucesos y los datos de los titulares de tarjetas entre el clúster y el servidor de CCURE 9000. Figura 3.8.

[3] Agrupación de todos los controladores maestros y esclavos.

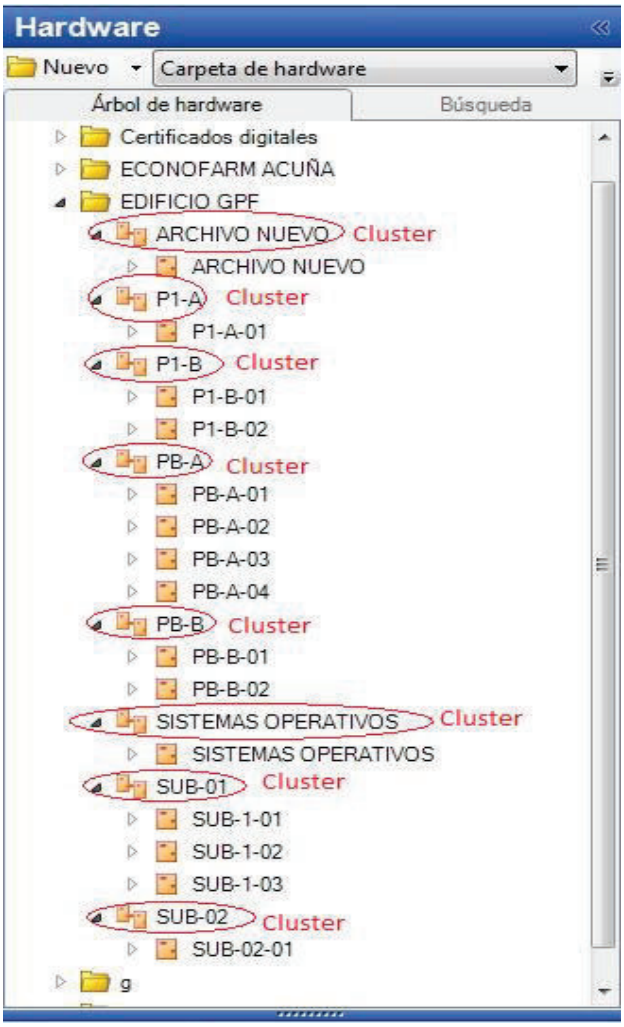


Figura 3.8 Clúster Sistema Control de Accesos.

Para crear la controladora realizar lo siguiente: presionar hardware> edificio corporativo> crear clúster> nueva controladora. Para cada controladora se asigna las lectoras y contactos magnéticos que posee. Luego se debe crear una puerta, que se realiza agrupando los dispositivos de entrada y salida que permiten controlar dicha puerta. Figura 3.9

Se dispone de controladoras de dos y cuatro lectoras. Dependiendo el material de la instalación, una lectora puede servir para el ingreso y la salida del personal (gypsum), caso contrario requiere dos controladoras, una para el ingreso y otra para la salida en la misma puerta (bloque).

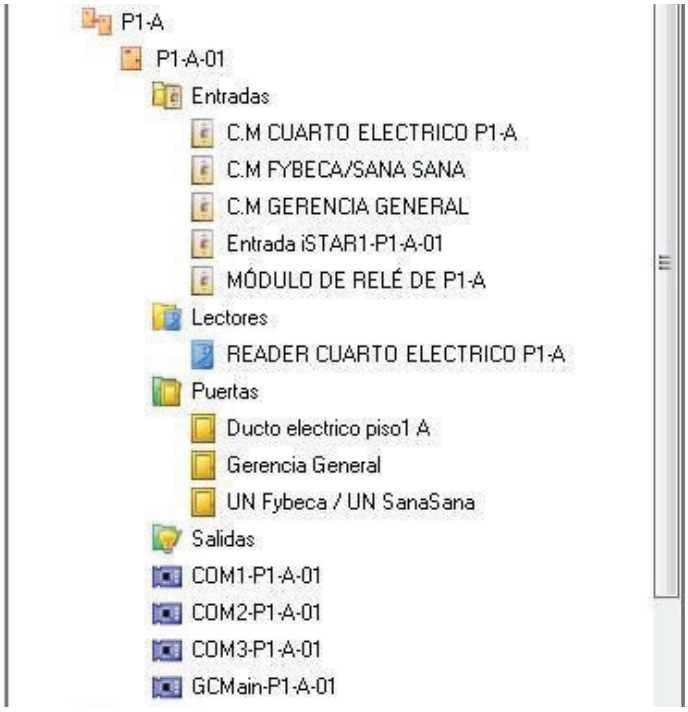


Figura 3.9 Dispositivos de una controladora.

3.3 CONFIGURACIÓN SISTEMA DETECCIÓN DE INCENDIO.

El sistema de detección de incendio se programa por medio de un software que facilita su configuración y se monitorea en tiempo real por medio de un convertidor RS 232/Ethernet que permite conectarse a través de la red intranet de la empresa para hacer monitoreos remotos a través del software de integración CCURE 9000.

Para establecer la comunicación entre el servidor de CCURE 9000 y el panel 4100ES se usa el dispositivo lantronix UDS1100 que es un convertidor serial a Ethernet. Esto debido a que el panel de detección de incendios se encuentra alejado del servidor de CCURE 9000.

La tarjeta RS 232 del panel simplex 4100ES y la interface de alarma de fuego en CCURE 9000 son configuradas con iguales propiedades de comunicación. Las propiedades por default en la tarjeta RS 232 son las recomendadas y se colocan cuando se programa en el 4100ES.

3.3.1 CONFIGURACIÓN DE TARJETA RS 232.

Para ingresar a la configuración de la tarjeta RS 232, se accede por medio del software programador de los paneles simplex 4100ES, se busca la tarjeta RS 232 navegando en el programa. Figura 3.10.

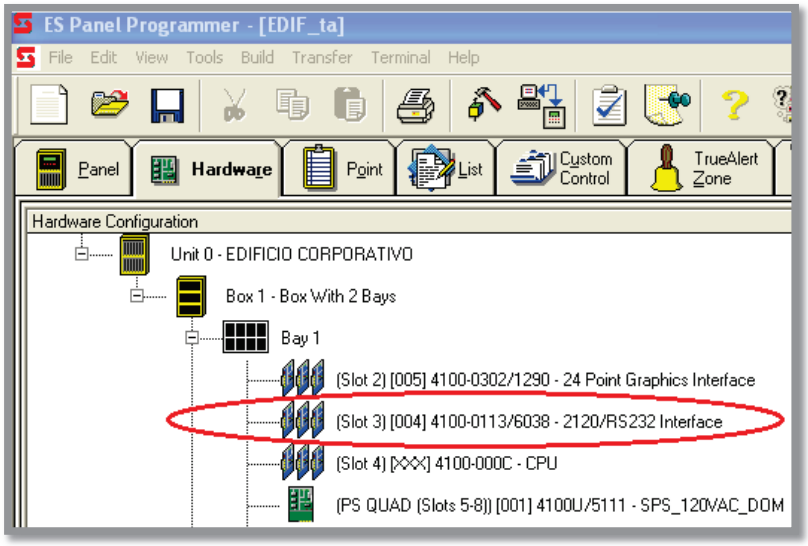


Figura 3.10 Programador paneles simples 4100 ES.

- Hacer doble click para abrir la ventana de configuración de esta tarjeta. Se accede al puerto B ya que el puerto A fue diseñado para dar servicio. Figura 3.11.

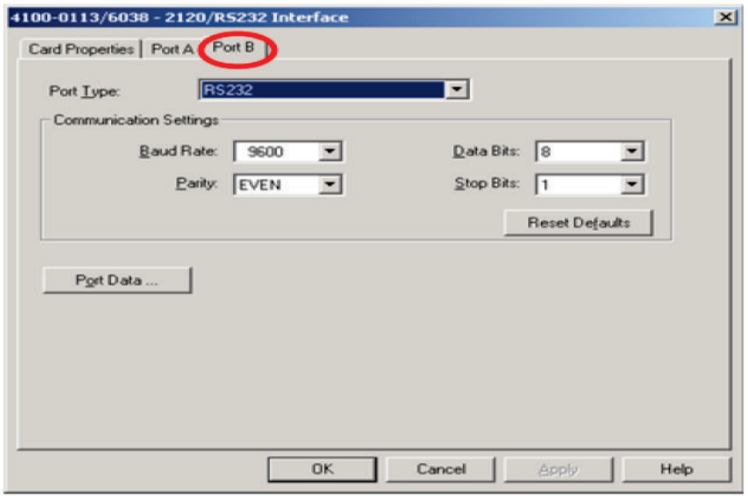


Figura 3.21 Ajustes de la tarjeta RS 232.

- En información general se configura como se muestra en la figura 3.12

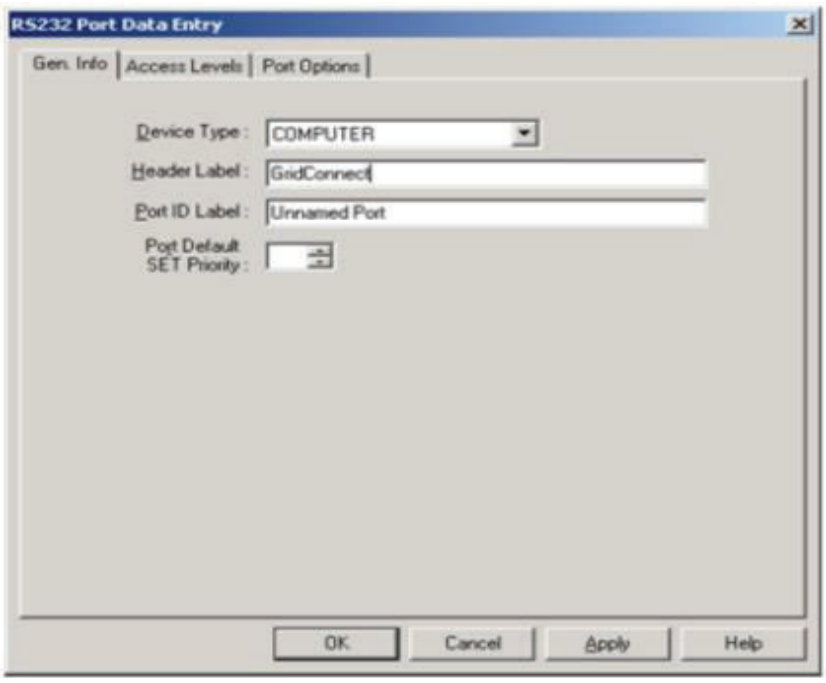


Figura 3.12 Ventana de configuración general.

- En niveles de acceso y opciones de puerto se deja los ajustes de default. Figura 3.12.

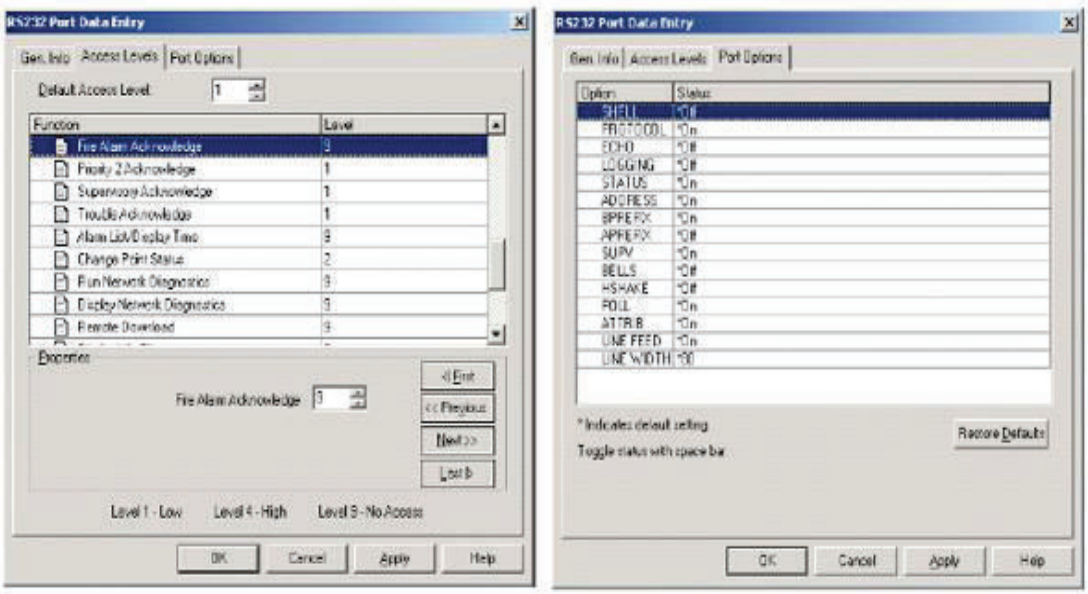


Figura 3.3 Configuraciones niveles de acceso y opciones de puerto.

3.3.2 CONFIGURACIÓN DE LANTRONIX.

Lantronix UDS 1100 es un convertidor de un puerto serial a un puerto Ethernet, el cual permite establecer comunicación entre el servidor de CCURE 9000 y el panel de detección de Incendios Simplex 4100ES. Seguir las siguientes instrucciones:

- Abrir el Buscador web y colocar la dirección 172.18.11.190 en la barra de direcciones. Esta es una dirección de default. El dispositivo USD1100 solicita un usuario y contraseña. Dejar los espacios en blanco y presionar OK.

Figura 3.4 Ventana de usuario y contraseña de lantronix UDS 1100.

- El administrador Web se despliega. Seleccionar Channel 1> serial settings (ajustes manuales) del menú de la izquierda y la página de configuración serial aparece como muestra en la figura 3.15.

- En ajustes seriales (serial settings) se configura el puerto de acuerdo a los ajustes del puerto serial de la tarjeta RS 232 del panel simplex 4100ES. Figura 3.15.

- Seleccionar Network del menú principal de la izquierda. Se despliega la página de ajustes de configuración de red (network). Colocar la dirección IP 172.22.50.23. Figura 3.16.

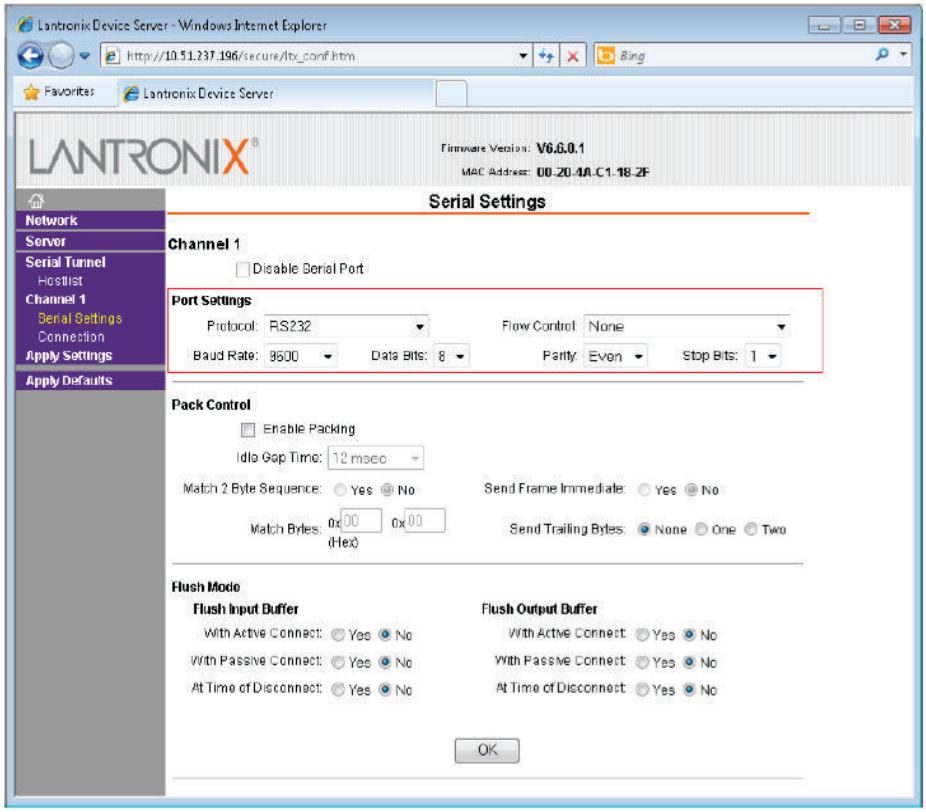


Figura 3.5 Ajustes Seriales.

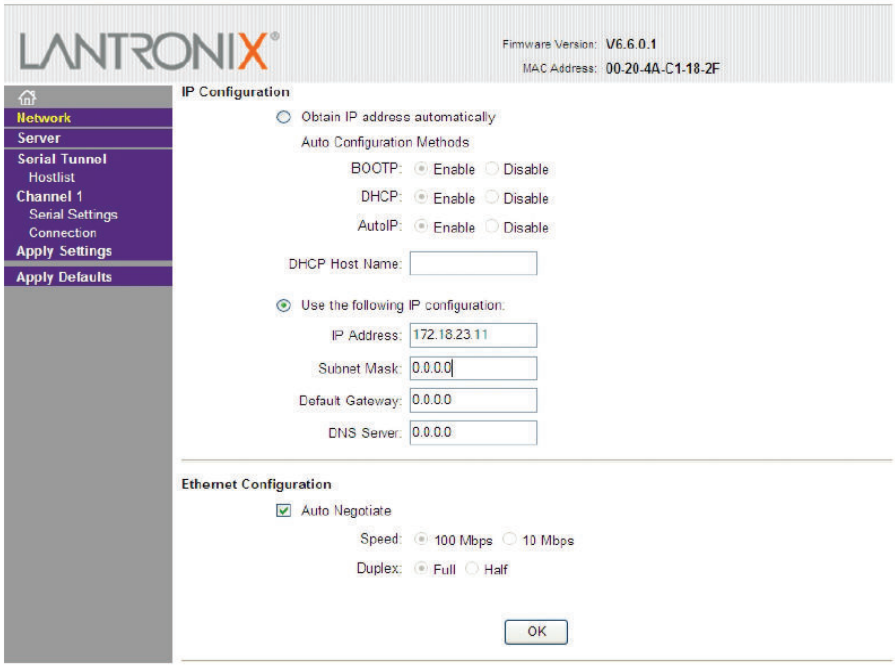


Figura 3.16 Ajustes de red.

3.3.3 ADQUISICIÓN DE DATOS.

Una vez creado el nuevo panel se debe sincronizar la base de datos de CCURE 9000 con el panel simplex 4100U. Se sincroniza usando adquisición de datos. Realizar el siguiente procedimiento:

- Navegar hasta el Panel Simplex 4100U por medio de la carpeta hardware, Seleccione el panel y luego haga clic derecho.
- Aparece un nuevo menú, hacer clic en data acquisition. Figura 3.17.

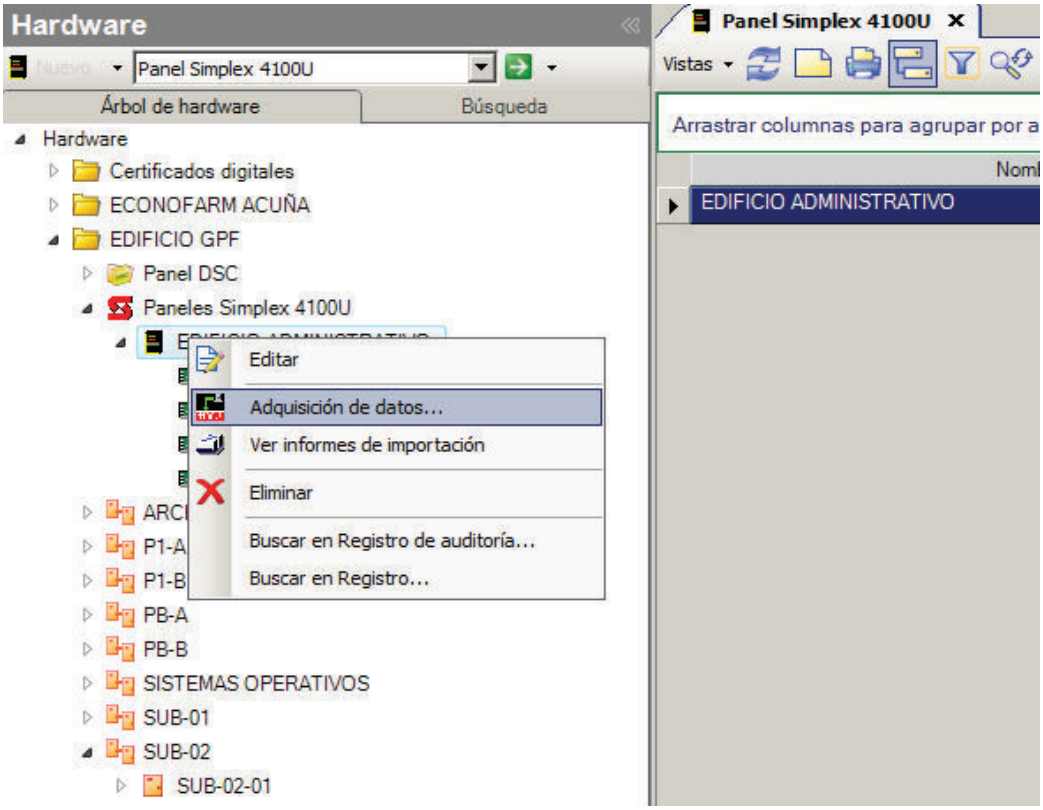


Figura 3. 6 Adquisición de datos.

- Una ventana de diálogo aparece y si la configuración es correcta, se despliega la siguiente información.

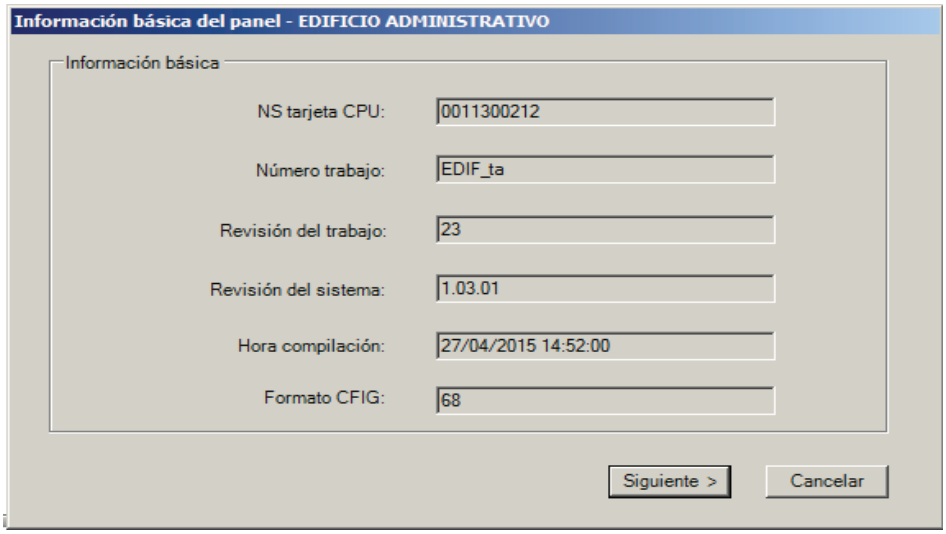


Figura 3. 7 Información básica del panel 4100ES.

- Click en next y el sistema presenta el reporte de datos importados al sistema CCURE 9000. Figura 3.19.

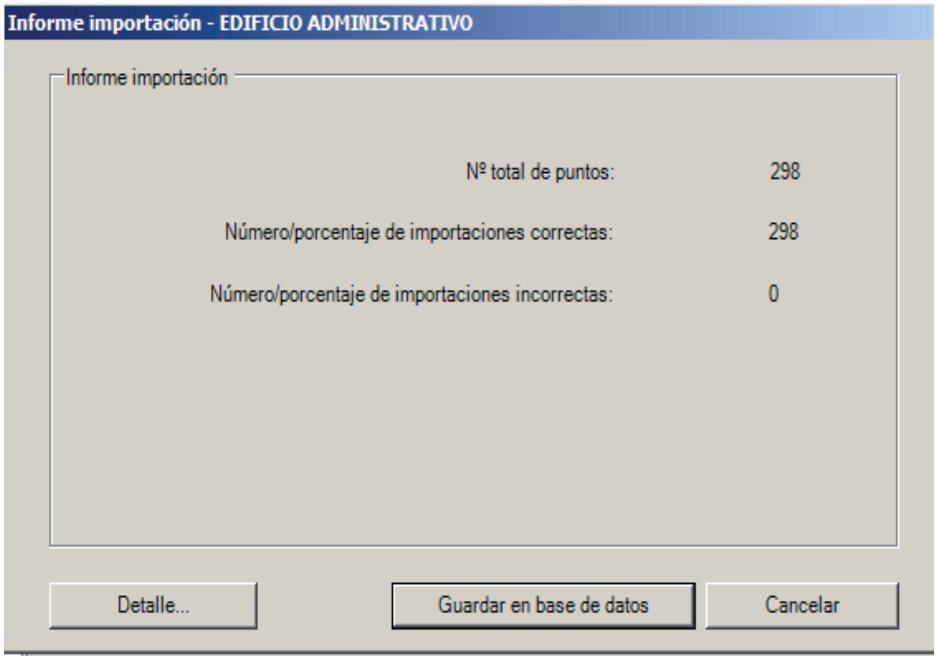


Figura 3. 8 Reporte importado.

- Para guardar en la base de datos de CCURE 9000, presione “save to database”. Una vez que los datos se han guardado en la base de datos,

aparece el siguiente mensaje. La Adquisición de datos está completa y se cierran todas las ventanas.

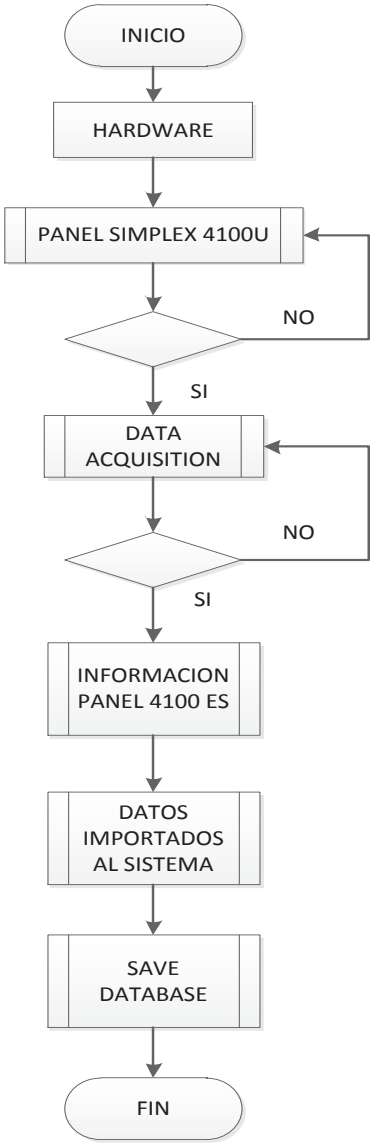


Figura 3. 9 Adquisicion de datos.

3.3.4 CREACIÓN DE EVENTOS.

Un evento es un objeto que permite vincular acciones, mensajes y activaciones de tiempo en un único componente. Los eventos son activados por cambios de estado de los dispositivos involucrados en los sistemas de seguridad implementados. CCURE 9000 administra eventos mediante una estrategia de causa y efecto. Todo lo que CCURE 9000 puede monitorizar puede usarse para

generar un evento y el evento puede activar cualquier acción. En este caso se usa para mostrar planos del edificio y visores de cámaras. CCURE 9000 usa triggers, los cuales se configuran para activar eventos basados en las propiedades de los objetos. El trigger automáticamente ejecuta una acción específica cuando una condición particular ocurre.

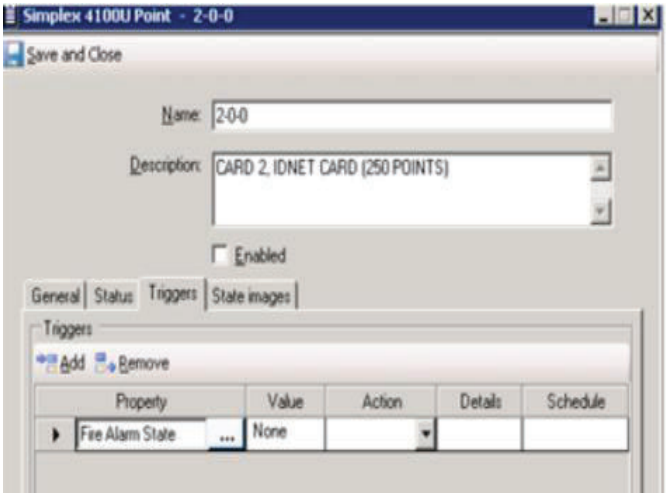


Figura 3.21 Creación de trigger.

- Trigger para mostrar cámaras

Para mostrar las cámaras del edificio se utiliza las propiedades que tiene el objeto. Si el sensor o la estación manual se encuentra activo, activa el evento llamado mostrar cámara.

Es decir, a cualquier momento (horario siempre), el estado de alarma de fuego (propiedad) es igual a anómalo necesita reconocimiento (valor), activar el evento (acción) llamado mostrar cámara. Tabla 3.3. Figura 3.22

Tabla 3. 3 Trigger de cámaras.

Propiedad	Valor	Acción	Detalles	Horario
Estado de alarma	Anómalo necesita reconocimiento	Activar evento	Mostrar cámara	Siempre

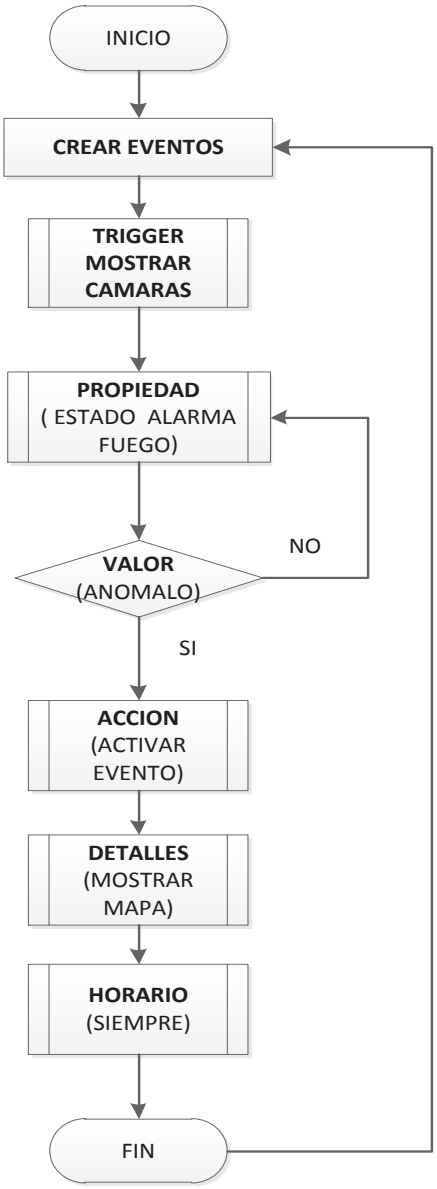


Figura 3.22 Creación de Eventos mostrar cámaras.

- Trigger[4] para mostrar planos. [9]

Para mostrar los planos del edificio corporativo en el momento que se activa una estación manual o sensor, se sigue la siguiente lógica.

[4] Trigger (activadores) son procedimientos configurados para activar acciones, eventos o salidas para un dispositivo iSTAR. Ejecuta una accion especifica

A cualquier momento (horario siempre), el estado de alarma de fuego (propiedad) es igual a anómalo necesita reconocimiento (valor), activar el evento (acción) llamado mostrar mapa. Tabla 3.4. Figura 3.23

Tabla 3. 4 Trigger mostrar planos.

Propiedad	Valor	Acción	Detalles	Horario
Estado de alarma	Anómalo necesita reconocimiento	Activar evento	Mostrar mapa	Siempre

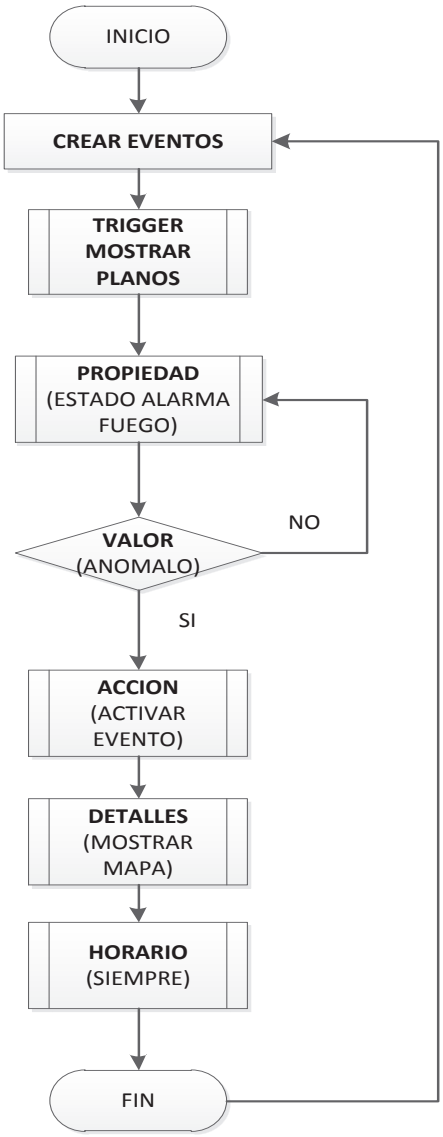


Figura 3.23 Creación de Eventos mostrar mapas.

3.4 CONFIGURACIÓN SISTEMA CCTV.

3.4.1 CONFIGURACIÓN DE DIRECCIONES IP.

El sistema está formado por un grabador de video y cámaras distribuidas en las instalaciones de la Corporación GPF. El departamento de sistemas asignó direcciones IP para sus dispositivos. Tabla 3.5 y 3.6.Figura 3.23

Tabla 3. 5 Dirección IP grabador de video.

Servidor:	**Video Edge** 
Usuario::	admin
Clave:	Es9001
Dirección IP	172.22.36.1

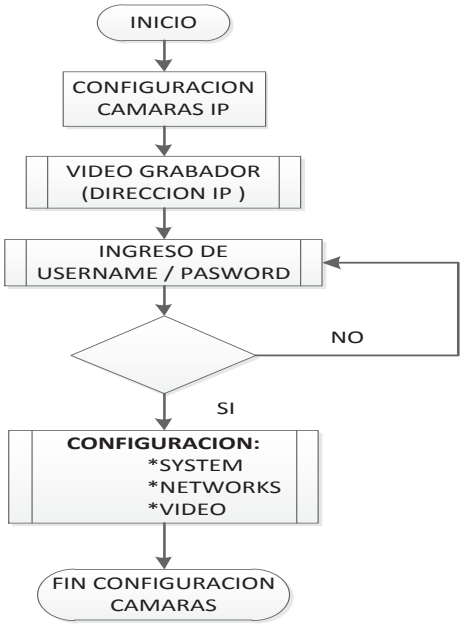


Figura 3.23 Configuracion camaras IP.

Tabla 3. 6 Asignación de direcciones IP a cámaras de seguridad.

N.	DESCRIPCION	CAMARA	DIRECCION IP	UBICACIÓN
1	**PRIMER PISO**	CAM-PP-PTZ-1	172.22.36.101	Exterior frontal
2	**PLANTA BAJA**	CAM-PB-PTZ-2	172.22.36.102	Exteriores puerta posterior edificio
3	**SUBSUELO 2**	CAM-S2-2	172.22.36.103	Exteriores de archivo
4		CAM-S2-3	172.22.36.104	Externa lagunas
5		CAM-S2-1	172.22.36.105	Archivo
6	**SUBSUELO 1**	CAM-S1-2	172.22.36.106	Parqueaderos ejecutivos
7		CAM-S1-1	172.22.36.107	Puerta parqueaderos ejecutivos
8		CAM-S1-3	172.22.36.108	Contabilidad gradas-archivo
9		CAM-S1-5	172.22.36.110	Puerta posterior contac center-contabilidad
10		CAM-S1-4	172.22.36.111	Seguridad-parqueaderos ejecutivos
28		CAM-S1-6	172.22.36.112	Cámara salida auditorio
11	**PLANTA BAJA**	CAM-PB-1	172.22.36.113	Pasillo gerencia Servicios Corporativos
12		CAM-PB-2	172.22.36.114	Pasillo tecnología
13		CAM-PB-4	172.22.36.115	Puerta terraza-financiero
14		CAM-PB-3	172.22.36.116	Baños planta baja
15		CAM-PB-6	172.22.36.117	Ingreso principal
16		CAM-PB-5	172.22.36.118	Baño proveedores-servicios
17		CAM-PB-7	172.22.36.119	Comercialización
18	**PRIMER PISO**	CAM-PP-1	172.22.36.120	Gerencia general
19		CAM-PP-2	172.22.36.121	Escaleras unidad de negocio
20		CAM-PP-4	172.22.36.122	Recepción
21		CAM-PP-3	172.22.36.123	Asuntos Responsabilidad Corporativa
22		CAM-PP-5	172.22.36.124	Pasillo auditoria-do-finanzas
23	**OUTLET**	CAM-OUT-2	172.22.36.125	Caja Oki-Doki
24		CAM-OUT-1	172.22.36.126	Ingreso Oki Doki – Produbanco
25	**COMEDOR**	CAM-CD-1	172.22.36.127	Comedor
27	**ARCHIVO**	CAM-EN-1	172.22.36.128	Archivo
26	**SIST. OPERATIVOS**	CAM-SIS-1	172.21.9.200	Sistemas Operativos

3.4.2 INSTALACIÓN DEL DRIVER DE INTEGRACIÓN.

El driver de integración de Video Edge – CCURE 9000 permite monitorear y controlar las cámaras, ver, reproducir, exportar y generar alarmas de video. Recibe estados y eventos en la estación de supervisión de CCURE 9000. Procedimiento de instalación:

- Click en CCURE_9000_Commend_VideoEdge4.0_Integration.exe.
- Click en “next” para continuar la instalación.
- Seleccione “I agree” en el acuerdo de licencia.
- Clic en la tecla de instalación.
- Cuando se ha completado la instalación aparece un mensaje que dice que inicie los servicios en CCURE 9000.
- Clic finalizar para completar la instalación.

3.4.3 CREACIÓN DE NVR EN CCURE 9000.

Para la creación del grabador de video seguir el siguiente procedimiento:

- Hacer clic sobre video para abrir las opciones de video, desde el panel de navegación de la estación de administración de CCURE 9000. Figura 3.24.

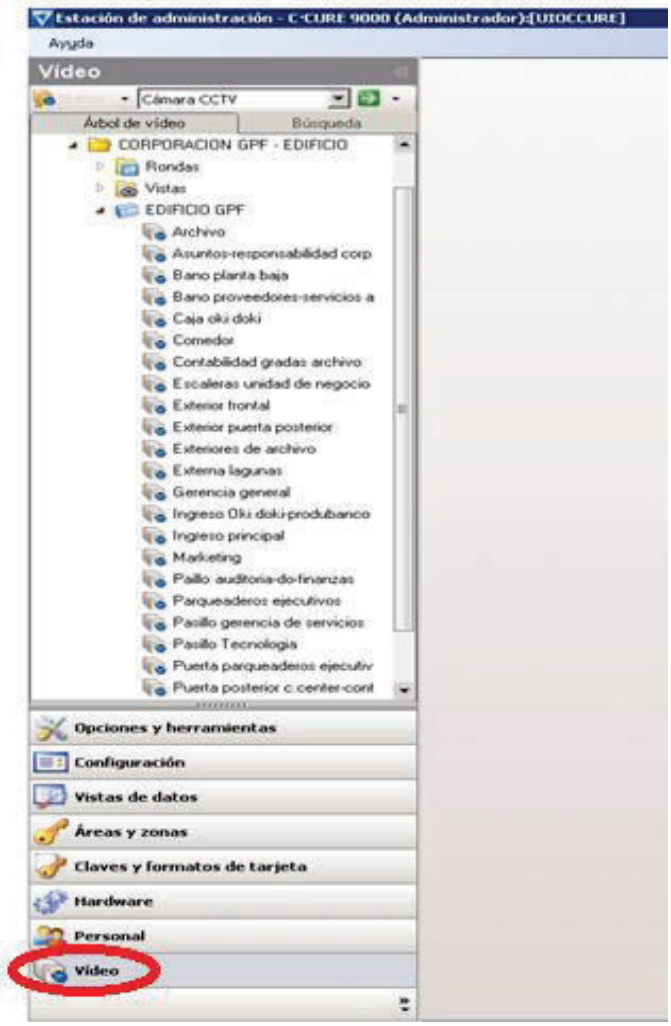


Figura 3.24 Creación del grabador de video.

- Expandir la estructura de árbol del panel de video. Hacer clic derecho sobre la carpeta company name y seleccionar Servidor Video Edge 4.0 y luego nuevo.
- Configura el servidor de video Edge desde el editor que se abre.
- Ingresar un nombre y hacer click en habilitar la opción para establecer comunicación entre CCURE 9000 y el servidor de Video. Figura 3.25.

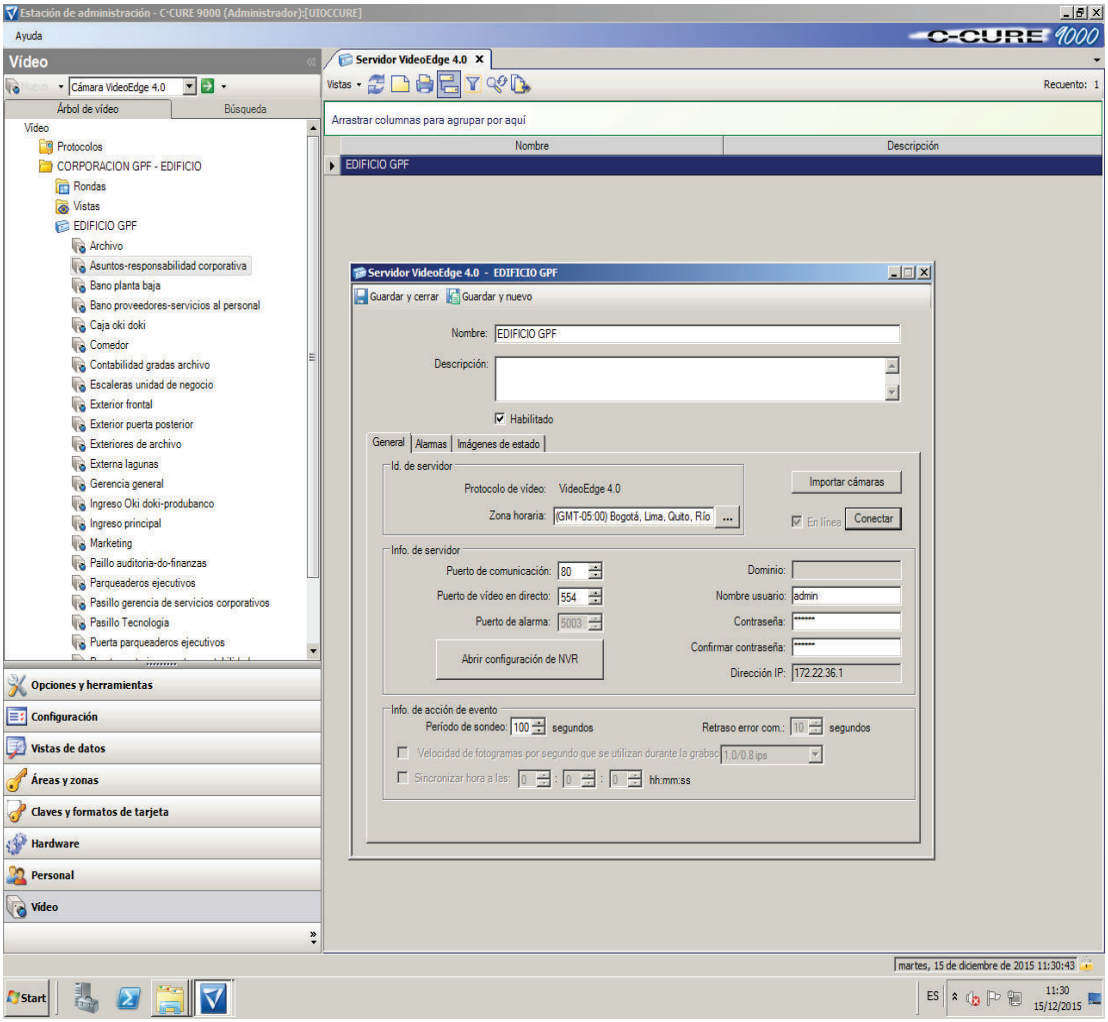


Figura 3.25 Editor de configuración de grabador de video.

- Llenar con los siguientes datos: dirección IP: 172.22.36.1, usuario: admin, clave: es9001.
- Después de terminar con la configuración, clic en guardar y cerrar.

3.4.3 CONFIGURAR ALARMAS PARA EL NVR.

Se configura alarmas para el grabador de video. De esta manera cuando ocurra una alarma, se visualiza el registro de la figura 3.26, en la estación de monitoreo.

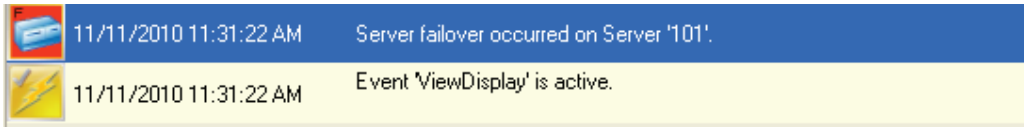


Figura 3.26 Alarmas en la estación de supervisión.

Procedimiento:

- Ir a alarmas en la ventana de configuración del NVR, seleccionar una propiedad, un valor y una acción. Figura 3.27.

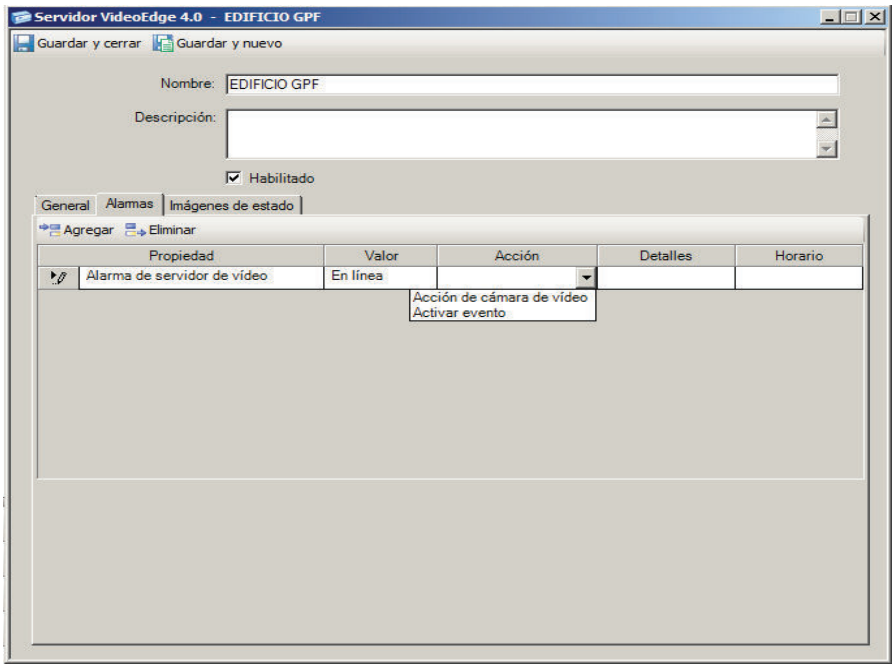


Figura 3.27 Configuración NVR.

Es decir, a cualquier momento (horario siempre), la alarma del servidor de video (propiedad) es igual a online (valor), activar el evento (acción) llamado mostrar. Tabla 3.3.

Tabla 3. 7 Trigger de cámaras.

Propiedad	Valor	Acción	Detalles	Horario
Estado servidor video	Online	Activar evento	Mostrar	Siempre

3.5 CONFIGURACIÓN SISTEMA DE INTRUSIÓN.

3.5.1 CONFIGURACIÓN TARJETA IT-100 Y LANTRONIX UDS 1100.

El departamento de sistemas de la corporación GPF asignó ciertas direcciones IP a los convertidores Lantronix. Tabla 3.8

Tabla 3. 8 Direcciones IP Centrales de Intrusión.

Lantronix	DIRECCIÓN IP
Consola Seguridad	172.22.50.22
Archivo	172.22.50.24
Casa estudio	172.22.50.26

Seguir el siguiente procedimiento para la configuración:

- Abrir el Buscador web y colocar la dirección 172.18.11.190 en la barra de direcciones. Esta es una dirección de default. El dispositivo USD1100 solicita un usuario y contraseña. Dejar los espacios en blanco y presionar OK.
- El administrador Web se despliega. Seleccionar Channel 1> serial settings (ajustes manuales) del menú de la izquierda.
- En ajustes seriales (serial settings) se configura la velocidad de transmisión, bits de datos, paridad, bits de parada y control de flujo. Figura 3.28.

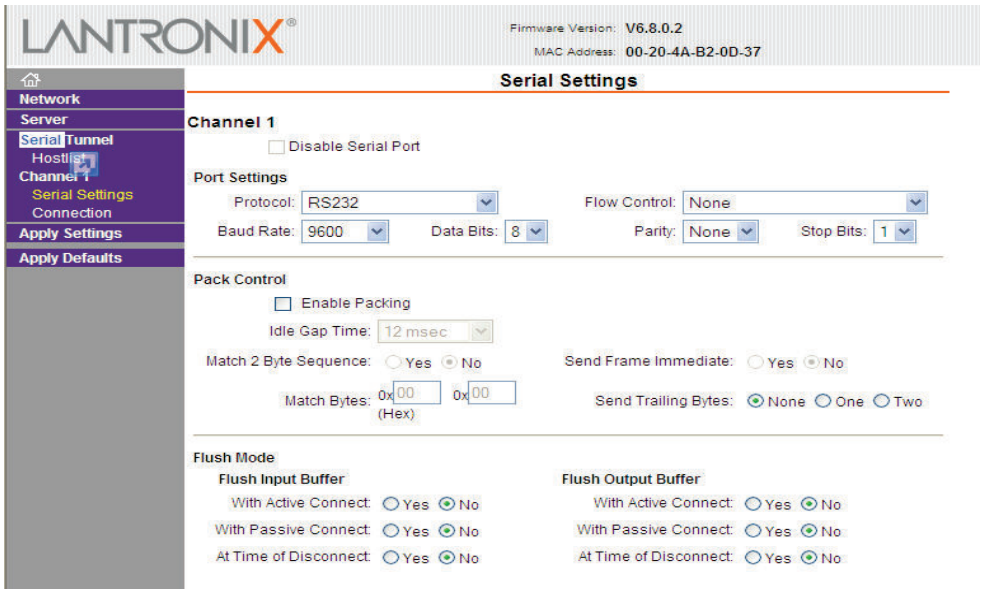


Figura 3.2810 Ajustes Seriales.

- Luego hacer clic en connection y configurar de acuerdo a la figura 3.29.

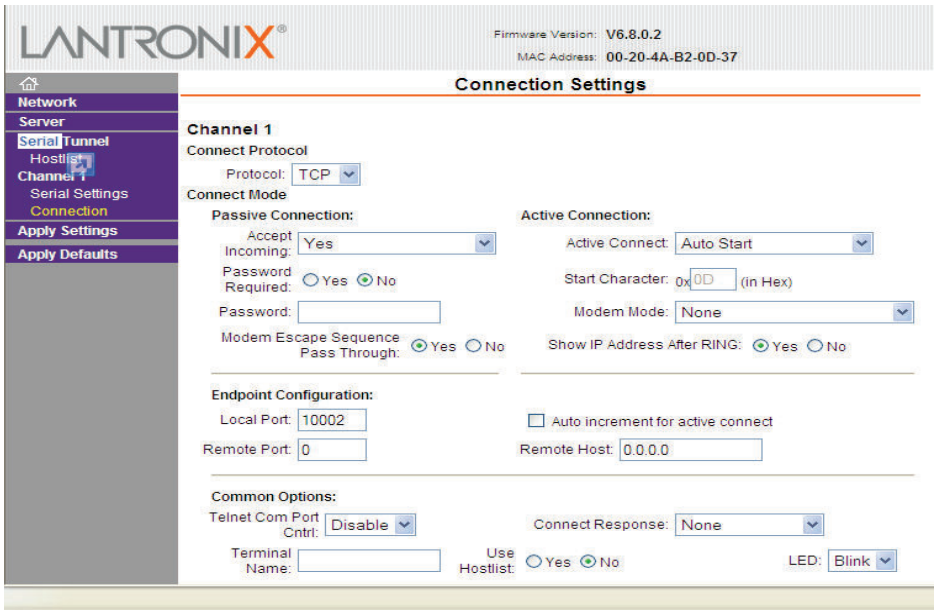


Figura 3.29 Ajustes de conexión.

- Seleccionar Network del menú principal de la izquierda. Se despliega la página de ajustes de configuración de red (network). Colocar la dirección IP 172.22.50.22. Figura 3.30.

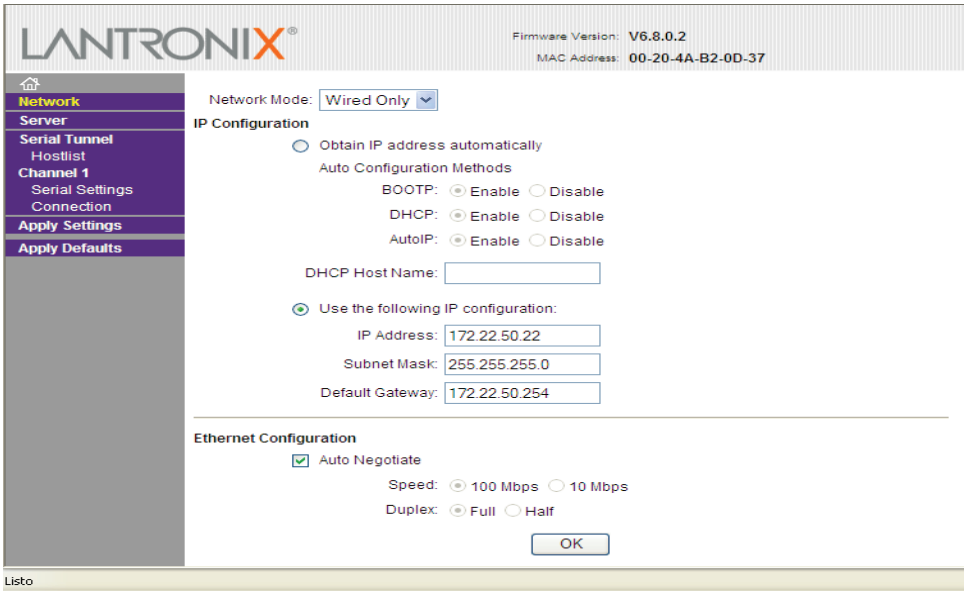


Figura 3.30 Ajustes de red.

En la Figura 3.31 se describe la configuracion del LANTRONIX

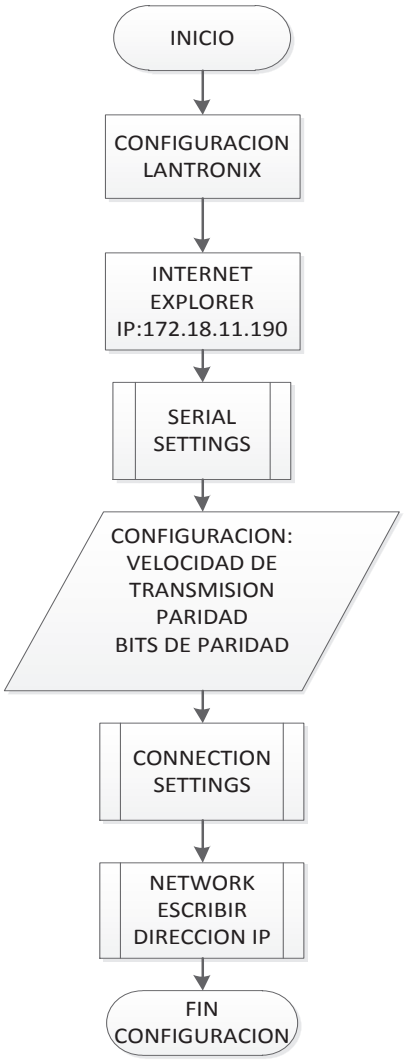


Figura 3.31 Configuracion Lantronix

3.5.3 INSTALACIÓN DEL DRIVER DE INTEGRACIÓN.

El driver de integración CCURE 9000 – DSC permite supervisar los dispositivos del sistema de intrusión a través de la estación de supervisión. Monitorea el estado, arma y desarma particiones desde la estación de administración.

Características

- Soporta la gestión remota a través del dispositivo Lantronix UDS 1100.
- Revisa partición y estado de zona.

- Arma y desarma partición.
- Teclado virtual.
- Implementa partición de armado/desarmado, alarma de incendio, auxiliar y pánico.

Seguir los siguientes pasos para instalar el driver de integración:

- Doble click sobre DSCPowerSeriesIntegration.exe.
- El programa de instalación determina si la versión de CCURE 900 instalada en la PC es la requerida.
- La pantalla de inicio de instalación aparece. Presionar siguiente.
- Click aceptando los términos de la licencia y luego siguiente.
- Seleccionar credenciales de autenticación de Windows de usuario actual
- Click siguiente para continuar con la instalación.
- Click finalizar para completar la instalación, y usar la aplicación del servidor de administración para iniciar los servicios de Crossfire.

3.5.4 CREACIÓN CENTRAL DE DSC.

El panel DSC en CCURE 9000, se refiere al hardware real DSC. El panel de dialogo DSC puede ser importado a CCURE 9000. Una vez importado el cuadro de diálogo se mostrará la versión del software, la partición y la información de las zonas.

- En el panel de navegación de la estación de administración del CCURE 9000, hacer click en Hardware.
- Clic derecho en la carpeta Company name.
- Seleccionar Panel DSC y clic en nuevo. Figura 3.32.

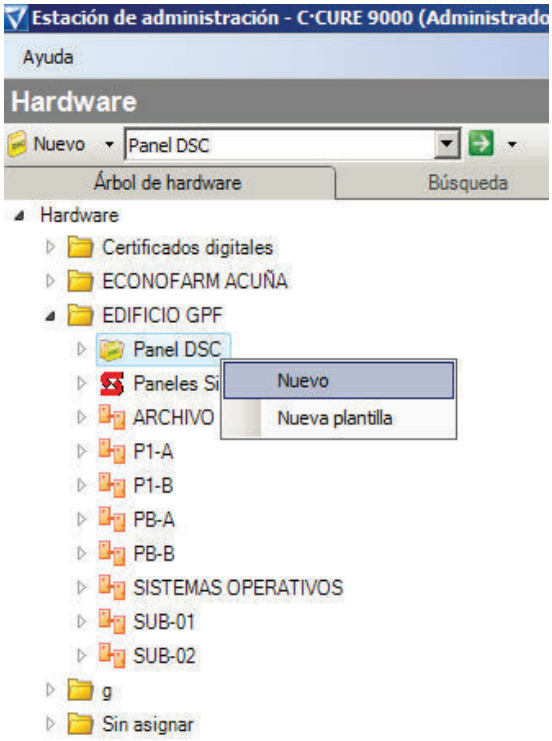


Figura 3.112 Creación panel DSC.

- Se abre el editor del panel DSC. Ingrese un nombre para el panel.
- Ingrese la información de comunicación. Verifique el puerto de red, dirección IP y puerto TCP.
- Click guardar y cerrar.

3.5.5 ACCESO AL PANEL DSC.

En el panel de navegación de la estación de administración del CCURE 9000, presionar botón de funciones, seleccionar hardware para acceder al panel de navegación Figura 3.39.

Una vez ingresado al panel DSC, se accede a un cuadro de diálogo que tiene la posibilidad de ingresar los parámetros necesarios para la integración del Sistema de Intrusión por medio del CCURE 9000. Figura 3.33

Figura 3.33 Acceder al panel DSC.

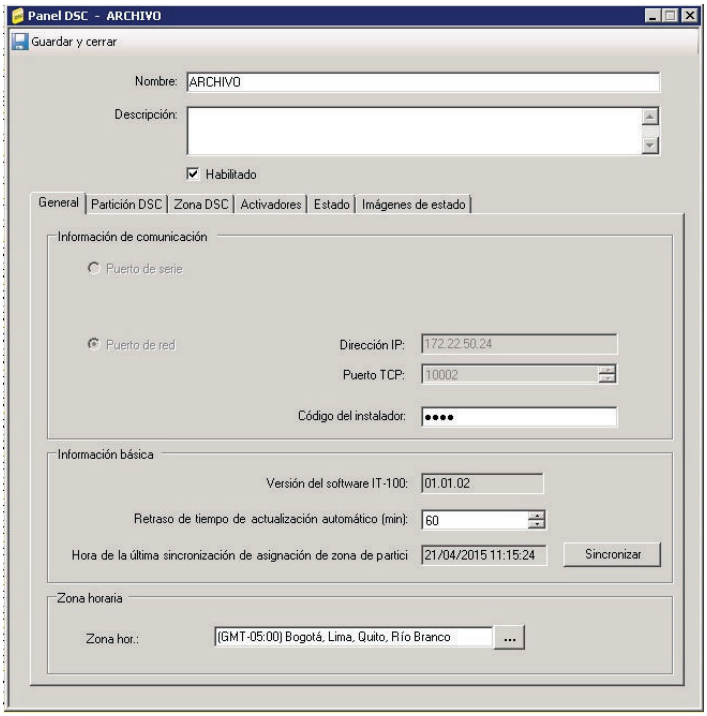


Figura 3.3412 Cuadro de dialogo Panel DSC.

En el cuadro de diálogo se puede modificar:

- General
    - Nombre del Panel
    - Información de comunicación:
        - Puerto Red (Dirección IP, Puerto TCP) o,
        - Puerto serie
- Partición DSC

La Partición es la distribución de zonas con los diferentes elementos como sensores, contactos magnéticos dependiendo de la necesidad que se requiera en cada departamento o área específica.

- Zona DSC

La zona DSC permite mirar una información básica de las zonas en el panel Nombre: Muestra el nombre de la zona

- Número: Muestra el número de la zona
- Status: Muestra el status de la zona

- **Activadores**

La pestaña Activadores, permite configurar activadores, procedimientos configurados usados por CCURE 9000 para activar acciones específicas cuando ocurre una determinada condición predefinida

La pestaña contiene una acción, “Activar evento”, que se puede vincular a un valor de estado de una importación de datos específica y a cualquier evento configurado en el sistema. Cuando el estado de la importación coincide con uno de estos valores, se activa la acción “Activar evento” vinculada y el evento definido por el usuario establece en un estado activo (si el evento lo permite, que debe ser armado en ese momento). Normalmente, se utilizaría el evento activado para enviar mensajes a la Consola de Seguridad cuando una importancia tenga un estado determinado, como “Desconectado” o “Error de conexión”.

- Estado

El Estado, nos permite verificar:

  - Estado en línea: **En línea** correcto funcionamiento
  - Estado de problema
  - Estado de sabotaje
  - Estado de comunicación

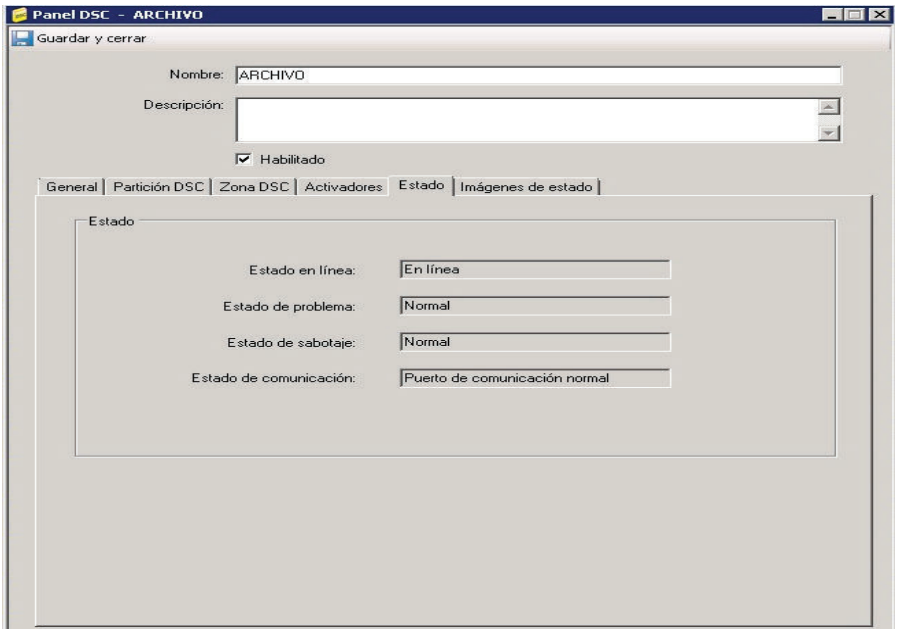


Figura 3.35 Panel DSC- Estado.

- **Imágenes de Estado**

Imágenes de Estado, en la zona DSC nos proporciona un medio para cambiar las imágenes por defecto para indicar el estado de la zona en la Consola de Seguridad Figura 3.36.

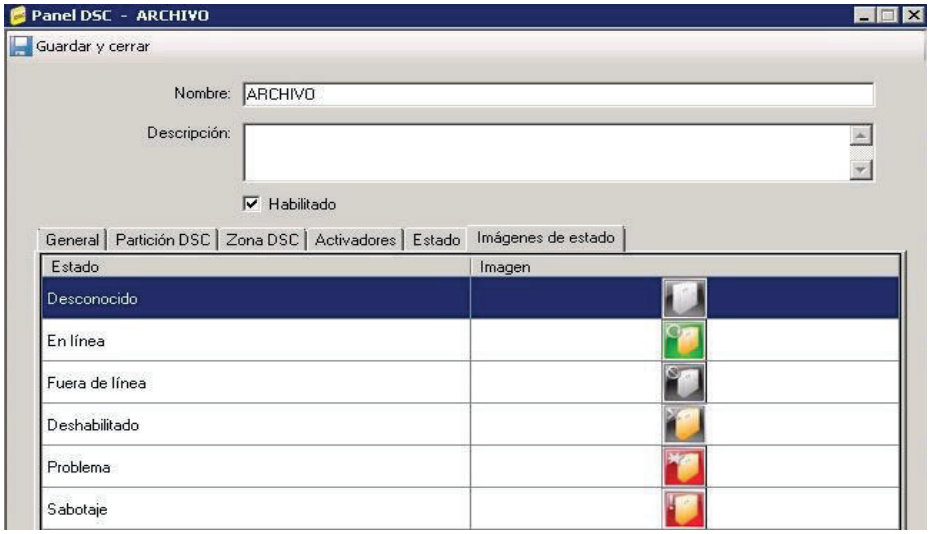


Figura 3.36 Estado de Imágenes.

CAPÍTULO 4

PRUEBAS Y RESULTADOS

En el desarrollo de éste proyecto se realizan algunas pruebas conjuntamente con sus avances. Éstas permiten tomar decisiones para actualizar el hardware de ser necesario y ajustar el diseño final.

4.1 PRUEBAS DE COMUNICACIÓN.

El servidor de CCURE 9000 debe tener comunicación con el sistema de detección de incendios, CCTV e intrusión a través del protocolo TCP/IP. Se utiliza el comando ping, que se suministra como una prestación estándar de la mayoría de los sistemas operativos. El ping permite enviar paquetes de datos a un equipo en una red y evaluar el tiempo de respuesta.

- Seleccionar Inicio > Ejecutar > cmd para mostrar la solicitud de comando.
- En la solicitud, introduzca el comando siguiente: ping [dirección IP o nombre]

Si el ping se realiza correctamente, se obtendrá un mensaje de tipo “Reply from”, mientras que los intentos no válidos devolverán mensajes indicando que se ha terminado el tiempo de respuesta o que no se puede obtener el acceso al host.

Las figuras 4.1, 4.2, 4.3 y 4.4 indican la comunicación con cada sistema.

- Sistema detección de incendio.

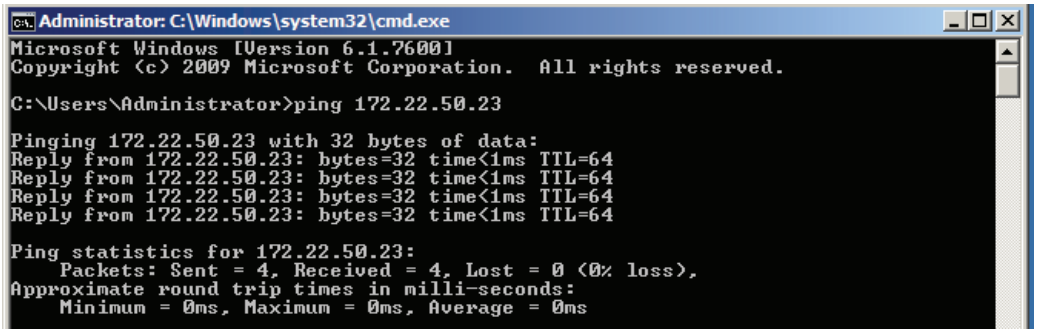


Figura 4.1 Comunicación con lantronix UDS 1100 del sistema de incendio.

- Sistema CCTV.

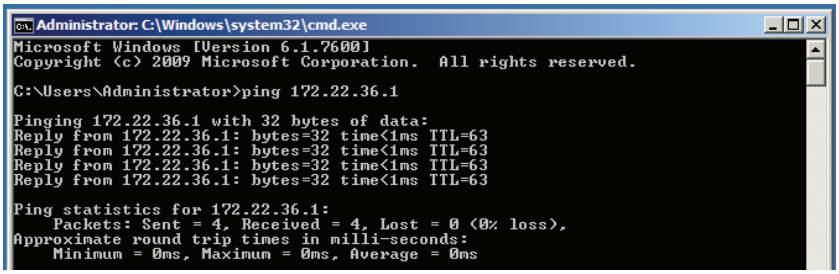


Figura 4. 2 Comunicación con el NVR.

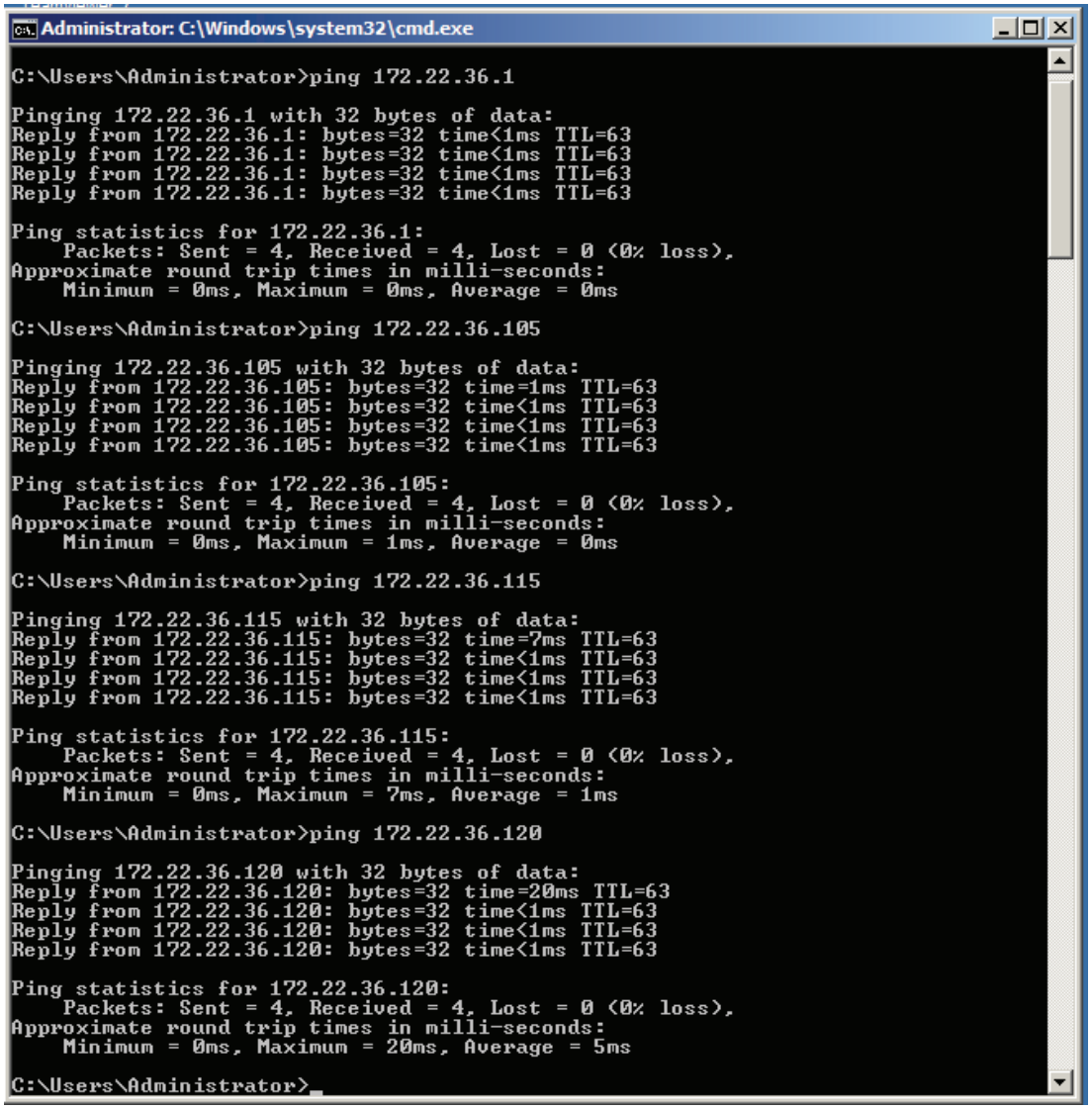


Figura 4. 3 Comunicación con las cámaras IP.

- Sistema de intrusión.

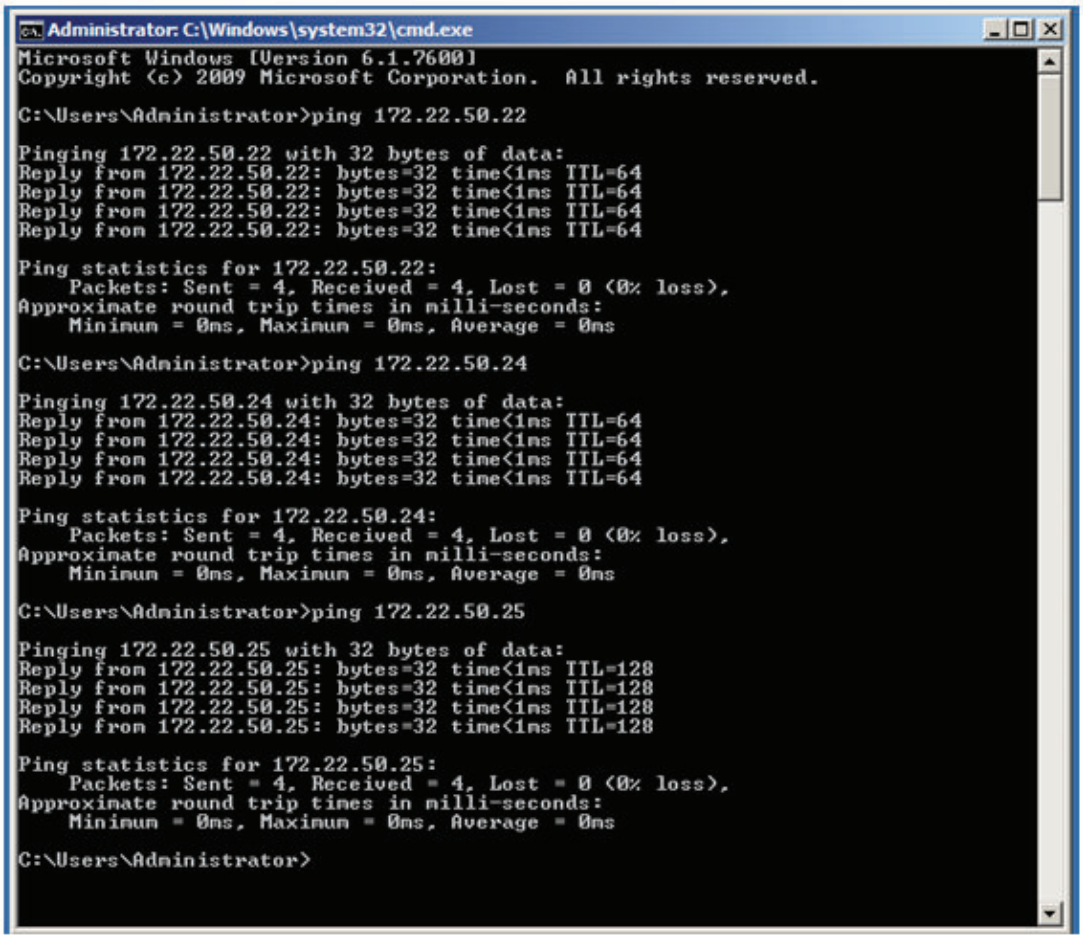


Figura 4. 4 Comunicación con los lantronix UDS 1100 de las centrales de intrusión.

Adicional se comprueba el estado de comunicación con cada sistema desde la estación de administración de CCURE 9000.

En las figuras 4.5, 4.6 y 4.7 se muestran los tres sistemas en línea.

- Sistema detección de Incendio.

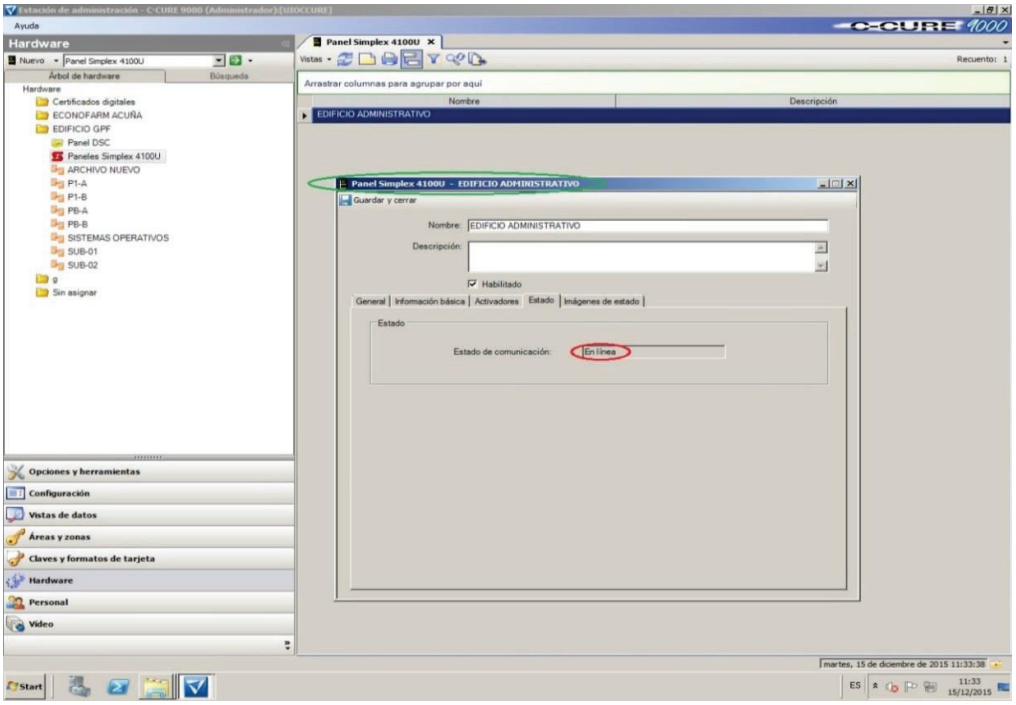


Figura 4. 5 Estado del panel de detección de Incendios.

- Sistema CCTV.

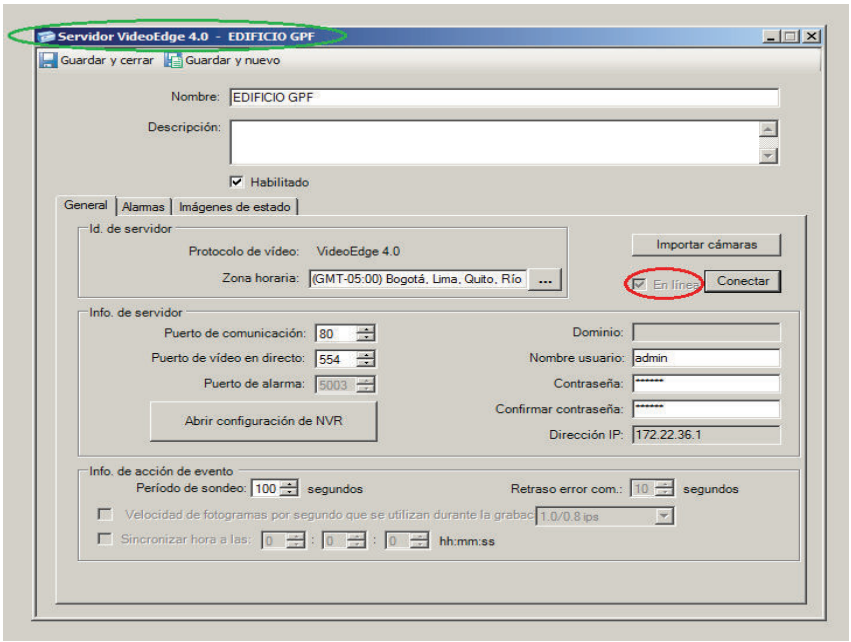


Figura 4. 6 Comunicación servidor de video.

- Sistema de Intrusión.

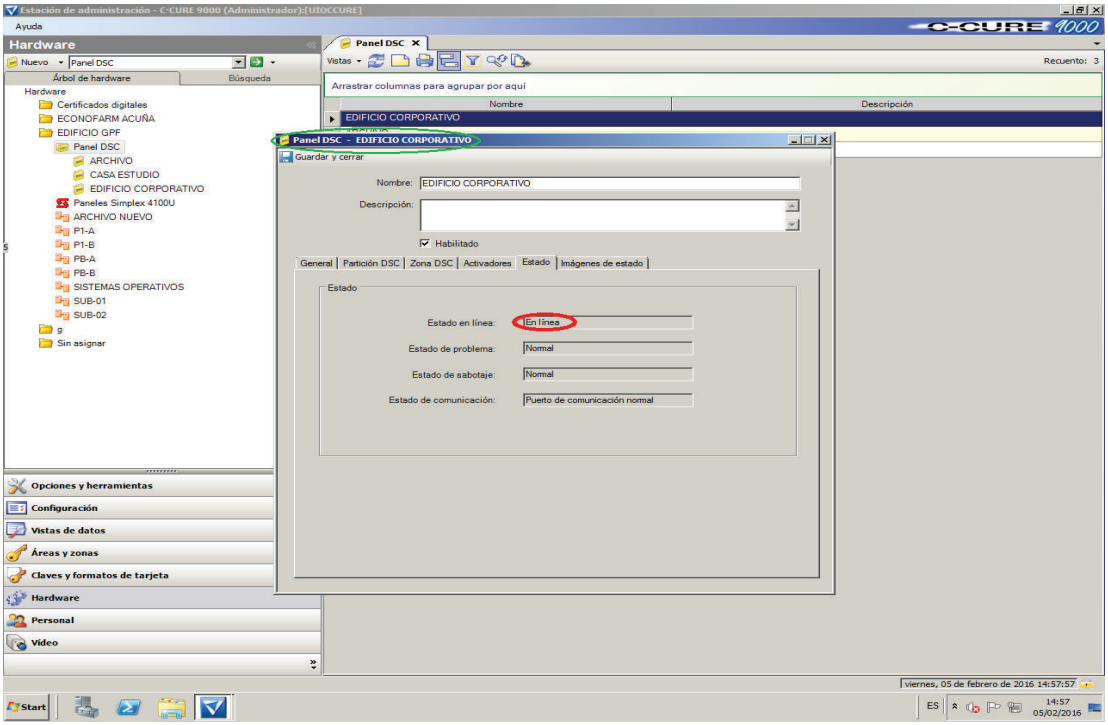


Figura 4. 7 Panel DSC en línea.

4.2 PRUEBAS DETECTANDO PROBLEMAS.

La estación de supervisión es una interfaz gráfica que permite a los operadores interactuar con el sistema. En ésta se muestra los cambios de estado de los dispositivos involucrados.

Se realiza pruebas retirando las cabezas de los sensores, dando como resultado que el sistema lo reconoce como problema y lo muestra en el visor de actividades de la estación de supervisión. Figura 4.8.

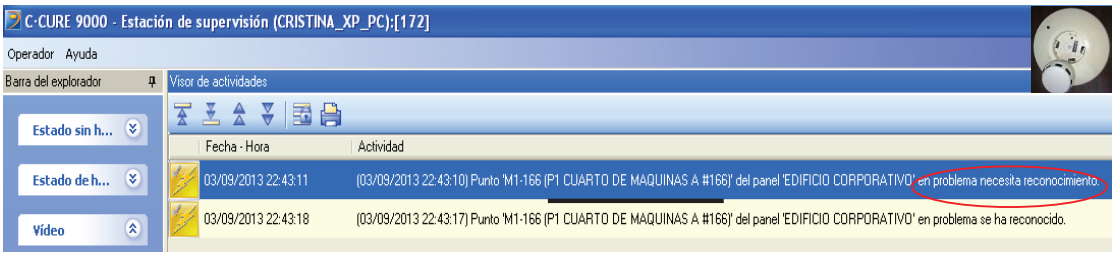


Figura 4. 8 Dispositivo en problema en visor de actividades.

El operador lee la actividad y de inmediato sabe con exactitud el lugar, piso y dispositivo que está presentando el problema. Cuando el problema ha sido solucionado, en este caso se ha vuelto a colocar la cabeza del sensor, se muestra en el visor de actividades que el dispositivo esta normal. Figura 4.9.

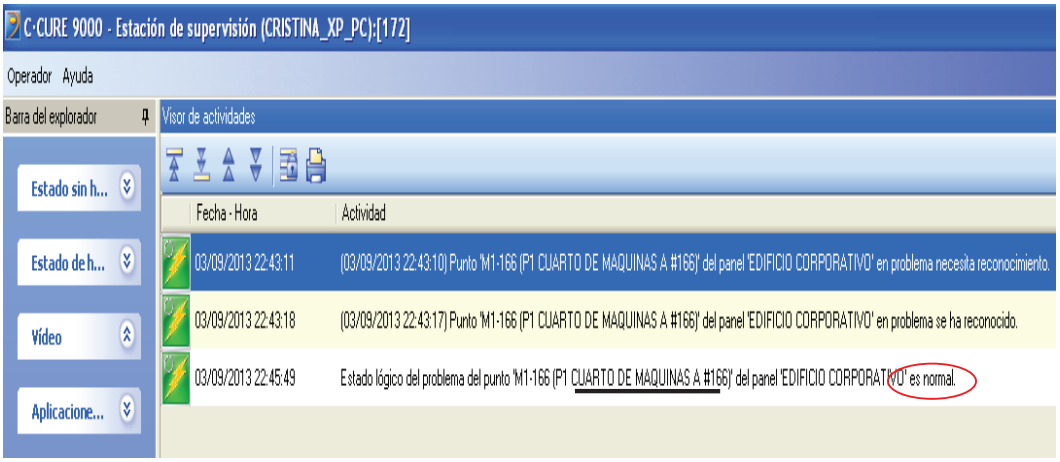


Figura 4. 9 Dispositivo normal en visor de actividades.

4.3 PRUEBAS ACTIVANDO SENSORES.

En el caso de un incendio se activan automáticamente los sensores de la edificación. Se utiliza un imán con el objeto de realizar pruebas, este dispositivo obliga al sensor a activarse. Inmediatamente se visualiza en la ventana de supervisión que hay una alarma de incendio, la misma que cambia a estado normal después de que se haya retirado el humo o se ha desactivado el sensor. Figura 4.10.

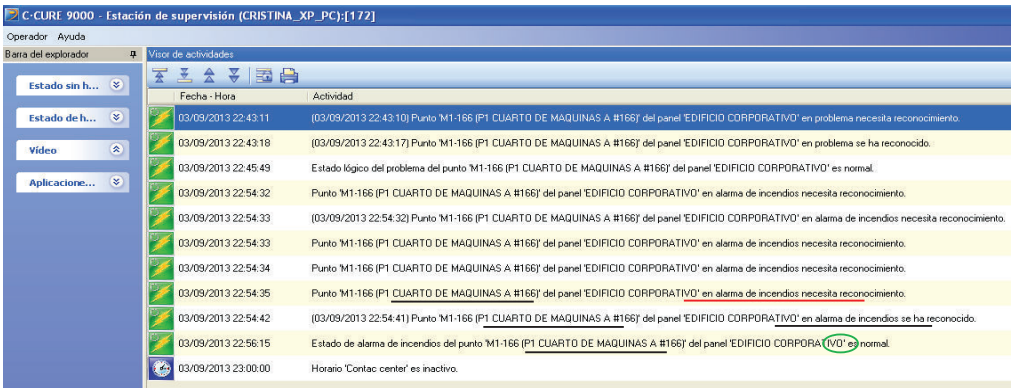


Figura 4. 10 Dispositivo en alarma en visor de actividades.

4.4 PRUEBAS PROVOCANDO EVENTOS.

Para comprobar que están bien configurados los eventos se activa un sensor. El dispositivo inmediatamente cambia de color verde a color rojo, indicando que está activo y se despliega una ventana emergente indicando la cámara más cercana. Figura 4.11.

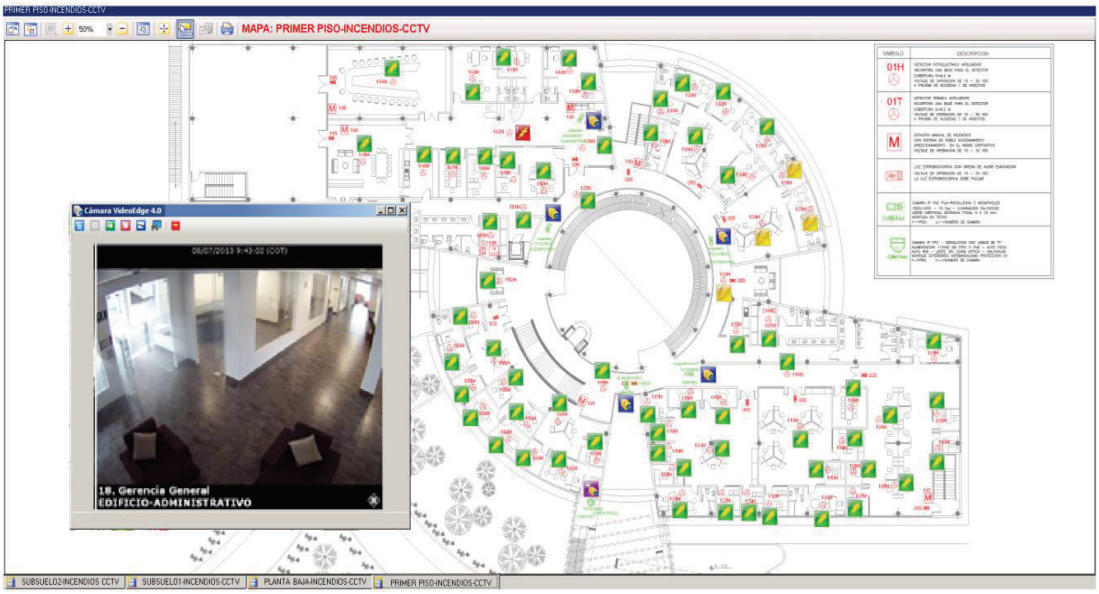


Figura 4. 11 Eventos programados.

4.5 PRUEBAS CAMBIANDO EL ESTADO DE DISPOSITIVOS.

Los dispositivos de detección de incendio en funcionamiento normal se despliegan de color verde (figura 4.12). Si estos se deshabilitan (figura 4.13) se muestran de color amarillo. Cuando están de este color quiere decir que no están funcionando, que intencionalmente se los puso en ese estado para realizar algún trabajo en esa área y con esto evitar falsas alarmas.

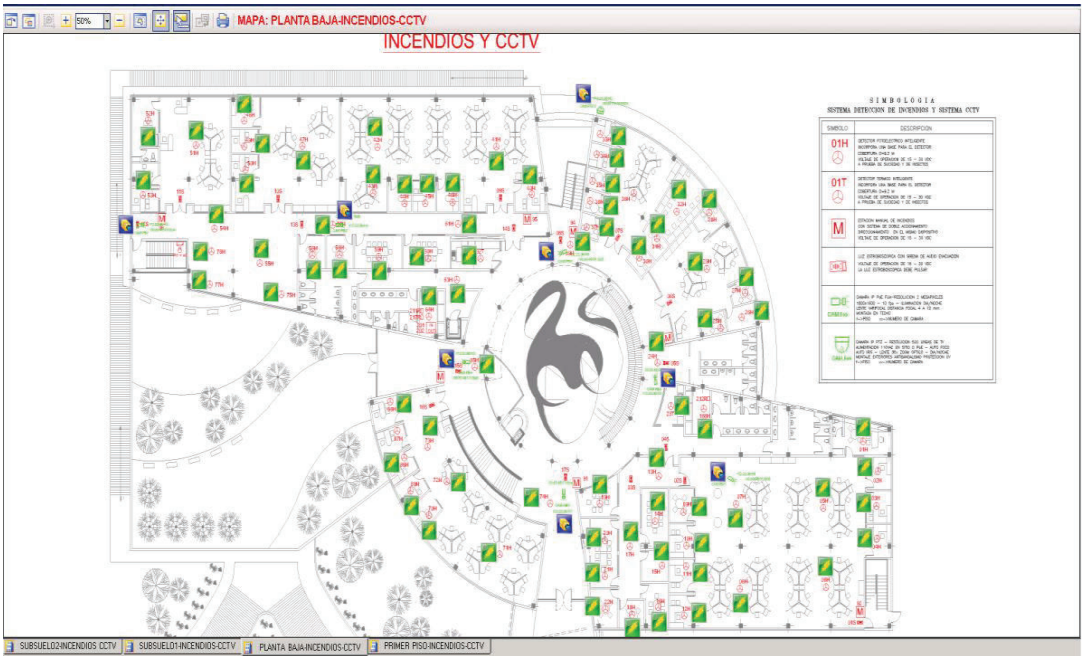


Figura 4. 12 Plano planta baja con sensores habilitados.

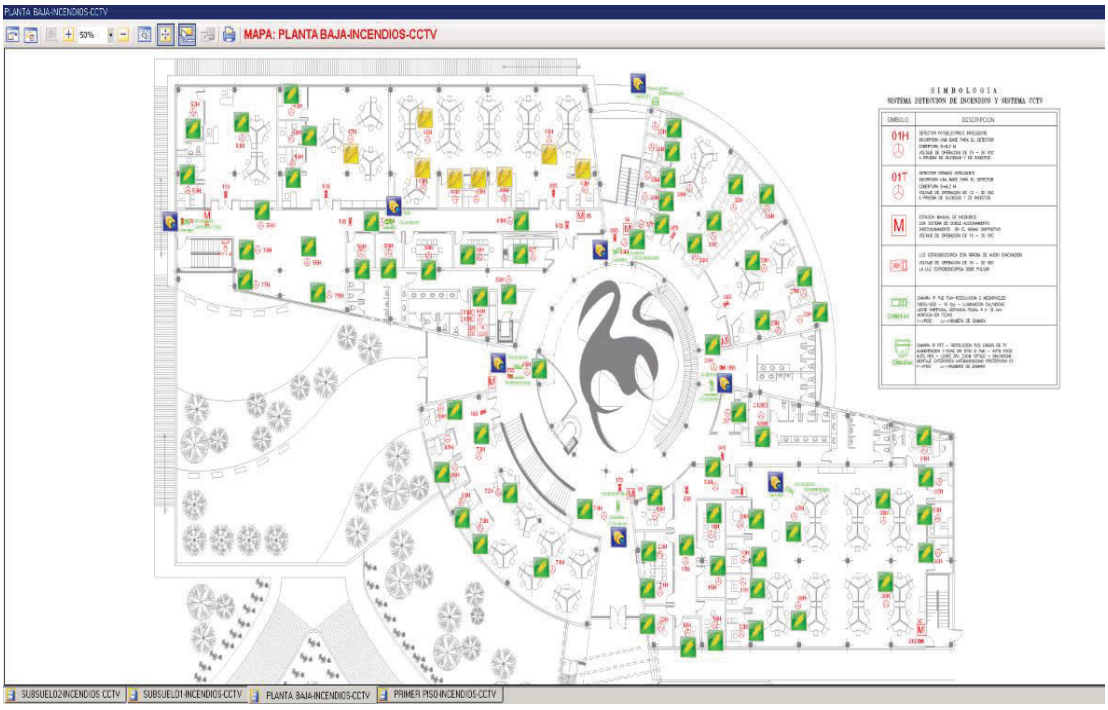


Figura 4. 13 Plano planta baja con sensores deshabilitados.

Los dispositivos de intrusión y control de acceso muestran sus símbolos de color azul y verde cuando las puertas se encuentran cerradas y los sensores inactivos. Caso contrario se visualizan de color rojo.

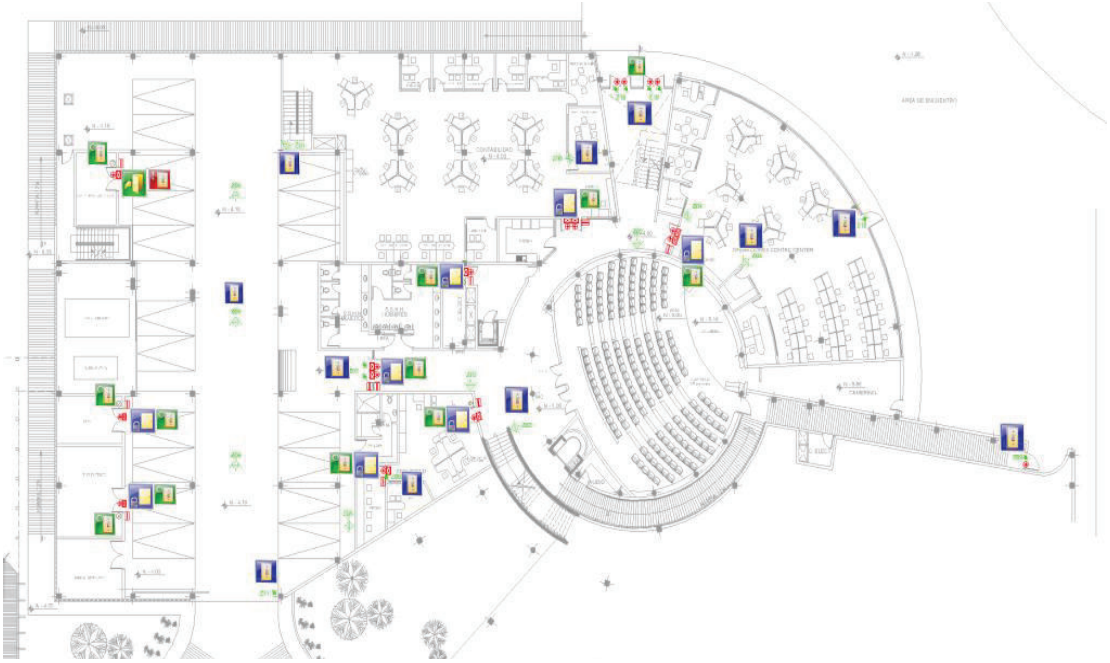


Figura 4. 14 Estado de los dispositivos de intrusión y control de acceso.

4.2 PRUEBAS DE TODOS LOS SISTEMAS.

Se realiza una inspección física de la instalación, recorriéndola desde el primer punto hasta el último. Primero es necesario verificar el funcionamiento de cada sistema independiente, tomar datos y realizar un registro. Con esto se verifica que la instalación haya sido bien realizada y cumple con los estudios y especificaciones inherentes del proyecto.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES.

Las conclusiones se han dividido en conclusiones generales y específicas, siendo generales las que se han logrado obtener al finalizar el proyecto aquí mostrado, en tanto las conclusiones específicas son el resultado obtenido en el transcurso del mismo.

5.1.1 CONCLUSIONES GENERALES.

- El proyecto realizado cumple con los objetivos propuestos inicialmente que son la integración de un sistema centralizado de seguridad electrónica con la utilización de tecnología IP para el edificio de la Corporación GPF. Adjunto al trabajo se ha armado el hardware necesario para incorporar a la red los sistemas de detección de incendio, CCTV, e intrusión.

- El sistema implementado en el presente proyecto ha sido realizado para aprovechar el software gestor de eventos CCURE 9000, del sistema de control de acceso, e integrar los sistemas de seguridad existentes en el edificio de la Corporación GPF. Con esto se consigue la visualización de estos sistemas de seguridad desde una misma plataforma.

- El sistema integrado de seguridad electrónica realizado en este proyecto de titulación logra centralizar los eventos de cuatro sistemas en un solo software, agilita al operador para una respuesta rápida y permite que pueda controlar desde un solo lugar, los eventos de cuatro sistemas que ocurren simultáneamente.

- El sistema realizado en este proyecto de titulación logra integrar los sistemas de control de accesos, detección de incendios, CCTV e intrusión, los mismos que están colocados en el edificio pero que no están operativos.

- La integración de sistemas de seguridad permite que por medio de planos se visualicen las alarmas de detección de humo y a la vez, se desplegarán cámaras de video cercanas a la zona donde se produjo el incidente.

- La comunicación de los sistemas de seguridad es realizada usando el protocolo TCP-IP, con la ayuda de convertidores de comunicación serial a Ethernet (lantronix), para el caso de los equipos de detección de incendios y, tarjetas IT-100 - lantronix para el sistema de intrusión.

- El único elemento que permite el ingreso a las edificaciones es la tarjeta de proximidad otorgada por personal de Seguridad Física

5.1.2 CONCLUSIONES ESPECÍFICAS.

- Cuando la implementación física y el cableado ha estado a cargo de otra empresa, es indispensable comprobar detalladamente las conexiones hechas para tener la certeza que el sistema responda de acuerdo a lo esperado.

- El personal de Seguridad es el único que puede activar tarjetas y asignar horarios y niveles de ingreso a las diferentes áreas del edificio dependiendo del personal que lo solicite (personal de mantenimiento, proveedores, personal administrativo, etc.)

- Las versiones del firmware y software son indispensables al momento de integrar sistemas de seguridad. No todas las versiones son compatibles. Es necesario tener un registro de las versiones existentes e instalar solo las adecuadas.

- El software CCURE 9000 permite desbloquear puertas en caso de algún evento inesperado, para que el personal administrativo logre salir con facilidad a los puntos de encuentro ubicados a las afueras del Edificio Corporativo.

- En caso de activacion de algun dispositivo (sensor de humo, estacion manual, sensor de calor, magnetico, etc), en el mapa se va a poder identificar el dispositivo accionado.

- Todos los dispositivos del sistema contraoncendios son direccionables, es decir al instante que se active, el apnel identifica exactamente cual fue el dispositivo que se acciono.

5.2 RECOMENDACIONES.

- El personal de mantenimiento debe ser capacitado en el manejo del Software CCURE 9000, ya que es una herramienta muy poderosa en la que permite realizar muchas acciones que están implementadas en el edificio.

- Es indispensable que se establezca un cronograma de mantenimiento de todos los sistemas de seguridad instalados en el Edificio Corporativo para asegurar su correcto funcionamiento.

- Para mayor seguridad y confianza se recomienda actualizar continuamente los planos en la base de datos. Esto debido a que, por ampliación de áreas pueden variar los datos que se tienen en la actualidad.

- Los cuartos eléctricos deben estar totalmente ventilados (equipos de A/C), principalmente el cuarto eléctrico del primer piso lado A, donde se encuentra el servidor del CCURE 9000. Ya que el excesivo calor en el lugar puede ocacionar daños en los equipos.

- Se debe realizar una buena instalación a tierra e instalar protectores atmosfericos, ya que en el sector en donde se encuentra el edificio de la Corporación GPF existe gran cantidad de descargas atmosféricas, las cuales suelen producir daño a los dispositivos electrónicos como camaras, paneles, etc

- Se recomienda utilizar un monitor adicional para poder tener una visualización de los mapas en las que están los sistemas integrados.

- Al realizar trabajos de adecuaciones en el edificio se debe deshabilitar los dispositivos de detección de humo en las áreas intervenidas, ya que se pueden activar y dar falsas alarmas de evacuación

- Se debe capacitar a los brigadistas la activación y el significado de los dispositivos de emergencia que están instalados en lugares estratégicos del Edificio, (estación manuales y luces estroboscópicas) en caso de existir un evento como es un incendio o un terremoto

- Se recomienda que el mantenimiento del Sistema de Detección y Control de Incendio se lo debe realizar fuera de la jordana laboral con el fin de evitar alguna activación por error y crear un caos en el personal administrativo.
- Todo el Sistema Electronico de Seguridad debe estar conectados a energia regulada proporcionada por un UPS

REFERENCIAS BIBLIOGRAFICAS

[1] G.F.CEVALLOS, «https://sites.google.com/site/seguridadelectronicagcm/capitulo-1,» [En línea].

[2] GLOBENET INTERNACIONAL, «BLOG GLOBENET,» 2014. [En línea]. Available: https://www.globenetcorp.com/es/blog/sistema-detector-incendios/. [Último acceso: 12 06 2015].

[3] SEGURIDAD ELECTRONICA, «ADEATEL,» BOSCH, 01 06 2015. [En línea]. Available: http://www.adeatel.net/soluciones/seguridad-electronica/edificios-inteligentes. [Último acceso: 15 08 2015].

[4] DEFINICION DE, «DEFINICION.DE,» 2008. [En línea]. Available: http://definicion.de/ip/. [Último acceso: 15 04 2015].

[5] SISTEMAS DE SEGURIDAD A1, «SEGURIDADE A1,» Runa DC, 2013. [En línea]. Available: http://www.seguridadea1.com/index.php/ingenieria-proyectos/integracion. [Último acceso: 05 02 2015].

[6] TECNO CONTROL Y SISTEMAS S.A DE C.V, «TS,» [En línea]. Available: http://www.tecnocontrol.mx/servicios/integraci%C3%B3n-de-sistemas/. [Último acceso: 04 05 2015].

[7] CONTROL DE ACCESOS, «Elementos de Identificacion,» rnds, [En línea]. Available: http://www.rnds.ar.com.

[8] SIMPLEX, «Sensores direccionables,» 2011. [En línea]. Available: www.simplexgrinnell.com. [Último acceso: 05 05 2014].

[9] AMERICAN DYNAMICS, «ILUSTRA 600/610,» *Guia de instalación y operación,* vol. 03, p. 12, 2010.

[10] CCURE 9000 - SOFTWARE HOUSE, «<<Guia de configuracion de Hardware>>,» 20 7 2015. [En línea]. Available: http://www.swhouse.com.

[11] SOFTWARE HOUSE, «Guía de instalación y actualización,» *CCURE 9000 VERSION 2.1,* pp. 1-10, 2012.

ANEXOS

ANEXO A

DIAGRAMAS UNIFILARES SISTEMAS DE SEGURIDAD

Diagrama unifilar Sistema Control de Accesos lado A.

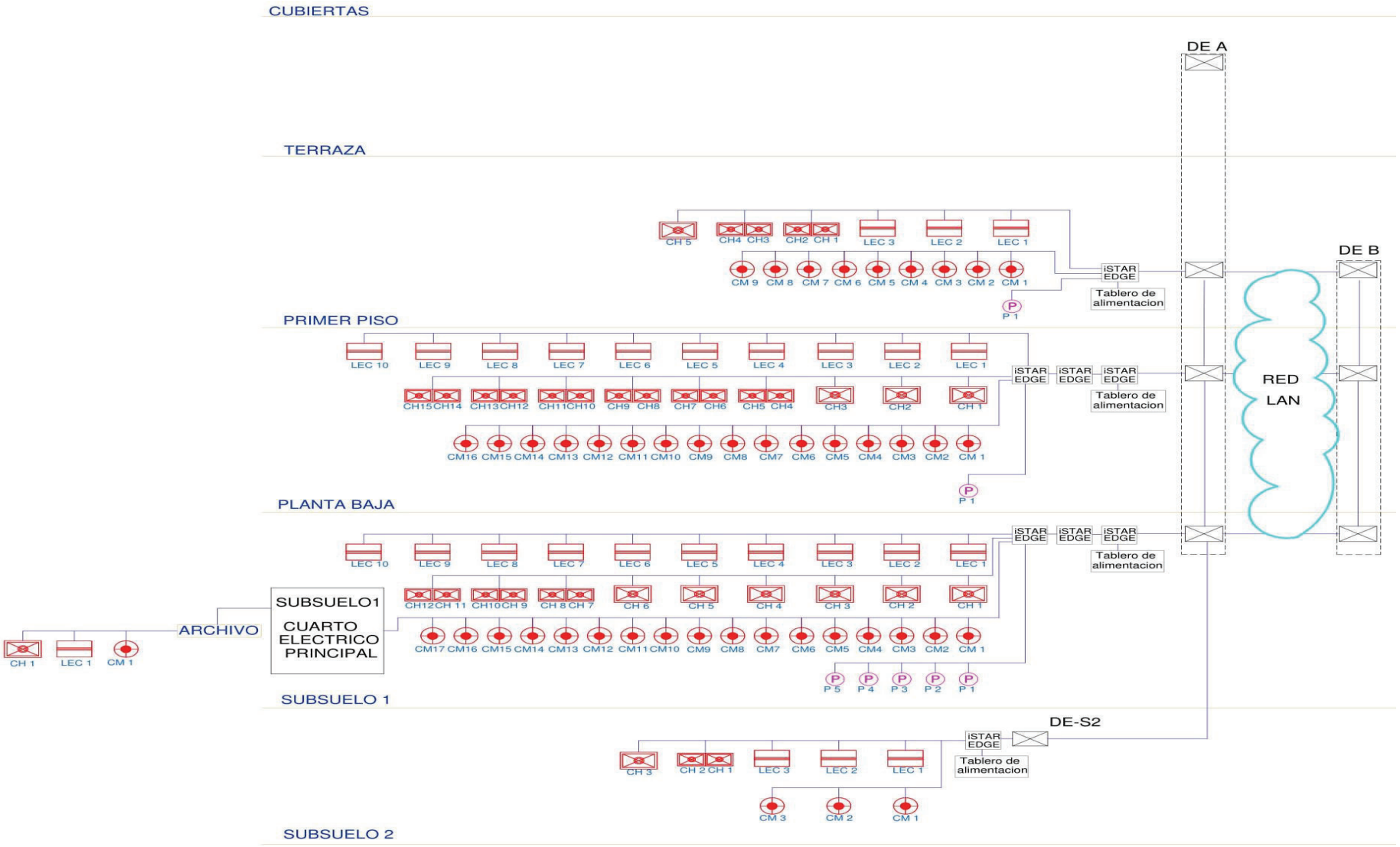


Diagrama unifilar Sistema Control de Accesos lado B.

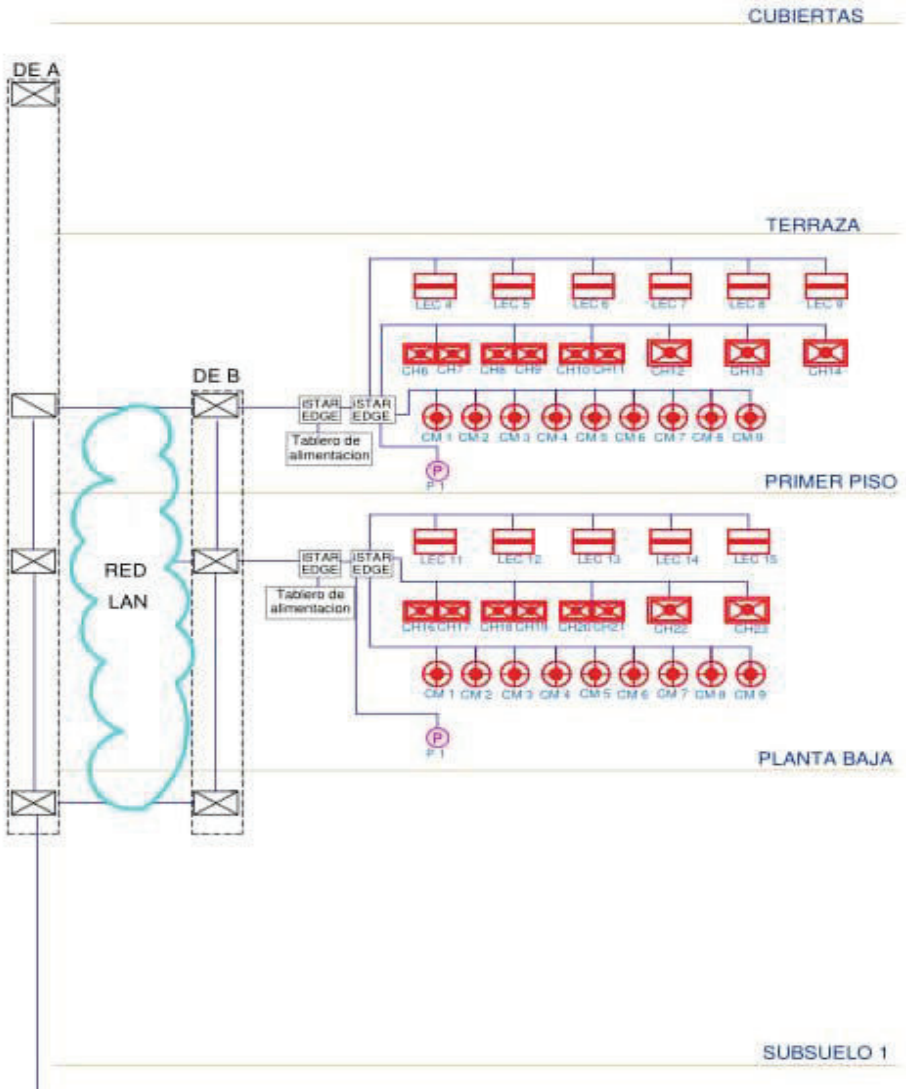
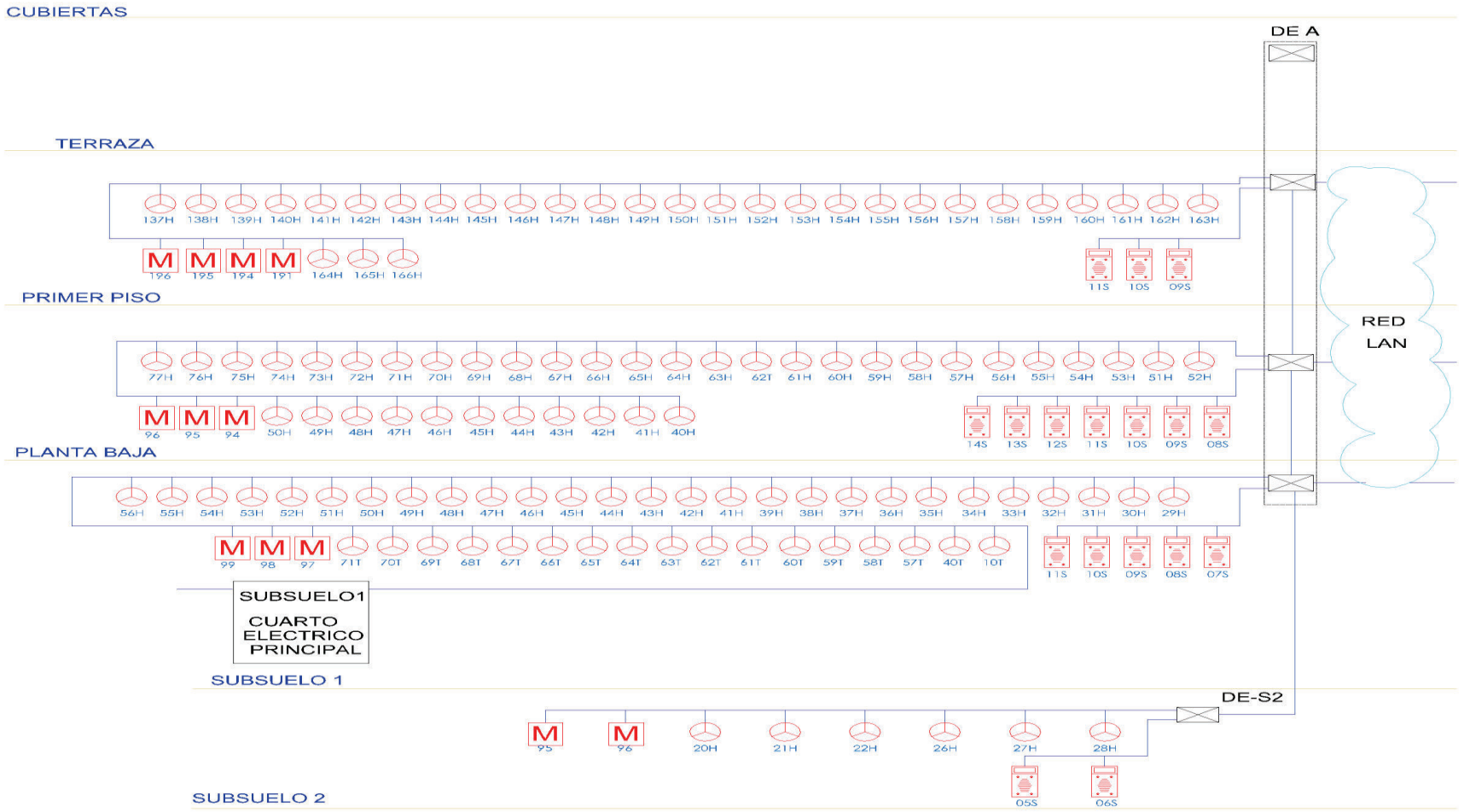


Diagrama unifilar sistema Detección Incendios lado A.



Unifilar sistema Detección Incendios lado B.

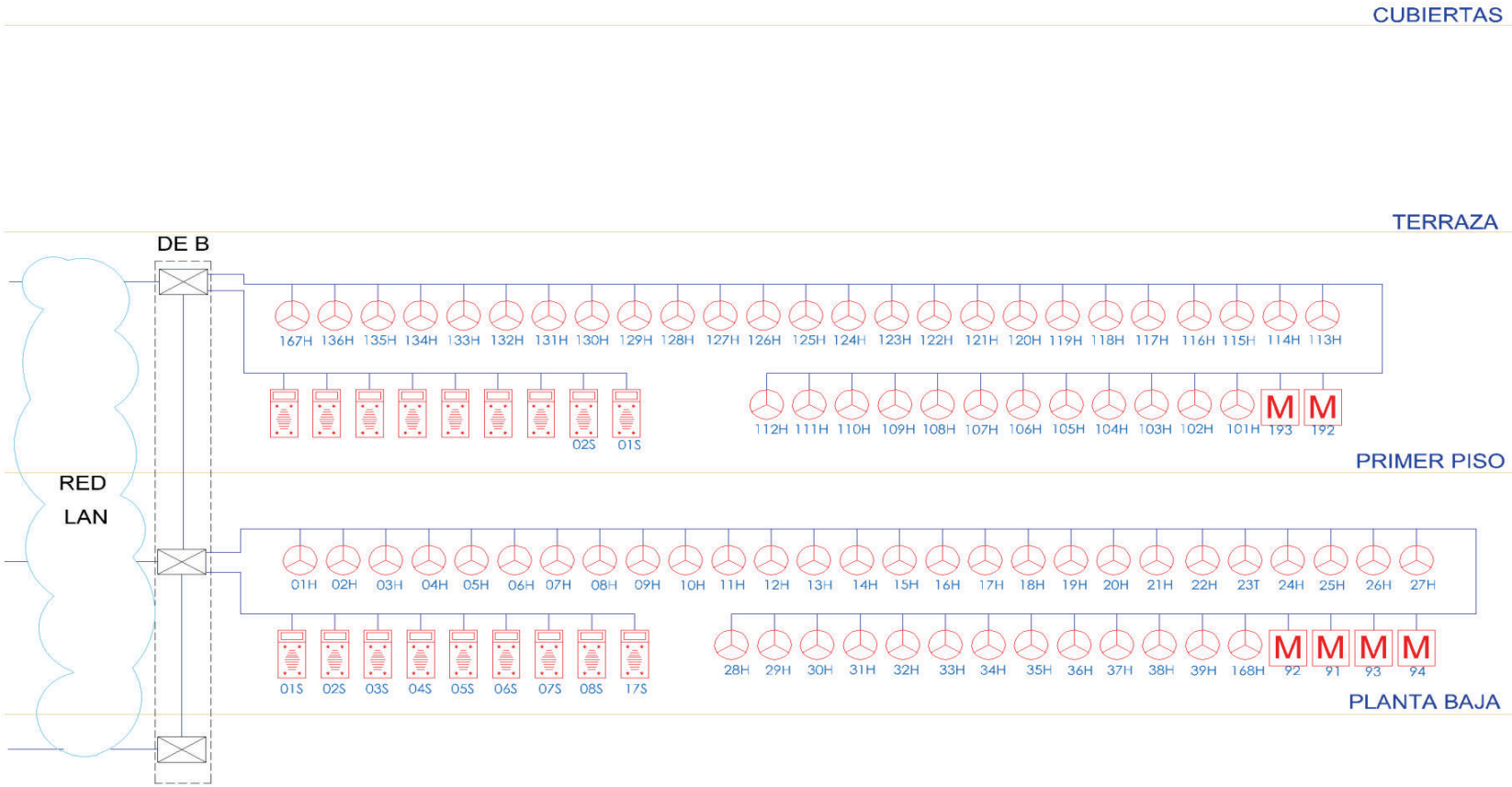


Diagrama Unifilar Sistema CCTV Lado A.

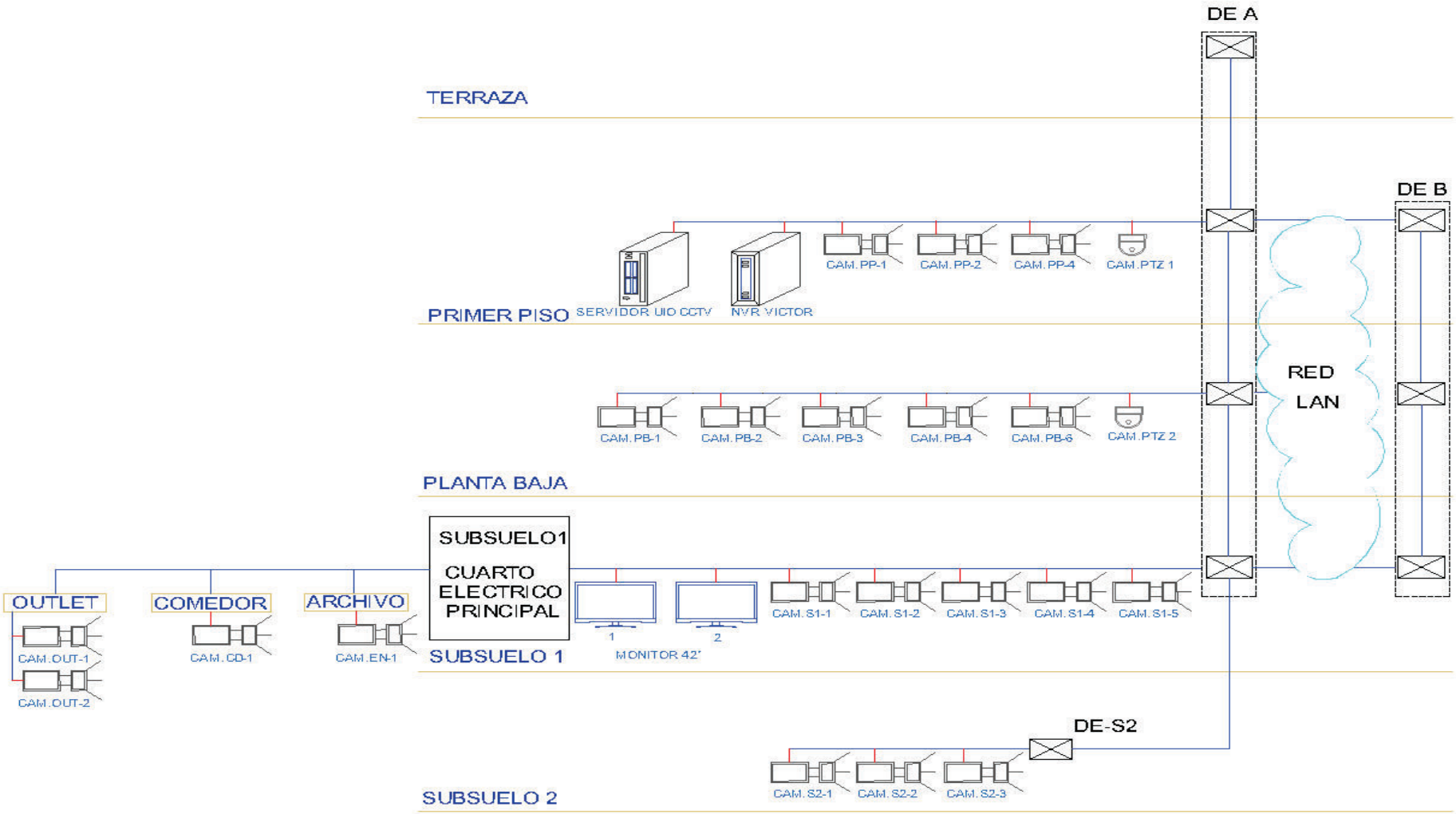


Diagrama unifilar Sistema CCTV lado B.

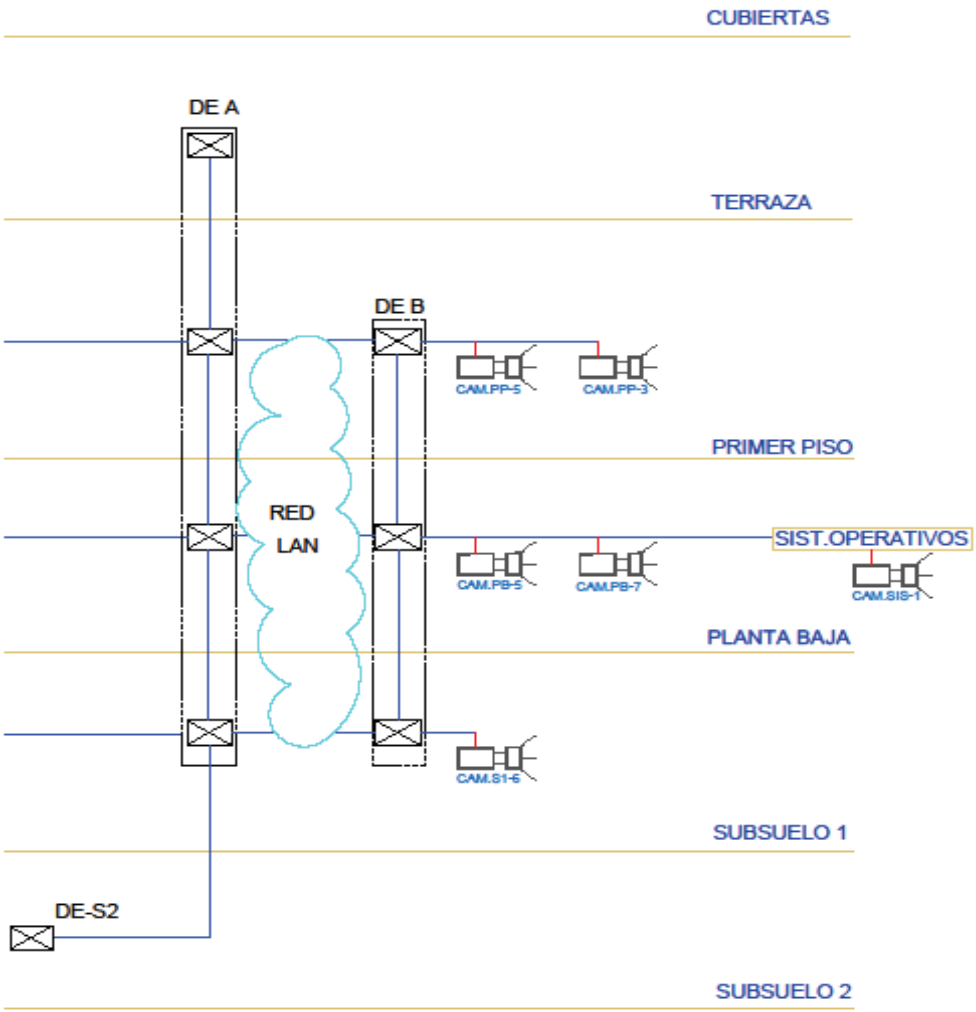


Diagrama unifilar Sistema Intrusión lado A.

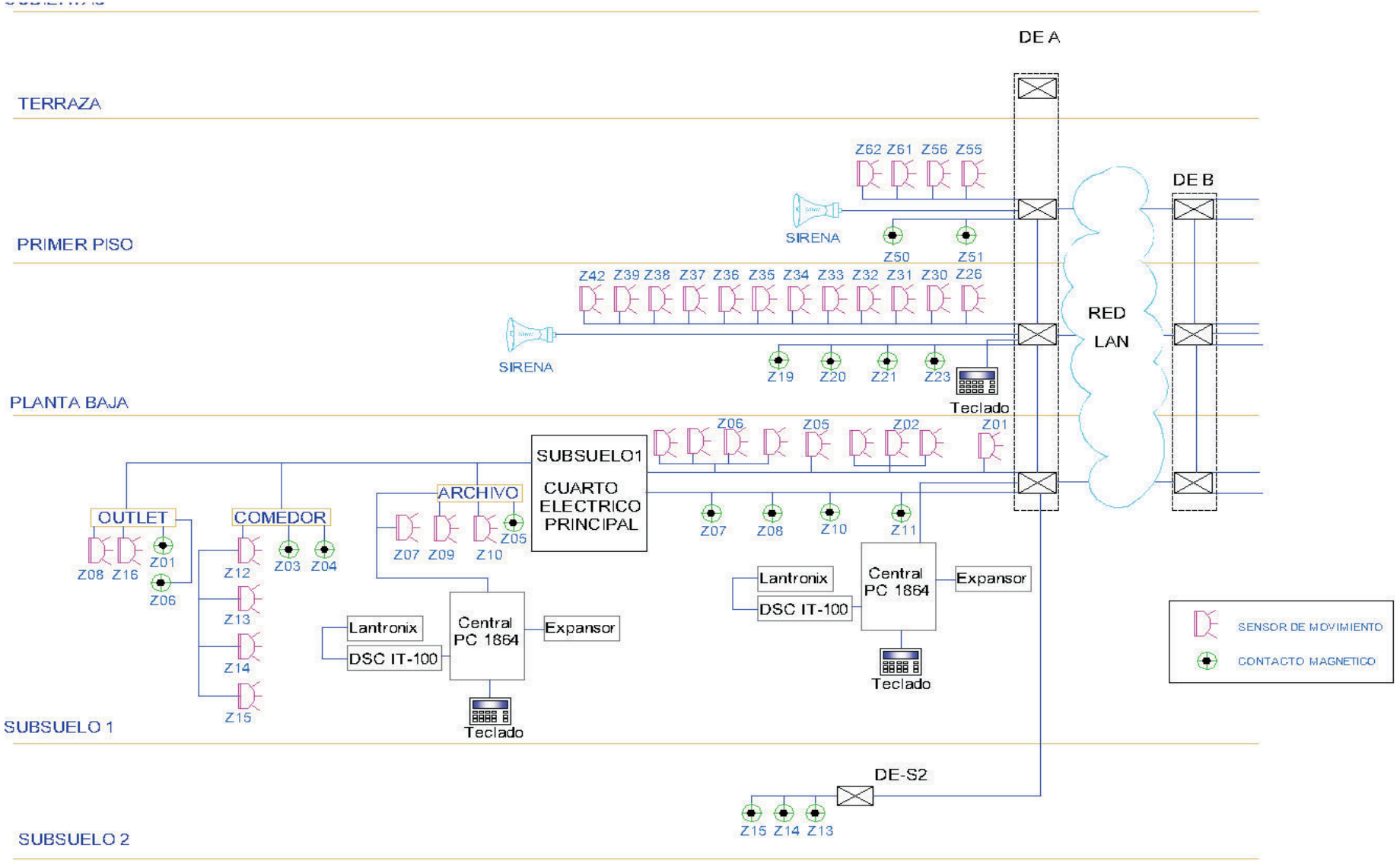
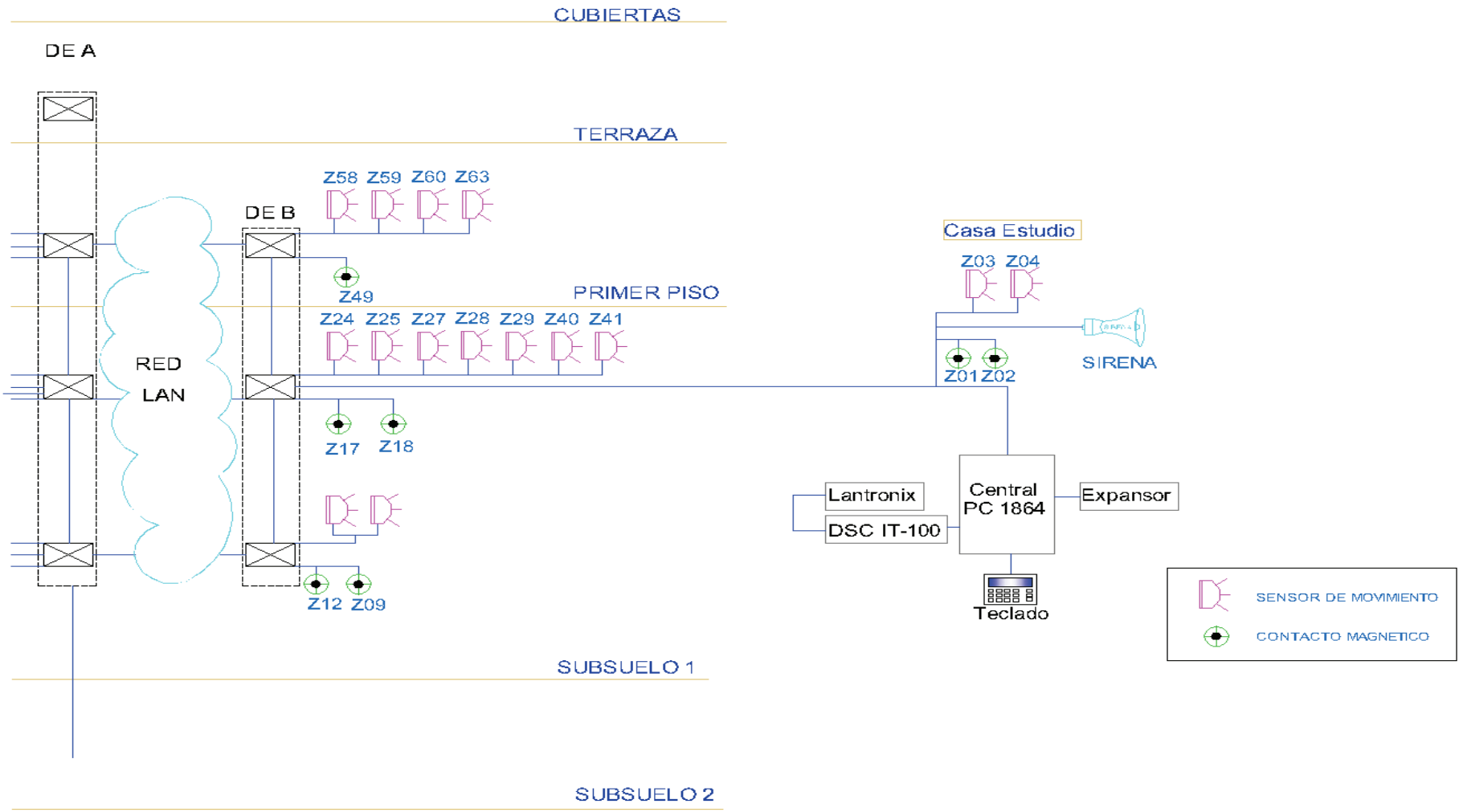


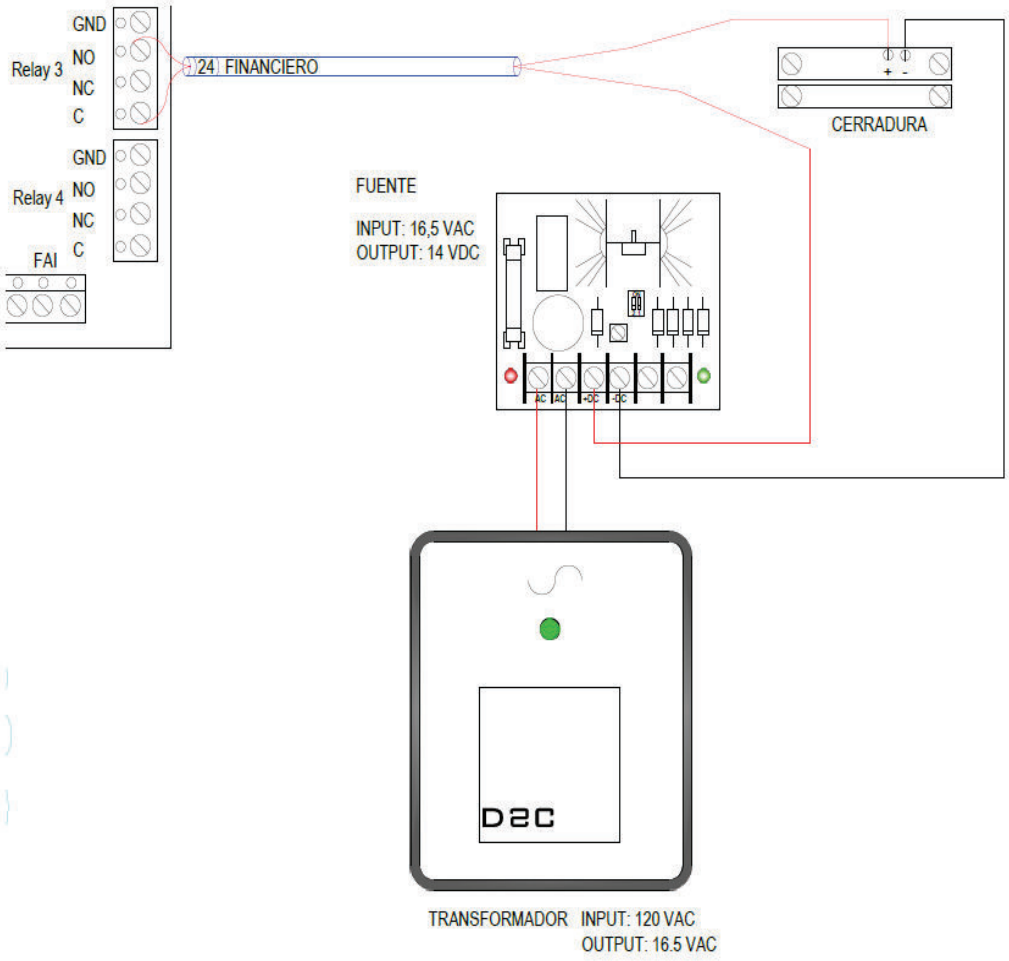
Diagrama unifilar Sistema Intrusión lado B.



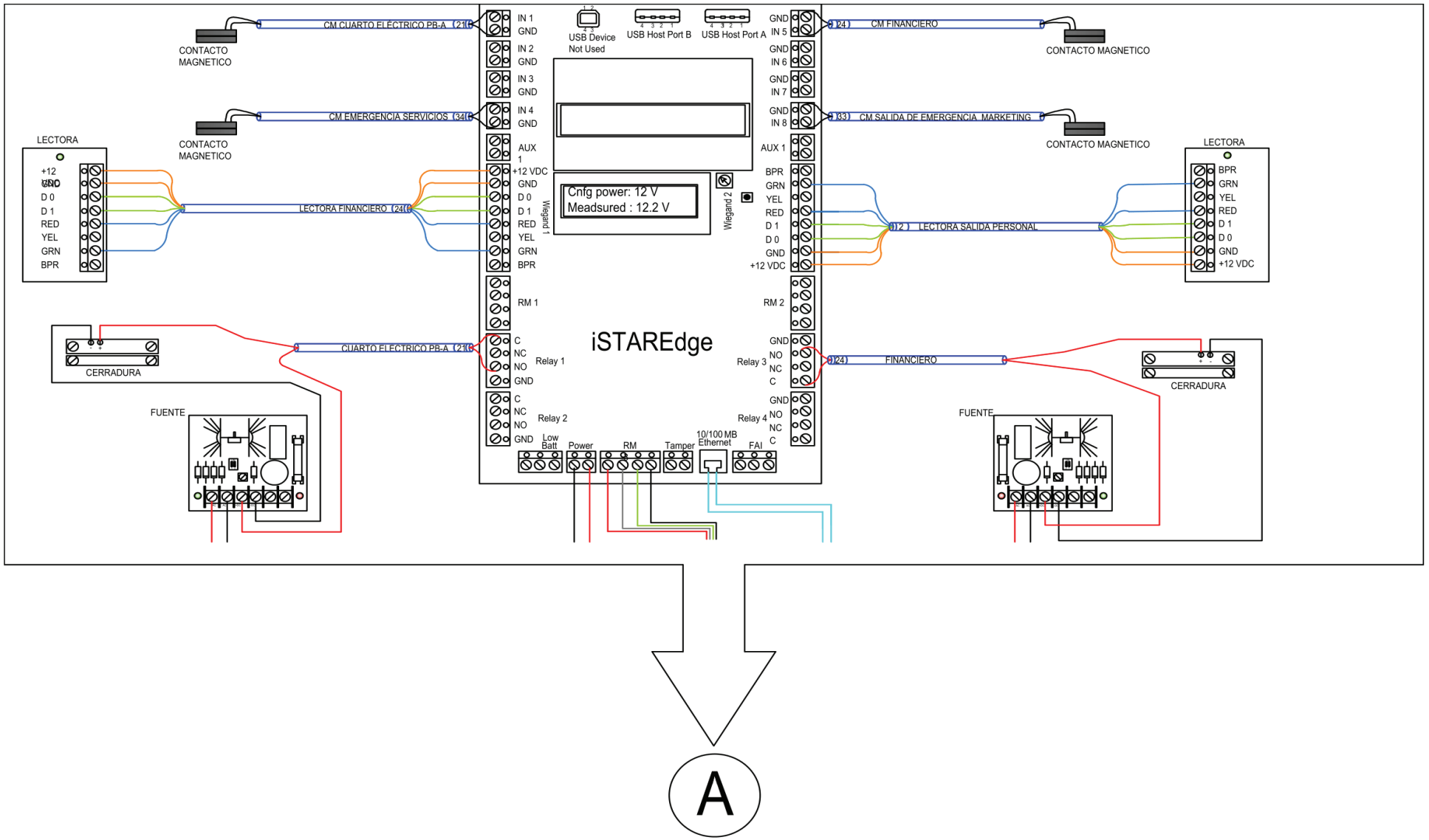
ANEXO B

CONEXIÓN DE DISPOSITIVOS

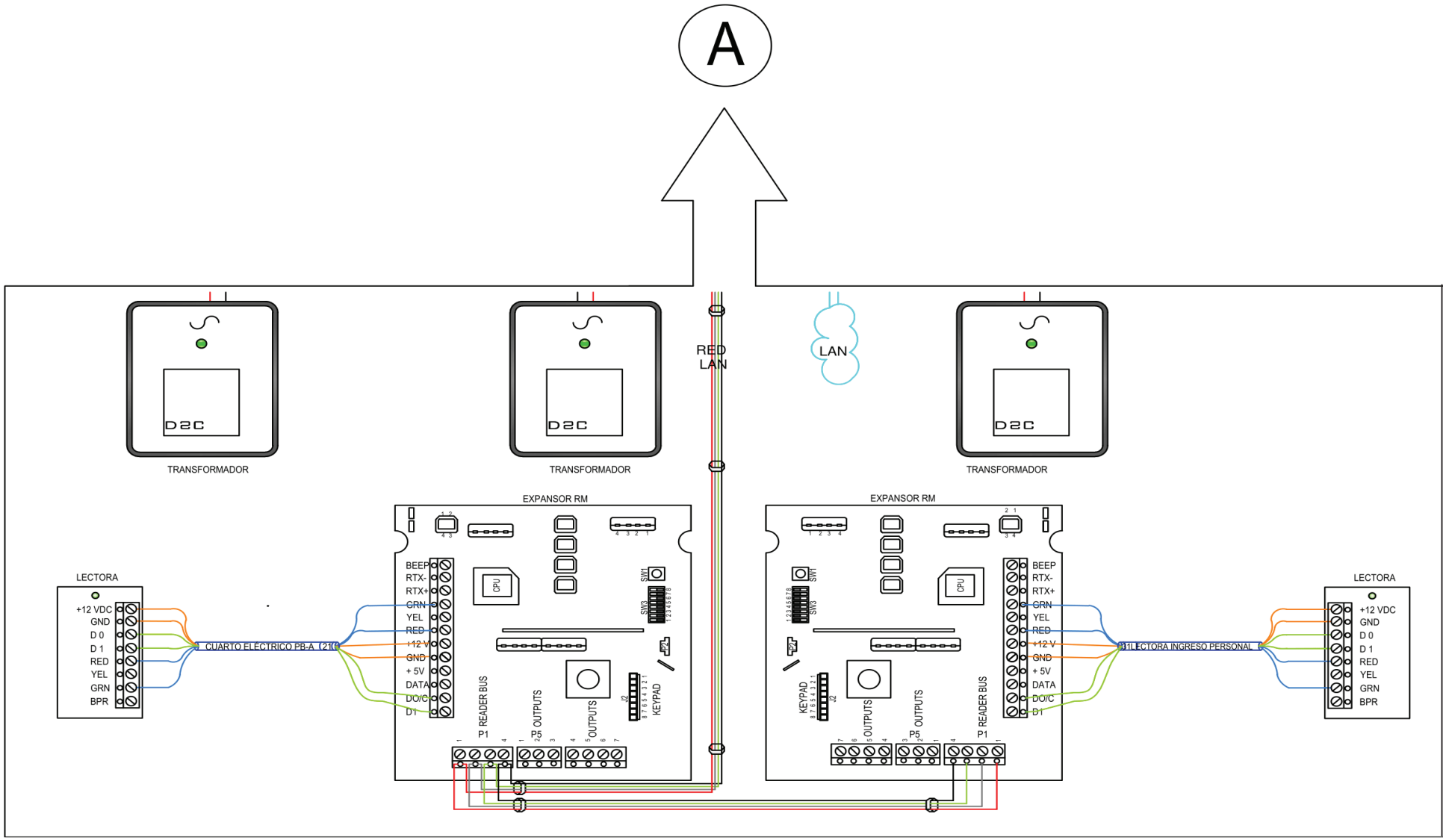
Conexión de cerradura al relay de la controladora iSTAR Edge.



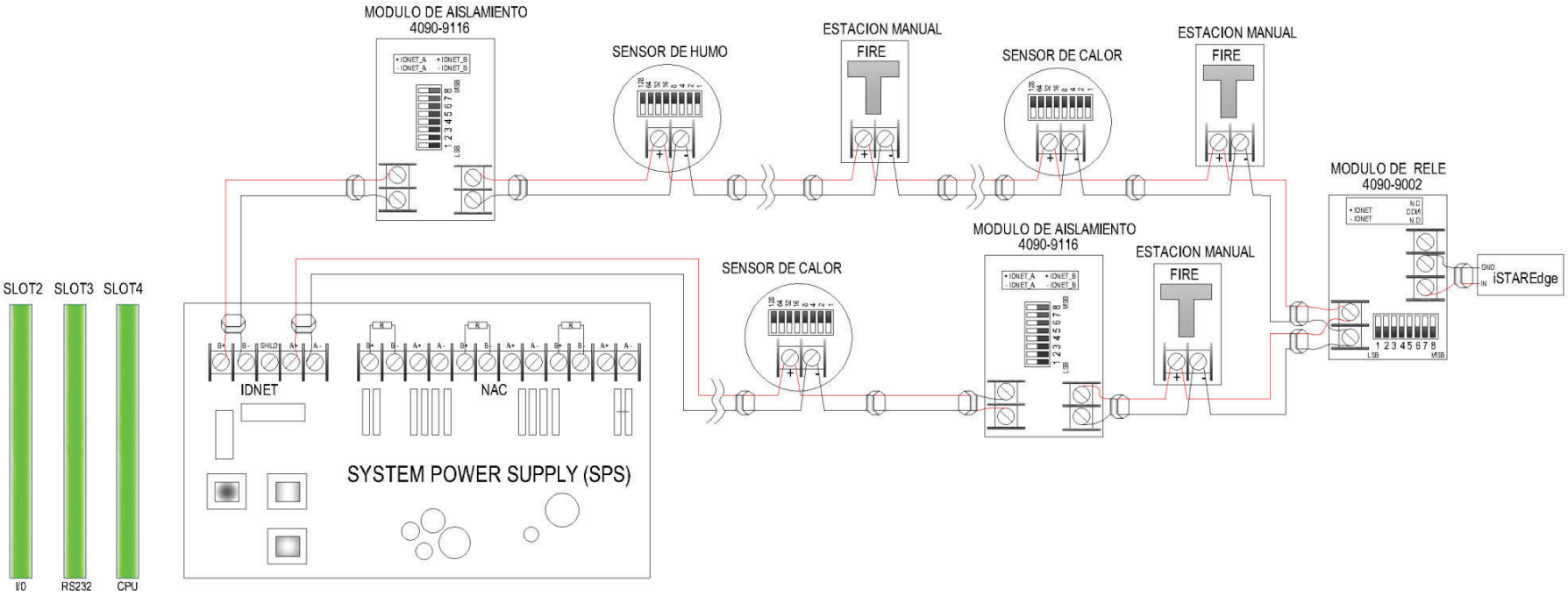
Conexión de dispositivos a la controladora iSTAR Edge.



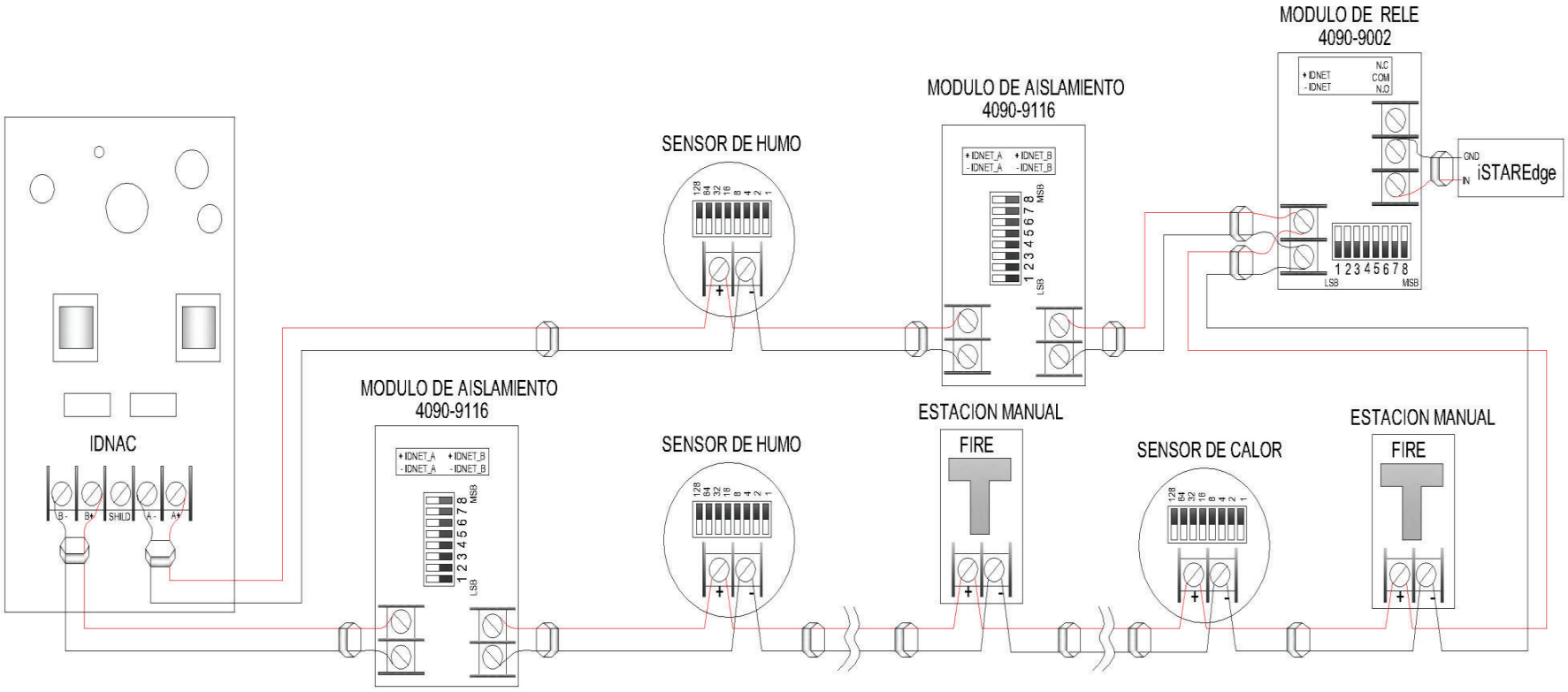
Conexión de dispositivos a la controladora iSTAR Edge.



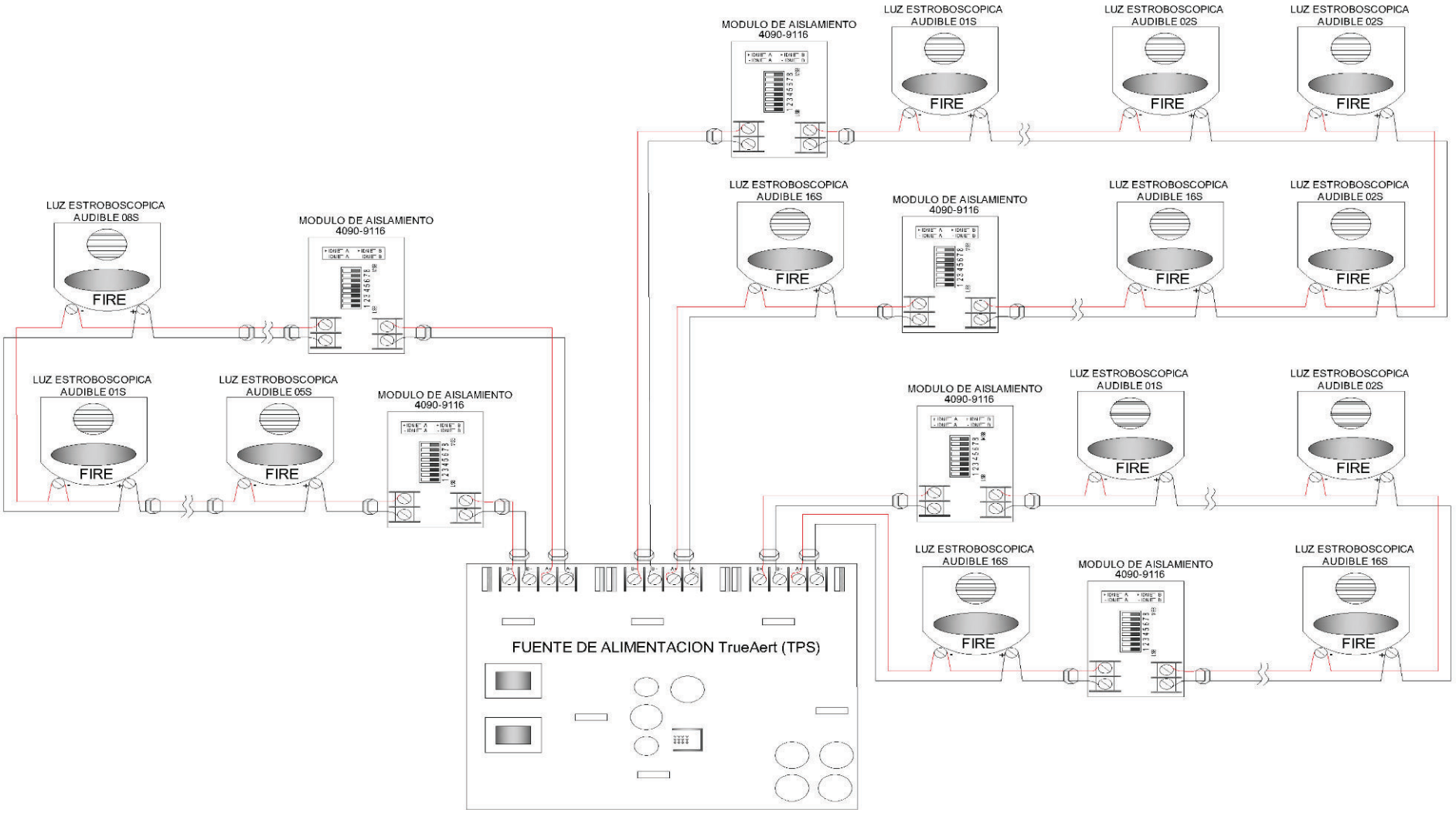
Conexión Bahía 1, IDNet 2, Clase “A”.



Conexión Bahía 2 IDNet 6, Clase “A”.



Fuente de Alimentación TrueAlert (TPS), Luces Estroboscópicas/Audibles.



ANEXO C

DIAGRAMAS DE FLUJO

Diagrama de flujo lógica del contacto magnético (Sistema Control de Accesos).

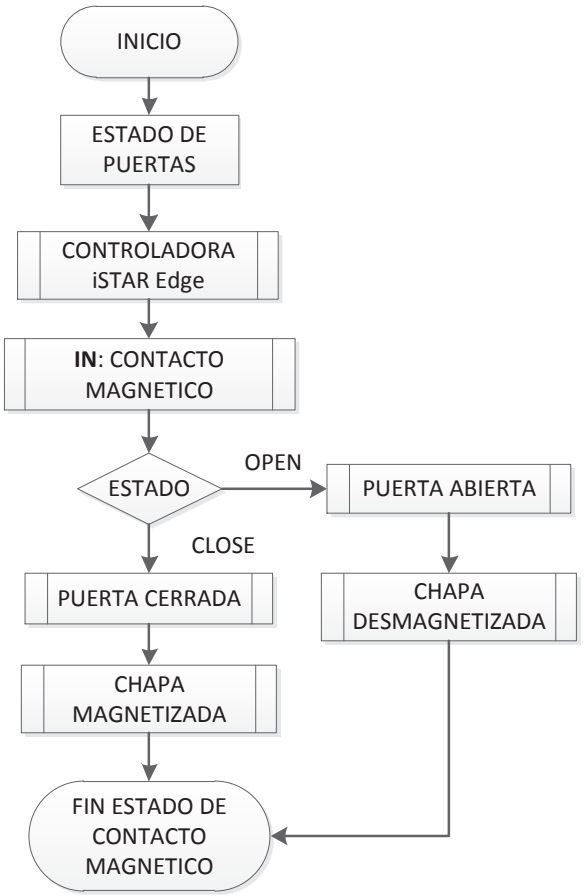
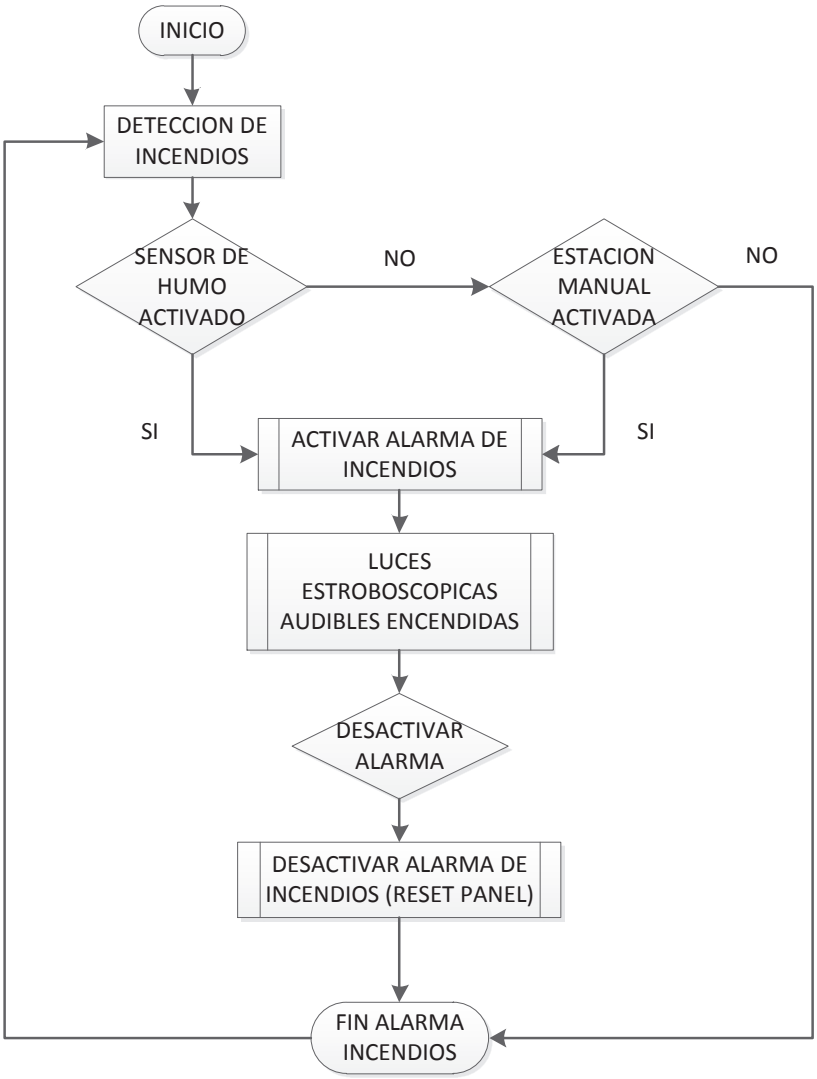


Diagrama de flujo del sistema Detección de Incendios.



Niveles de acceso a la central de alarmas (Sistema Detección de Incendios).

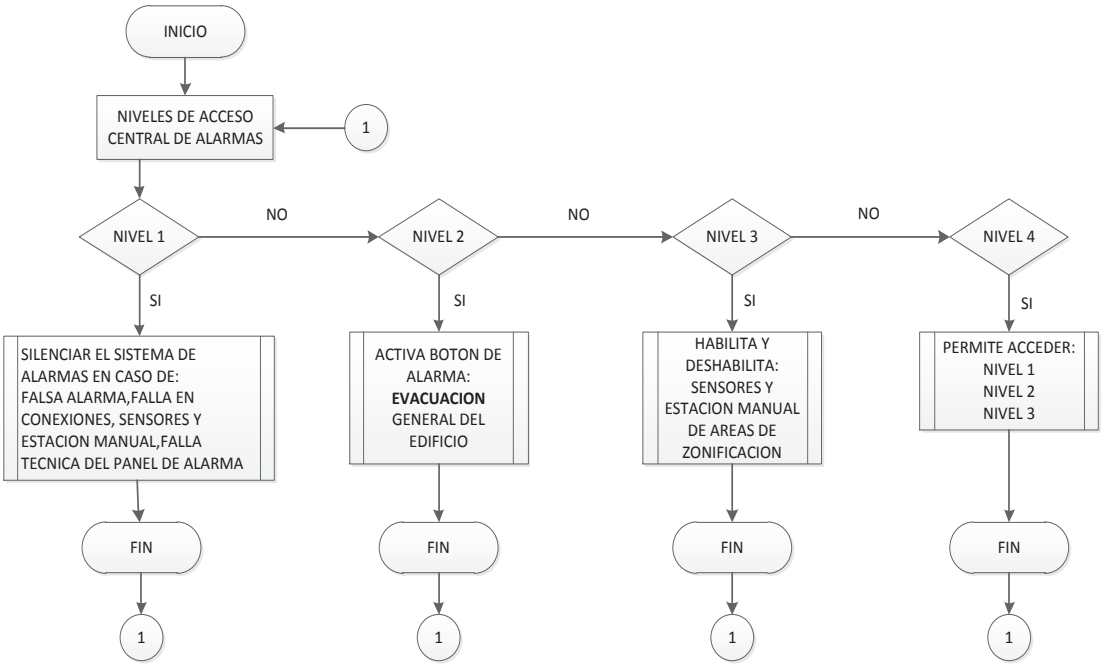


Diagrama de flujo Cambiar nivel de acceso (Sistema Detección de Incendios).

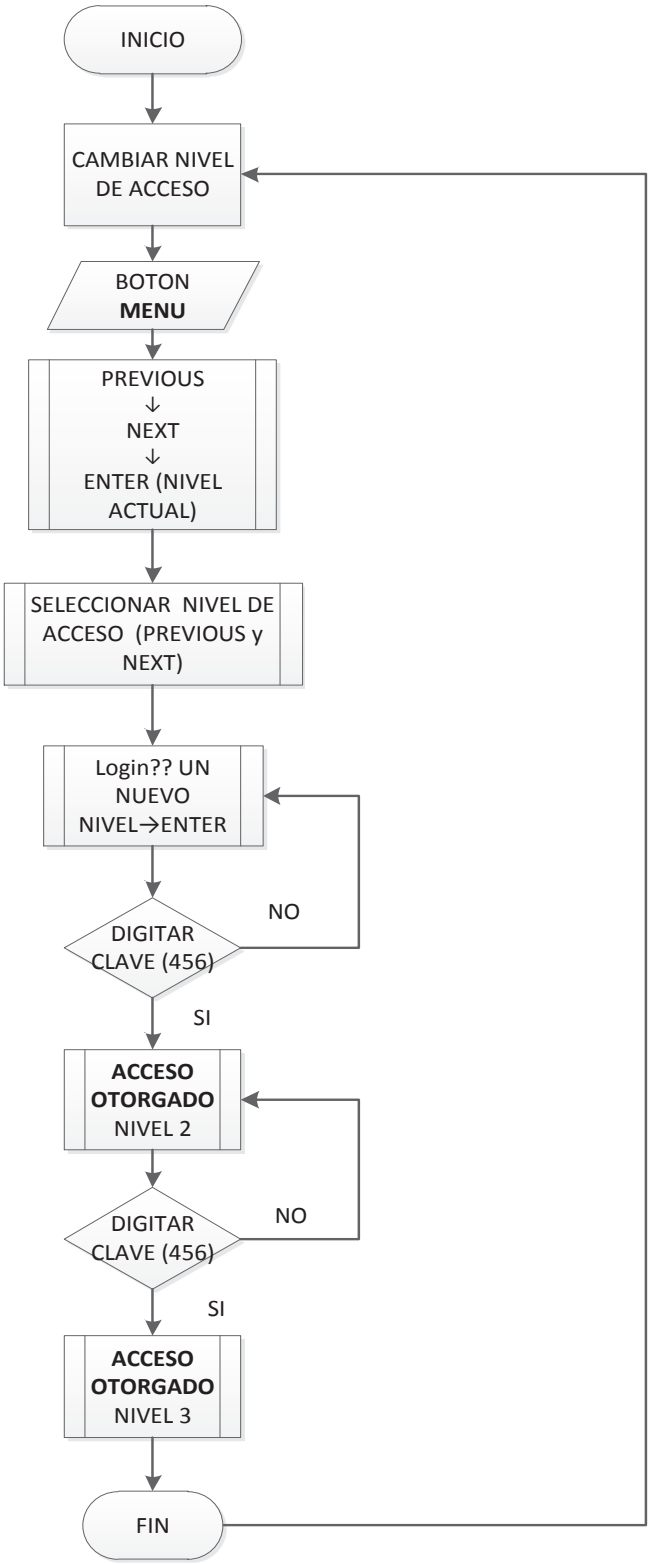


Diagrama de flujo activación de detector de humo o temperatura (Sistema detección de incendios).

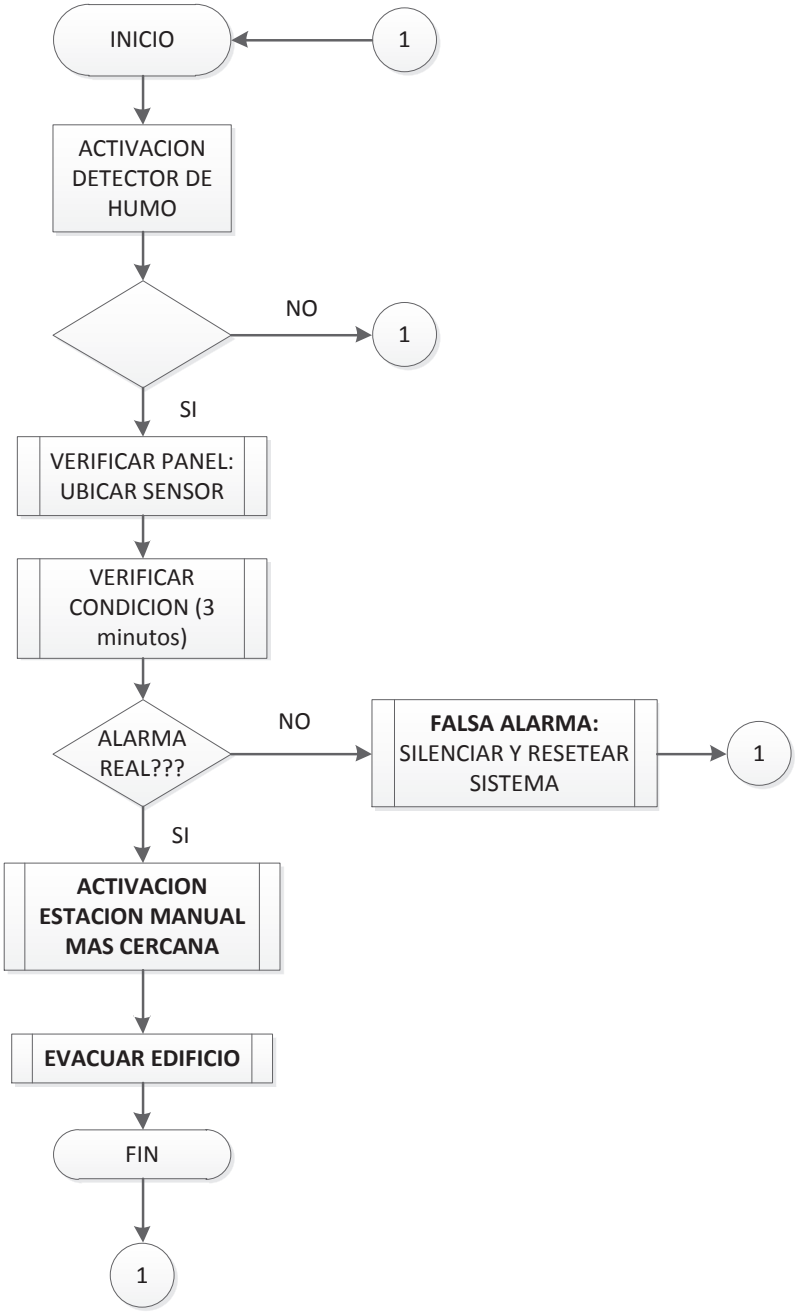


Diagrama de flujo activación estación manual (Sistema detección de incendios).

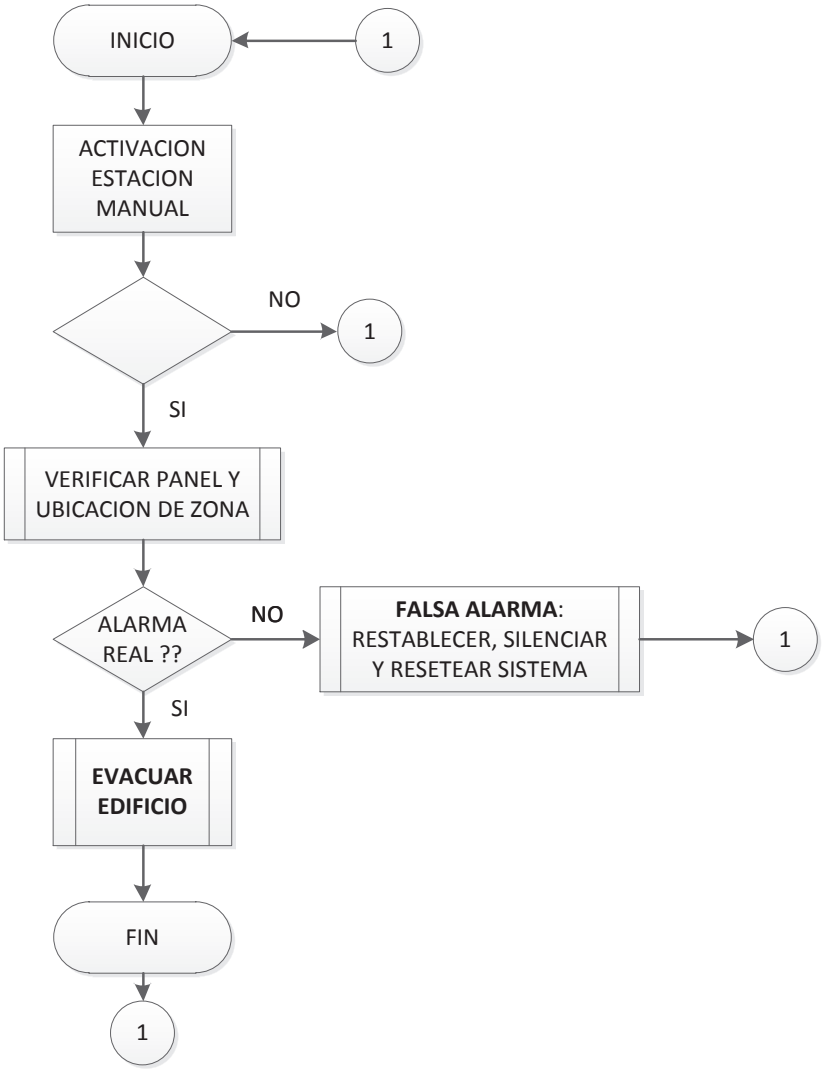


Diagrama de flujo restablecer sistema (Sistema detección de incendios).

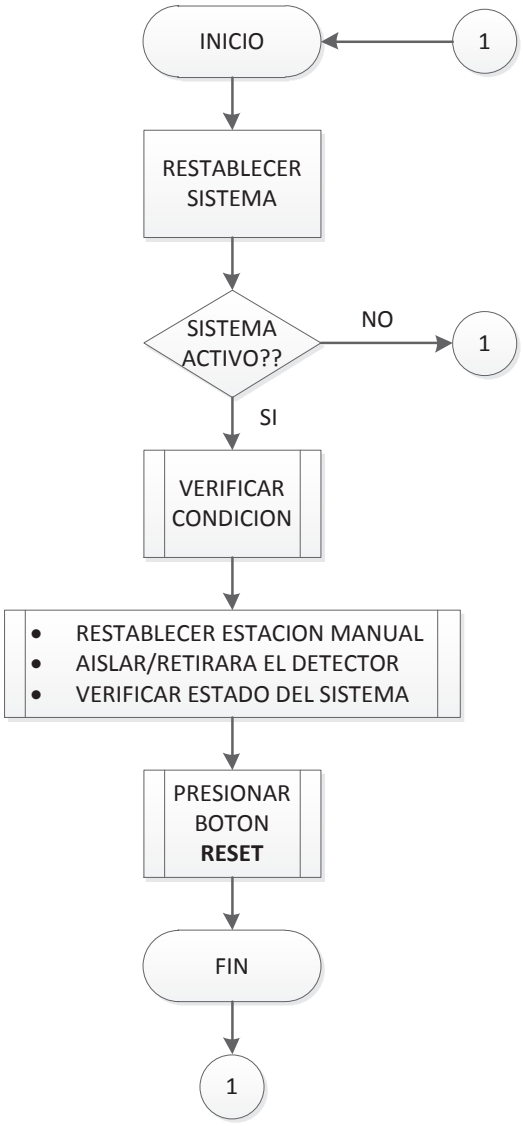


Diagrama de flujo de Históricos de fallas (Sistema de detección de incendios).

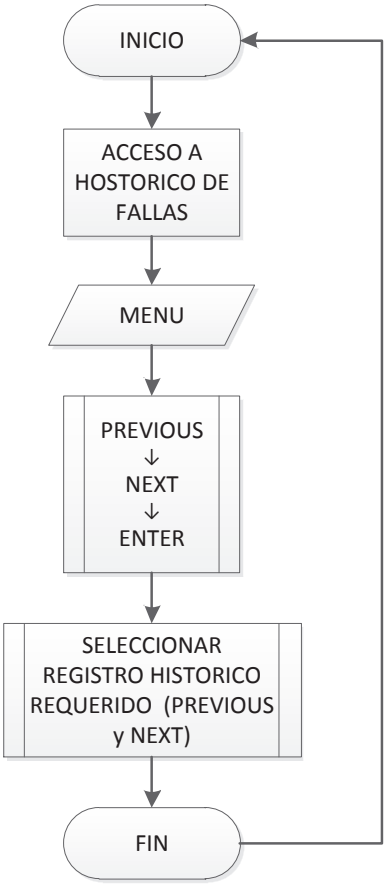


Diagrama de flujo para habilitar y deshabilitar Sensores de humo y Estaciones manuales (Sistema de detección de incendio).

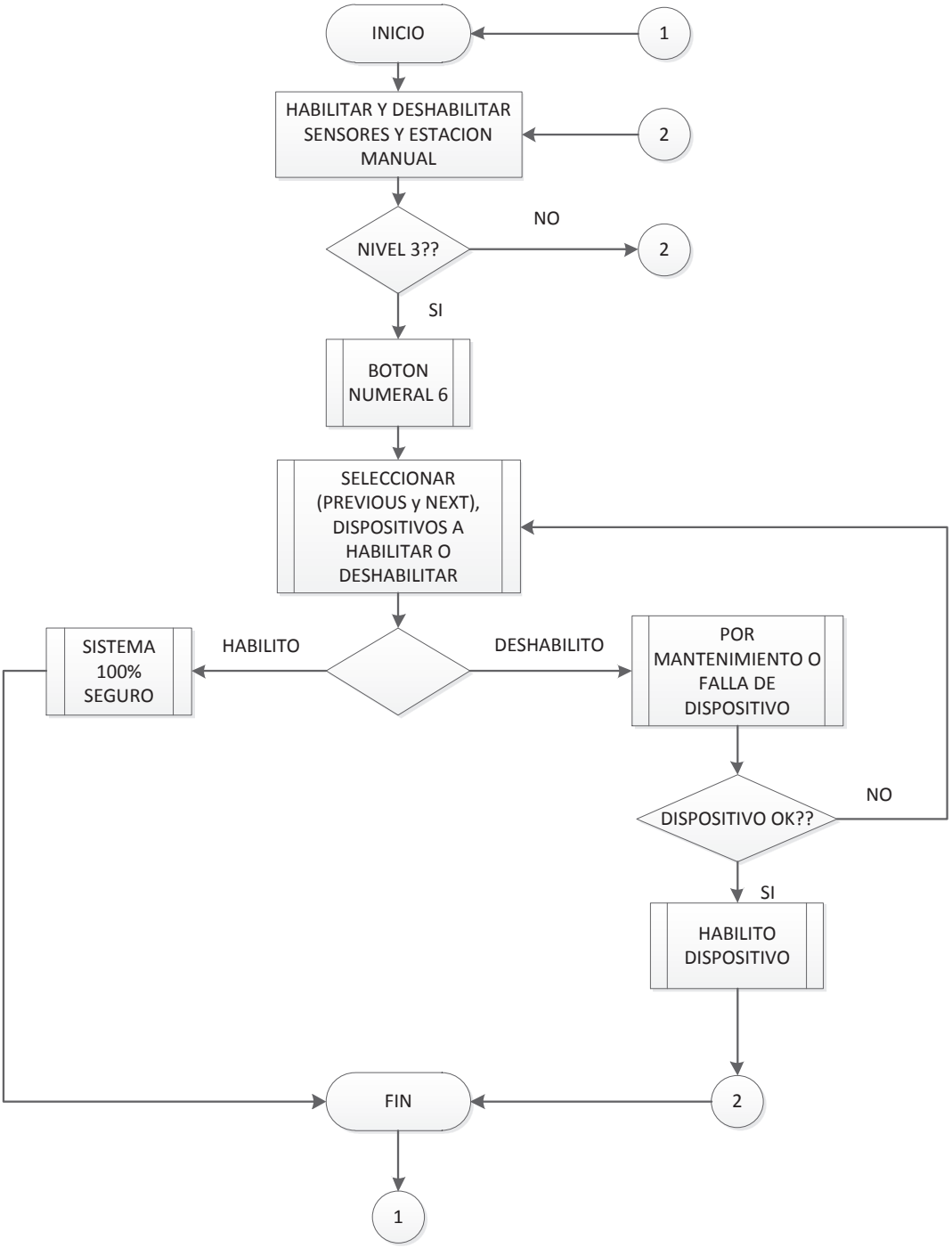


Diagrama de flujo para aislar áreas de zonificación (Sistema de detección de incendio).

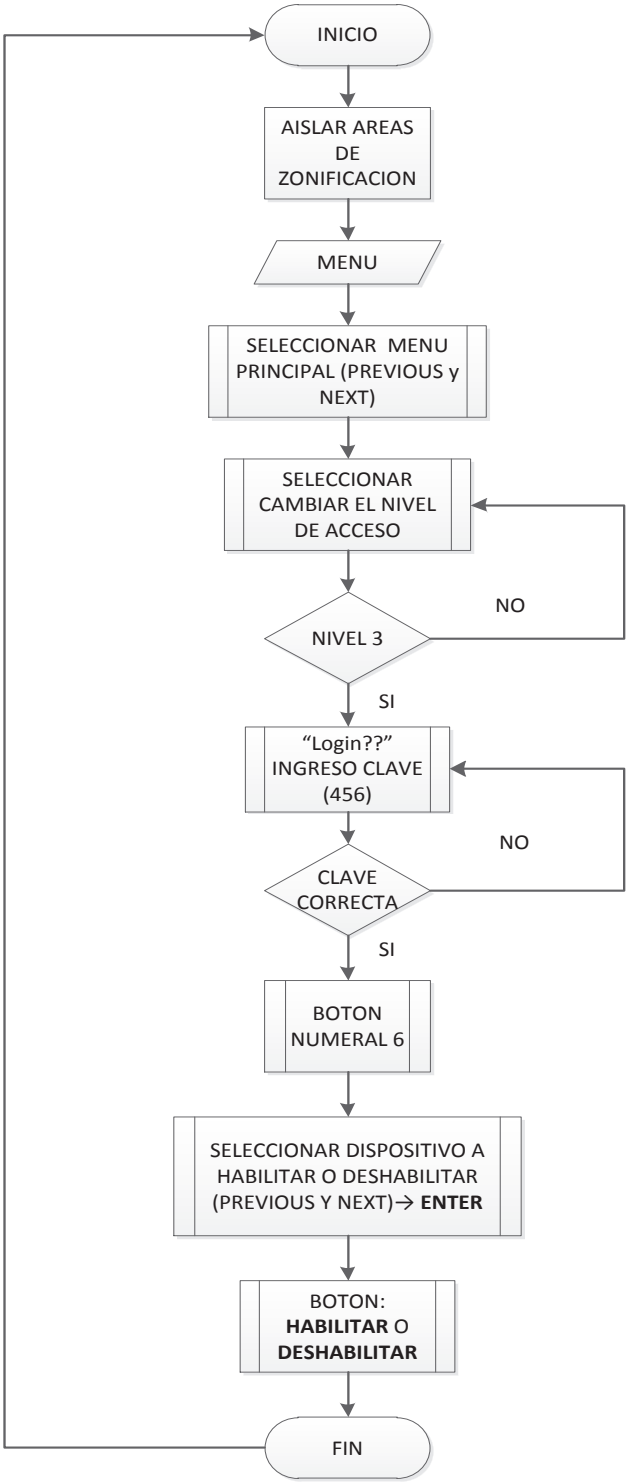
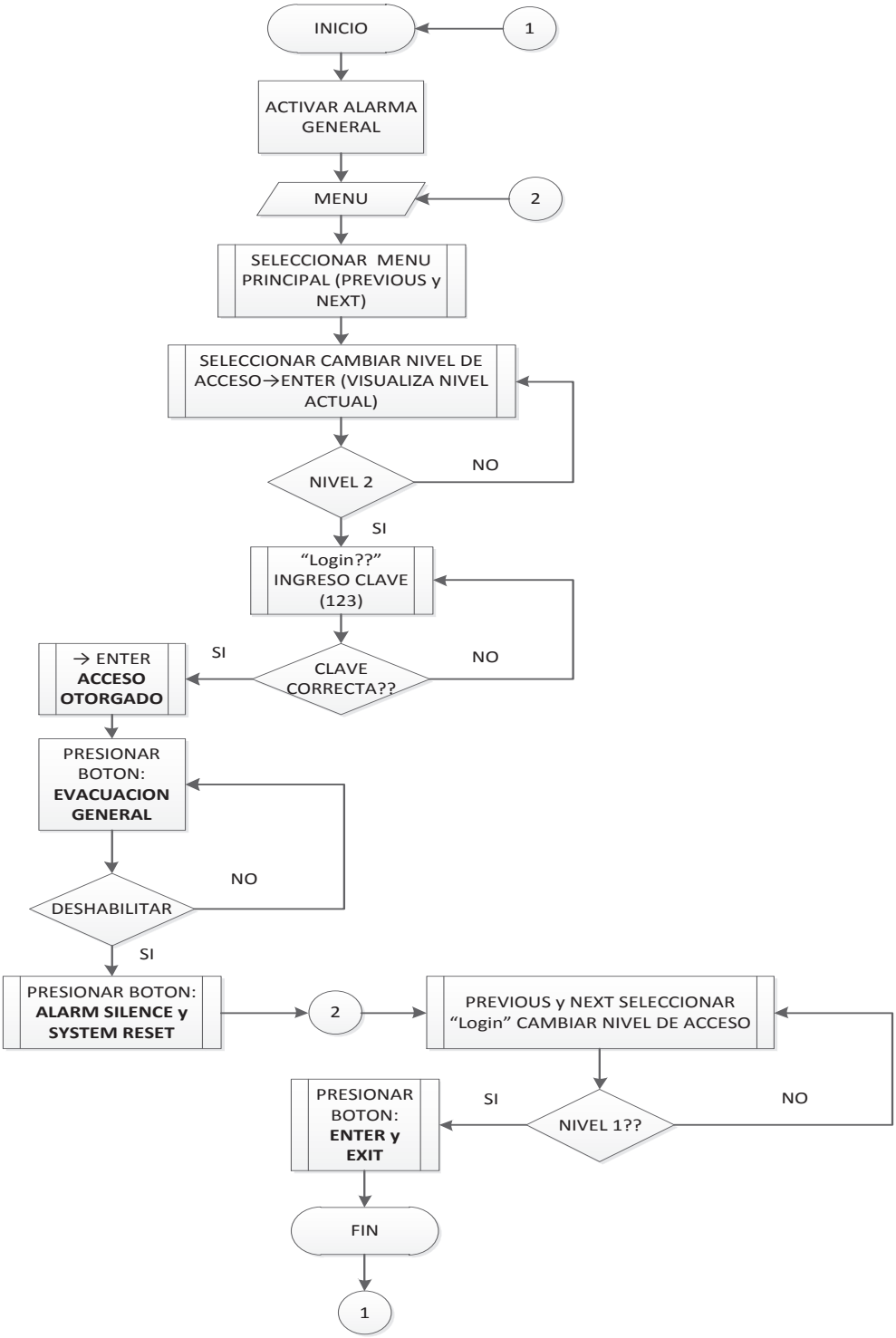


Diagrama de flujo Activación Alarma general (Sistema de detección de incendios).



Configuracion Camaras IP (Sistema CCTV).

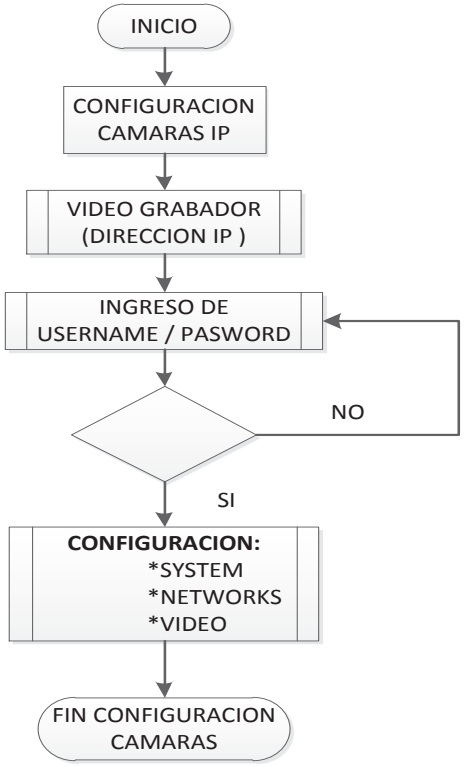
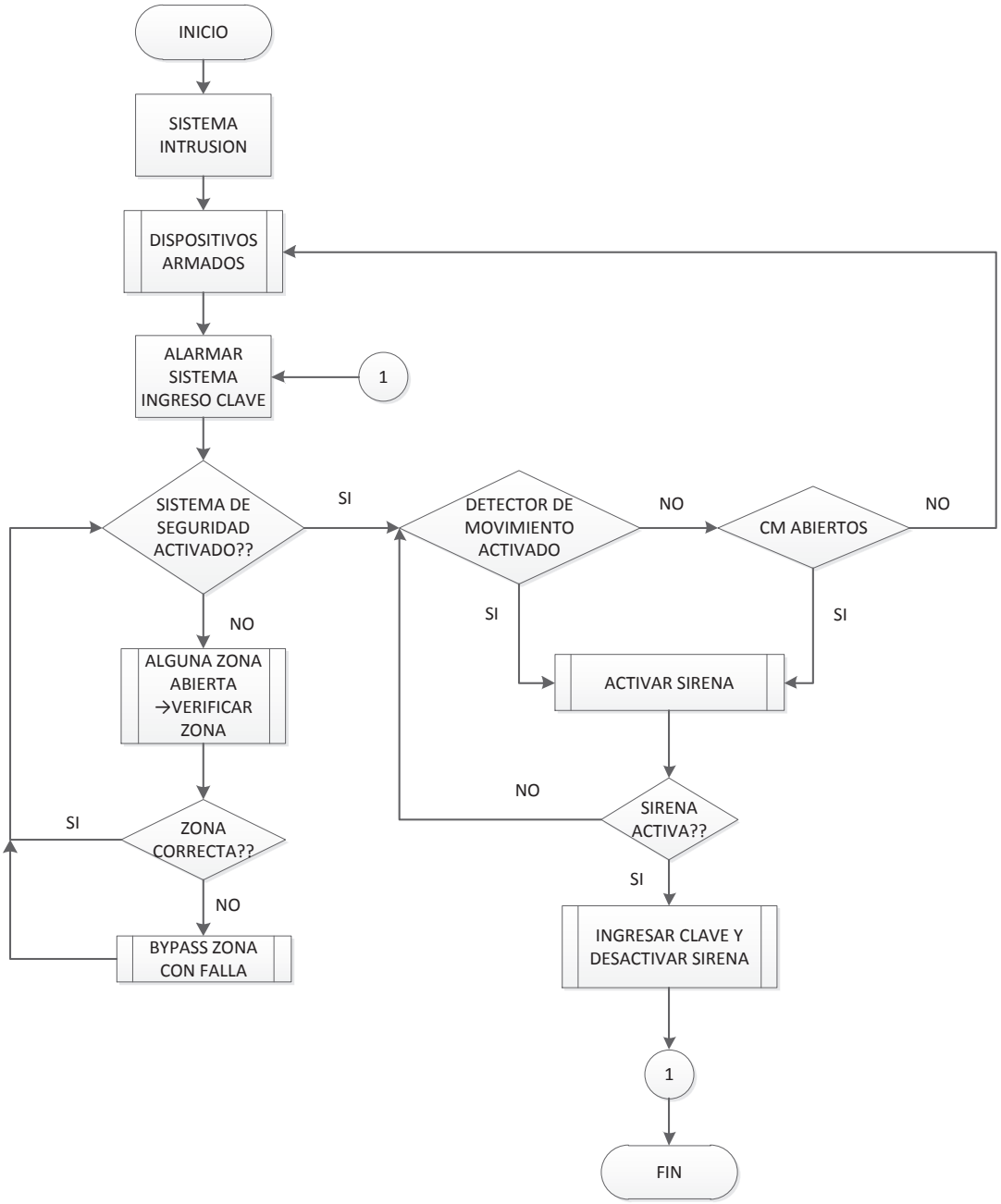


Diagrama de flujo Sistema de Intrusión.



ANEXO D

MANUAL DE USUARIO

INSTALACIÓN DEL SOFTWARE CCURE 9000

Durante el proceso de instalación de cada equipo, se solicita que especifique si va a realizar la instalación del cliente y/o del servidor.

Este sistema utiliza cuatro equipos. Se instala el software de servidor y cliente en el equipo que actúa como servidor/host (ubicado en el cuarto eléctrico lado A) y software de cliente en los equipos que se utilizan como clientes (departamento de seguridad, MAC y seguridad ocupacional).

Procedimiento:

Pre-requisitos.

- Seleccione el icono Pantalla en el Panel de control de Windows para establecer el tamaño de fuente pequeño en el servidor y en los clientes. CCURE 9000 no admite fuentes grandes.

- Abrir puertos en el firewall de Windows. CCURE 9000 exige el acceso a determinados puertos dentro del sistema. Habilitar una excepción o abrir un puerto para un programa o un servicio específico.

- Limitar la cantidad de memoria RAM asignada a SQL Server a un 50% del total de la RAM del equipo (ejecute SQL Server Management Studio y conéctese al servidor SQL> Seleccione el nombre del servidor en el panel del explorador de objetos>clic derecho>propiedades> clic en Memoria.).

- Configurar protocolos para SQL 2008 R2/2008/2005 Standard Edition (Inicio > Programas > Microsoft SQL Server 2008 R2/2008/2005 > Herramientas de configuración > Administrador de configuración de SQL Server> configuración de red de SQL Server 2008 R2/2008/2005> clic en la opción de protocolos para SQL> compruebe que los tres protocolos enumerados anteriormente ya tienen estado habilitado).

- Habilitar la compatibilidad con la administración de “Internet Information Services” (IIS). Comprobar que ASP.NET v2.01 de Microsoft Internet Information Services está configurado como permitida una vez habilitado/instalado IIS en Windows.

- Habilitar la característica Experiencia de escritorio de Microsoft para utilizar carnets en Windows Server 2008 R2 y Windows Server 2008 e niciar sesión con una cuenta con privilegios de administración en el equipo donde está instalando el sistema de CCURE 9000.

Se Instala el servidor en un equipo dedicado (cuarto eléctrico lado A) antes de instalar CCURE 9000 en los equipos de cliente (departamento de seguridad, MAC y seguridad ocupacional). El programa de instalación verifica que el sistema cumple los requisitos mínimos de hardware, software, y espacio en disco.

- Inicie el programa de instalación de CCURE 9000. Haga doble click en Launch.exe. Aparecerá la pantalla de selecciones del DVD de CCURE 9000, tal y como se muestra en la Figura 1

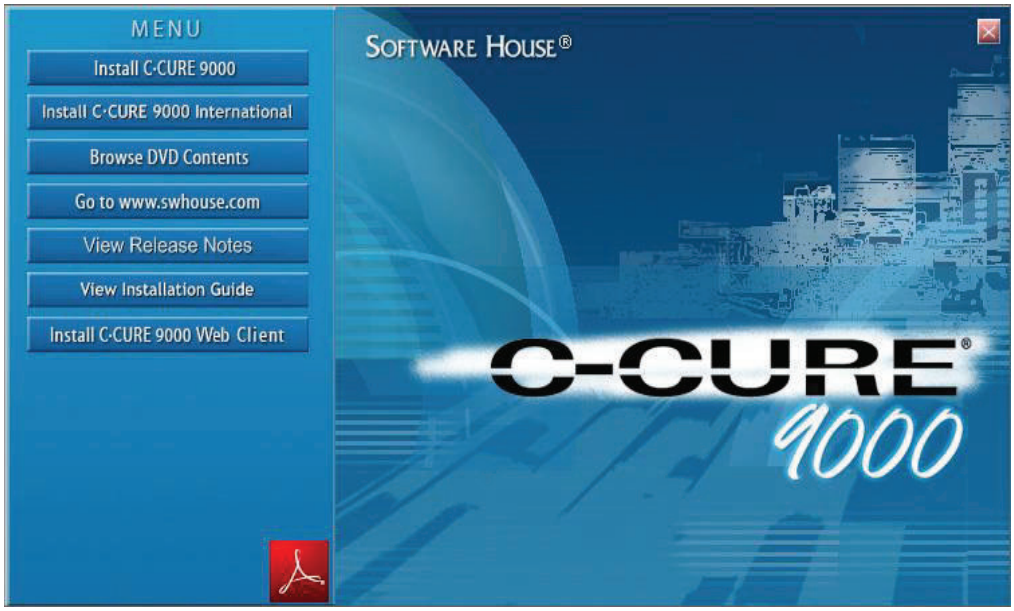


Figura 1 Pantalla de selecciones del DVD de CCURE 9000.

- Especifique si está instalando el software de cliente y servidor o solo el software de cliente. Figura 2.

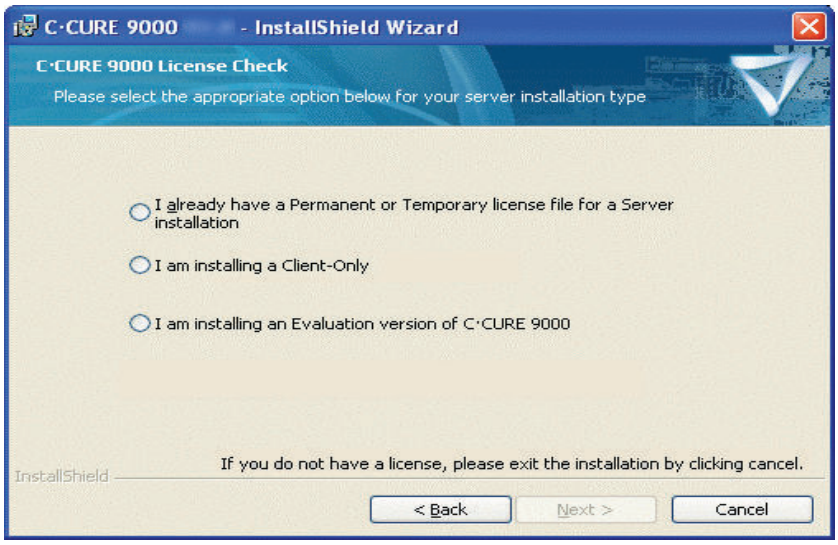


Figura 2 Cuadro de diálogo Comprobación de licencia de CCURE 9000.

- Seleccione Standalone Server Installation y clic en siguiente. Figura 3

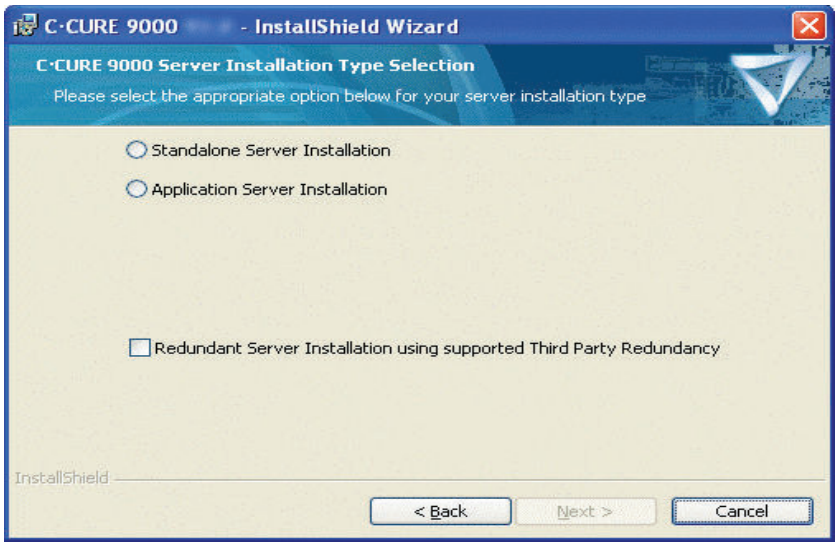


Figura 3 Selección de tipo de instalación de servidor de C•CURE 9000.

- Se abrirá el cuadro de diálogo del servidor de base de datos del sistema de CCURE 9000. Seleccione Instalar Microsoft SQL Server 2008 R2 Express Edition.

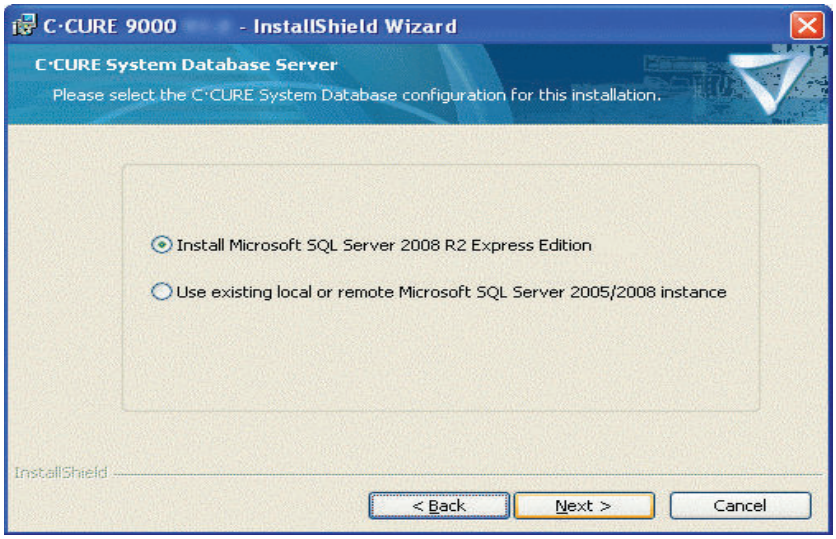


Figura 4 Opciones de SQL Server del sistema de CCURE 9000

- Instalar en primer lugar el servidor y a continuación, el cliente. Las versiones de software deben ser iguales para ambos.
- Después de instalar el software de servidor, registrar el software.
- Inicie los servicios del controlador que vaya a utilizar en el servidor de CCURE 9000. (Inicio > Todos los programas > Software House > CCURE 9000 > Aplicación de configuración del servidor).
- Inicie el software de cliente de administración o de la estación de supervisión de CCURE 9000 para empezar a usar CCURE 9000).

Dependiendo de la opción que haya elegido en el cuadro de diálogo comprobación de licencia de CCURE 9000 (Figura 2), el programa de instalación llevará a cabo alguno de las siguientes acciones:

- Instalación del servidor, instala siempre el servidor y el cliente.
- Instalación del cliente.

Escriba el nombre o la dirección IP (Servidor CCURE: 172.22.50.20) del equipo host que va a actuar como servidor de CCURE 9000 para este cliente. Figura 5.

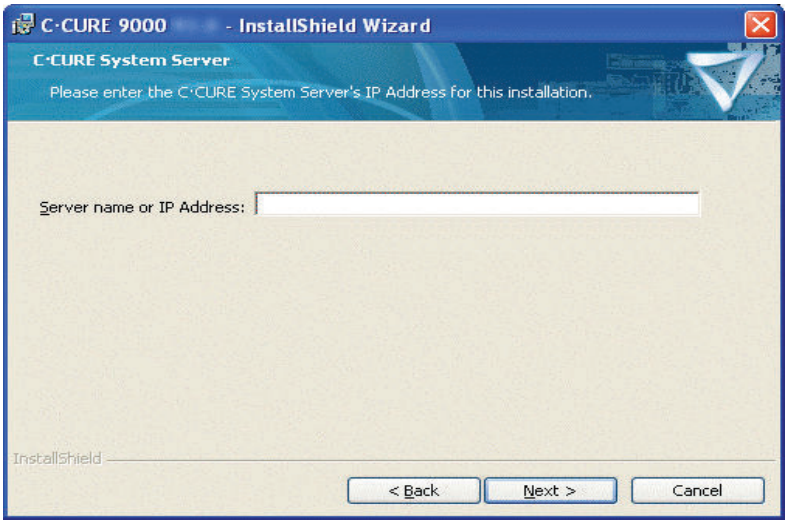


Figura 5 Servidor del sistema de CCURE 9000: dirección IP.

INSTALACIÓN INTERFACE DE CCURE 9000 – SIMPLEX FIRE ALARM.

El propósito principal de la interface de CCURE 9000-Simplex fire alarm, es mostrar al operador información de un status anormal como fuego o problema en la estación de supervisión de CCURE 9000. Esta interface incorpora los siguientes objetos a la base de datos de CCURE 9000:

- Panel Simplex 4100U: Es un objeto que sincroniza datos entre el hardware de simplex 4100ES y CCURE 9000. Configura tarjetas y puntos que quiere representar en el programa.
- Tarjeta Simplex 4100U: Son objetos creados automáticamente cuando se sincronizan los datos desde el hardware de Simplex 4100U.
- Puntos Simplex 4100U: Crea puntos físicos y pseudo puntos. Los puntos físicos son los puntos de fuego, tales como sensores, estaciones manuales, etc., en cambio los pseudo puntos presentan el status de hardware del panel.

Procedimiento de instalación.

- Cerrar todas las aplicaciones y deshabilitar el antivirus. Hacer clic en Simplex_4100U_Integration.exe del kit de instalación
- El programa de instalación revisa si el sistema tiene los requerimientos mínimos y si los encuentra aparece la pantalla de la figura 1.

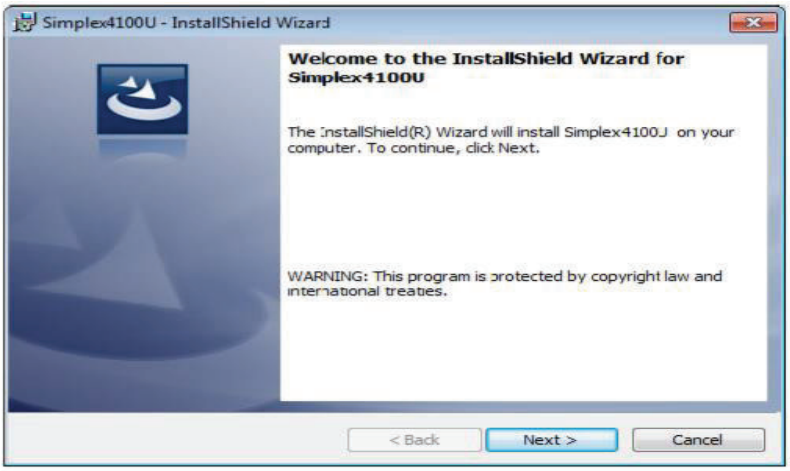


Figura 1 Ventana de inicio.

- Click en “next” para continuar la instalación. Seleccionar instalar los componentes en el servidor, o en el cliente o los dos. Dependiendo si está instalando en el servidor o en un cliente. Figura 2.

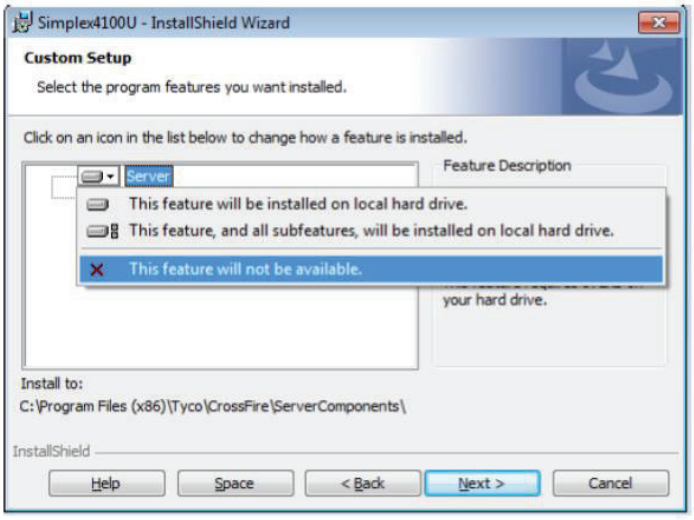


Figura 2 Componentes del servidor y cliente.

- Click en “next”, en pocos minutos se completa la instalación y aparece la siguiente ventana de la figura 3. Hacer clic en “finish” para finalizar el proceso de instalación.

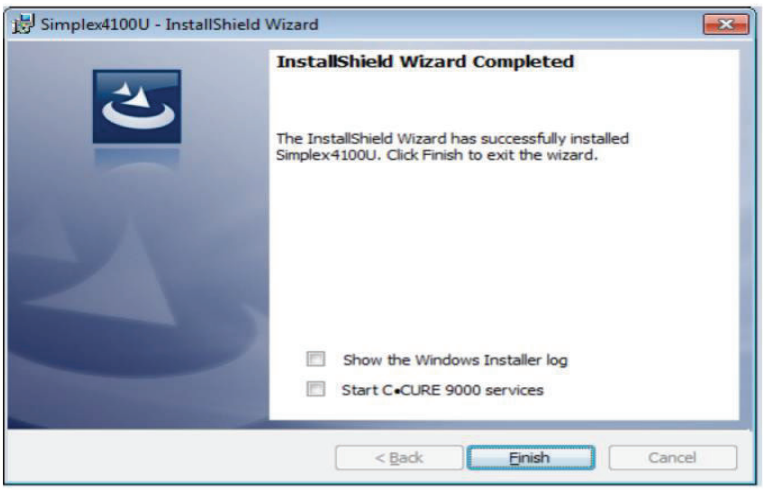


Figura 3 Ventana de finalización de instalación.

Para comenzar a configurar el panel simplex 4100ES desde CCURE 9000 se debe inicializar los servicios. Seguir los siguientes pasos:

- Seleccionar Start> All Programs> Software House> Server Configuration.
- Click en Server Components.
- Click derecho en Simplex 4100U Hardware Interface y seleccione Start Server component.

CREACIÓN DEL PUERTO DE COMUNICACIÓN.

Antes de configurar el panel Simplex 4100U, se debe crear un puerto de comunicación con el panel de detección de incendios (Simplex comm port). Seguir los siguientes pasos:

- Hacer clic en Hardware, desde el panel de navegación de la estación de administración. Figura 4.
- Seleccionar la carpeta donde se quiere crear el puerto de comunicación Simplex.
- Clic derecho y seleccionar “Simplex Comm Port”>new.
- Clic en guardar y cerrar

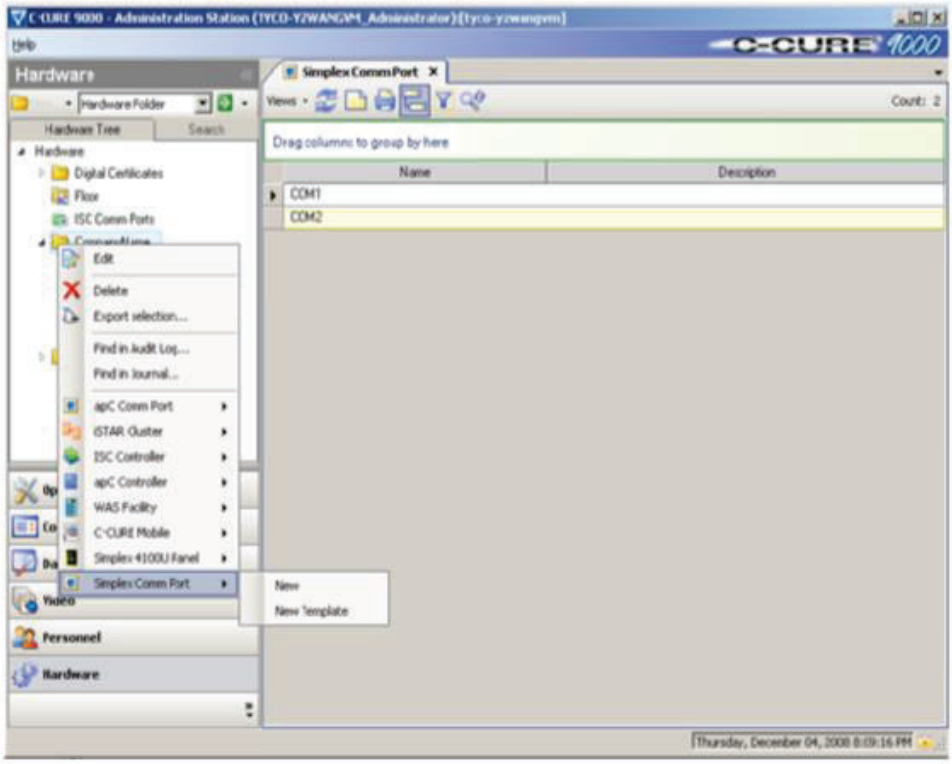


Figura 4 Creación de un puerto de comunicación.

Una vez que se ha guardado no se puede cambiar ningun valor. Si desea modificar algún campo se debe crear un nuevo puerto. El puerto de comunicación Simplex 4100U se muestra en la figura 5.

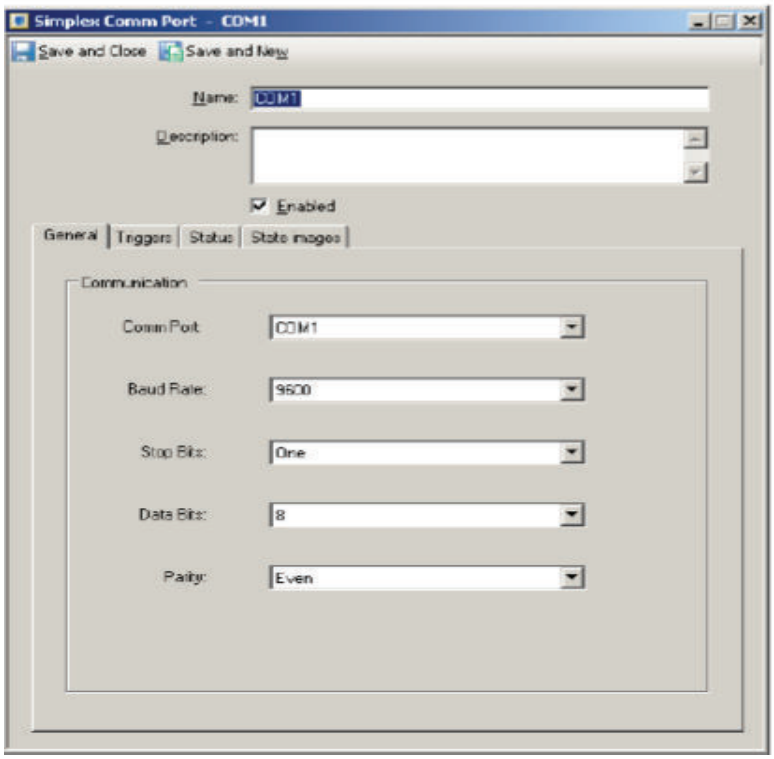


Figura 5 Ajustes puerto de comunicación.

CREACIÓN DE CENTRAL DE DETECCIÓN.

Cuando se crea el panel Simplex 4100U, este objeto aparece en la carpeta de Hardware. Seguir el siguiente procedimiento para crear un nuevo panel Simplex 4100U:

- Hacer clic en Hardware del panel de navegación de la estación de administración.
- Click derecho en la carpeta Company name.
- Seleccionar panel simplex 4100U y hacer clic en nuevo.
- Aparece el editor del panel Simplex 4100U.
- Hacer click en guardar y cerrar.

- Después de crear la central, se coloca la dirección IP 172.22.50.23 y se configura el panel de acuerdo a la figura 6.

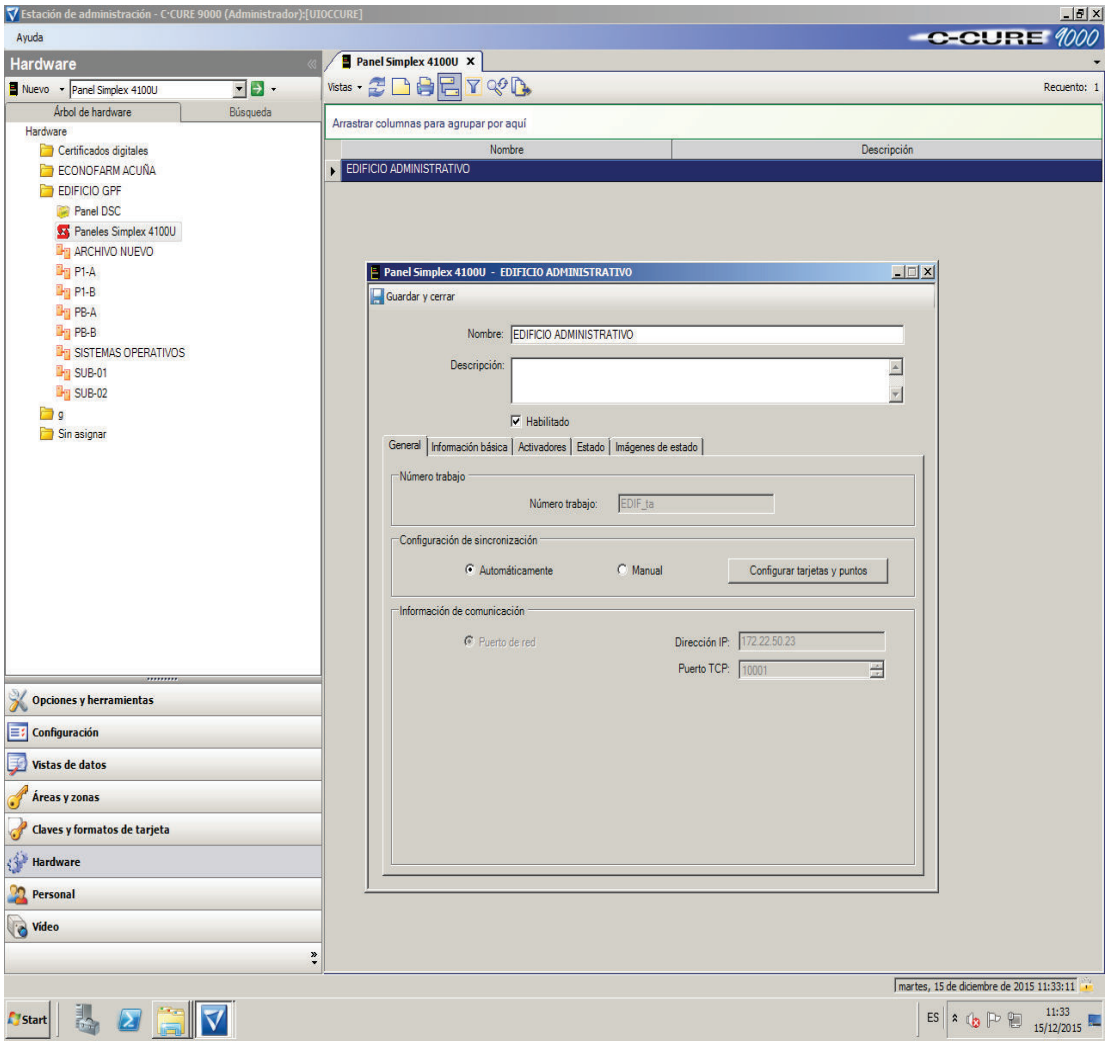


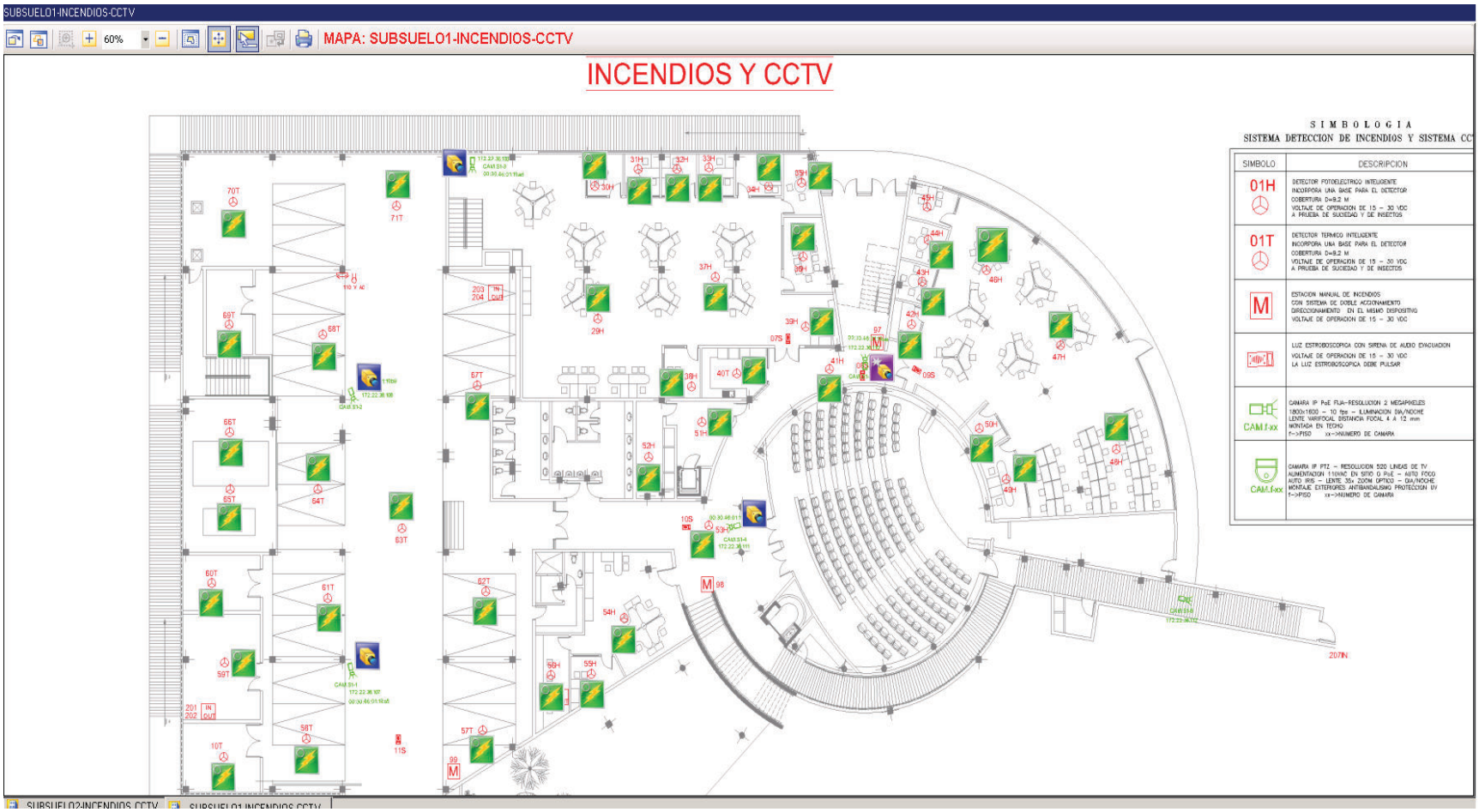
Figura 6 Ajustes de la central de detección de Incendio.

ANEXO E

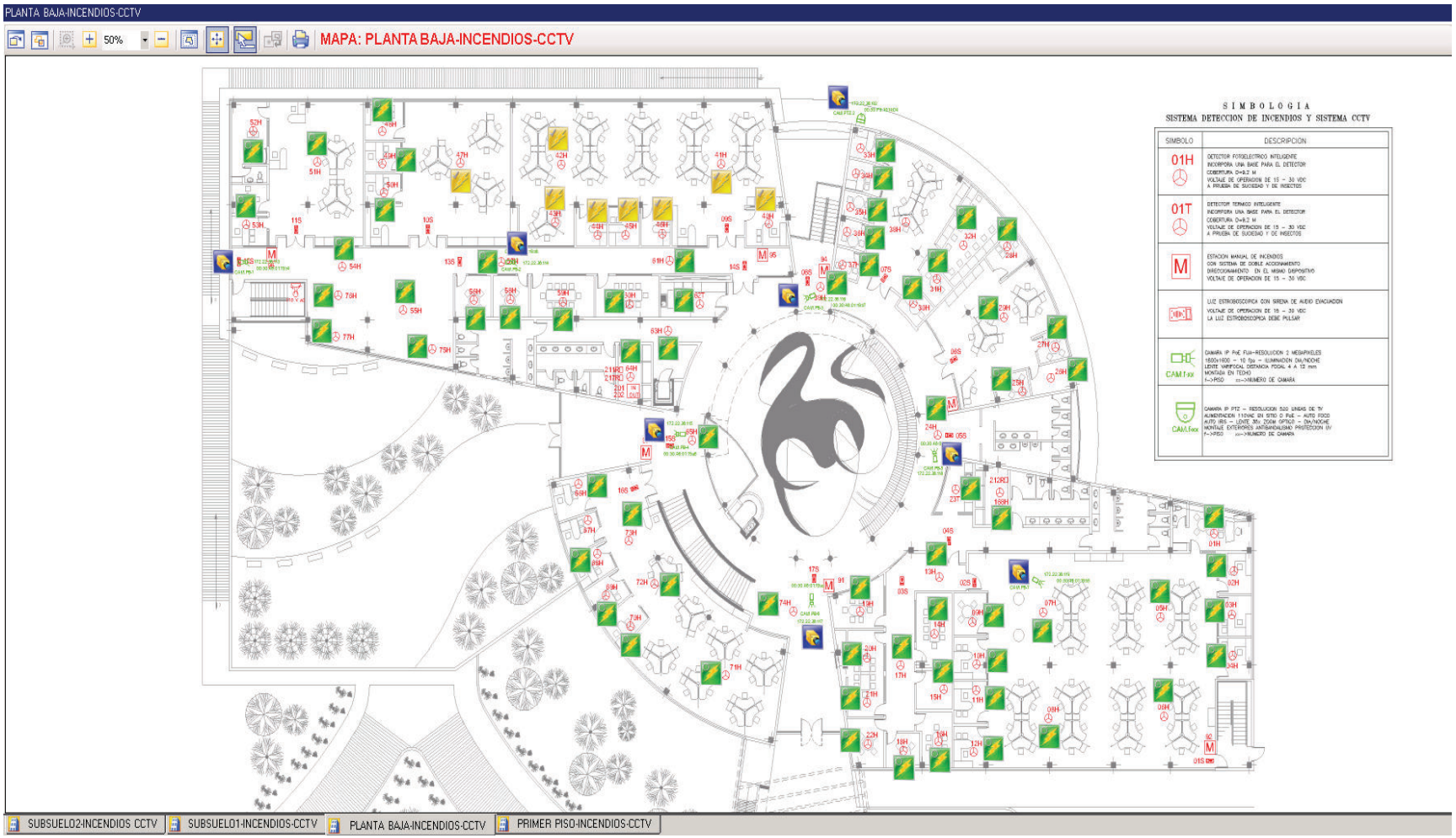
PLANOS INSTALACIÓN

Plano Subsuelo 2.

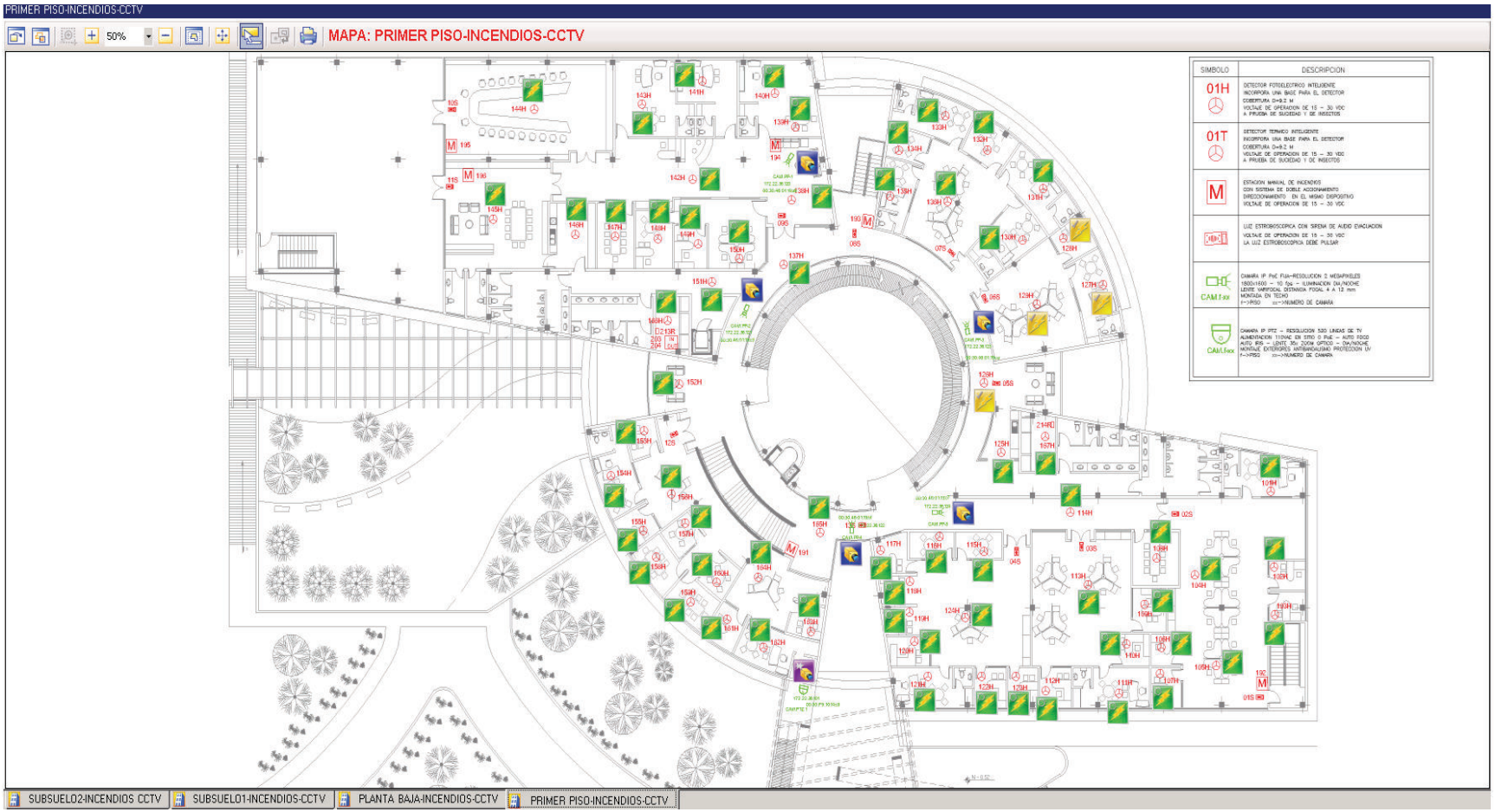
Plano Subsuelo 1.



Plano Planta Baja.



Plano Primer Piso.



Edificaciones exteriores (Comedor y Casa de estudio).

COMEDOR

CASA ESTUDIO

Edificaciones exteriores (outlet y archivo).

OUTLET

ARCHIVO