DISEÑO E INSTALACIÓN DE SISTEMAS DE SEGURIDAD ELECTRÓNICA CON SISTEMAS DE INTEGRACIÓN

Sergio Andres Moreno Avila

Código: 20161005030

Proyecto para la modalidad de pasantía

Director interno:

Ing. Gustavo Adolfo Puerto Leguizamón

Director externo:

Ing. Vianney Alexander Ruiz Ramirez

PROYECTO CURRICULAR DE INGENIERIA ELECTRÓNICA

FACULTAD DE INGENIERÍA

BOGOTÁ, COLOMBIA

2023

Agradecimientos

Primero doy gracias a mi familia por apoyarme en mis estudios y decisiones, son el pilar fundamental en mi día a día y la inspiración para desarrollar todos mis logros en mi vida. Gracias a mi universidad por permitirme desarrollarme como ingeniero y enseñarme grandes lecciones en el camino transcurrido y el que falta por recorrer.

Finalmente, y no menos importante, agradezco a la empresa CI2 por confiar en mi y permitirme realizar esta pasantía, que será el paso final para ser un profesional y el inicio de mi carrera como ingeniero. Mis especiales agradecimientos al Ingeniero Daniel Avila y al Tecnólogo Alexander Villalobos, por su paciencia, enseñanza y escucha, son maestros para mí, gracias por ayudarme en el desarrollo de este proyecto.

CONTENIDO

1. INTRODUCCIÓN ……..……2
2. OBJETIVOS ……...3
2.1. Objetivo General **……...3**
2.2. Objetivos Específicos **……3**
3. DESARROLLO DEL CRONOGRAMA DE ACTIVIDADES ……..4
3.1. Fase 1: Revisión del espacio físico **……4**
3.1.1. Listado de equipos **……...4**
3.1.2. Revisión e identificación **……4**
3.1.3. Mantenimiento **……4**
3.1.4. Cambio de equipos **……..4**
3.2. Fase 2: Pruebas **……..4**
3.2.1. Conexión de los equipos **……..4**
3.2.2. Identificación de errores **……..4**
3.2.3. Solución de errores **……..5**
3.2.4. Modificaciones **……5**
3.2.5. Evaluación **…….. 5**
3.3. Fase 3: Implementación **……5**
3.3.1. Programación **……..5**
3.3.2. Conexión **……5**
3.3.3. Aplicación **……...5**
3.3.4. Evaluación **…….. 5**
3.4. Fase 4: Socialización **……5**
3.4.1. Orientación **……..5**
3.4.2. Resultados **……...5**
3.4.3. Socialización **……...5**
4. DESARROLLO DE LOS OBJETIVOS ……...7
4.1. Revisión física y de mantenimiento preventivo de los equipos existentes en la empresa **……7**
4.2. Diseño e implementación de los sistemas de CCTV, de control de acceso, intrusión y de sistema de alarmas de incendios **……... 8**
4.2.1. Sistema de CCTV **……9**
4.2.2. Sistema de control de acceso **……12**
4.2.3. Sistema de intrusión **……..15**
4.2.4. Sistema de alarmas de incendios **……...19**
4.3. Implementación del sistema de integración **……25**
5. CONCLUSIONES Y RECOMENDACIONES ……..27
6. BIBLIOGRAFÍA ……..28

1. INTRODUCCIÓN

Los sistemas de seguridad electrónica con el transcurso del tiempo, se vuelven más y más necesarios para los diferentes establecimientos que hay en las ciudades, pueblos o zonas, llegando a ser en algunas ocasiones obligatorios incluirlos en el diseño de la edificación, como es el caso de los sistemas de alarmas de incendios, esto porque precisamente al incluir o implementar estos sistemas, se obtiene a cambio una seguridad del perímetro, control de personas o usuarios, vigilancia y memoria de los hechos de la zona comprendida, además de identificación y reacción inmediata en caso de emergencias. En este proyecto se realiza la implementación, descripción y se abordara los temas específicos de varios sistemas de seguridad electrónica, como lo son: sistema de circuito cerrado de televisión (CCTV), de control de acceso, de intrusión y sistema de alarmas de incendios.

La empresa Ci2, es una empresa colombiana que brinda al mercado nacional productos y soluciones tecnológicas a la medida. Con su diseño, ingeniería y productos de calidad reconocida, entrega a sus clientes finales soluciones para proyectos de telecomunicaciones, de seguridad electrónica, de sistemas de CCTV y aplicaciones marítimas (Compañía Internacional de Integración S.A.). Contratada por Corferias para la realización de un proyecto de seguridad electrónica en sus instalaciones.

Se plantea, realizar el diseño e instalación de diferentes sistemas de seguridad electrónica como lo son: sistema de CCTV, sistema de control de acceso, sistema de intrusión y también un sistema de alarma de incendios. Para esto se comprará el equipo necesario, dependiendo del presupuesto acordado por ambas partes, tanto la red como los dispositivos, se podrán consultar o hacerles un seguimiento en tiempo real mediante aplicaciones y software específico que brinda la marca Bosch. Es necesario centralizar la información en un equipo servidor, la totalidad de alarmas, sensores, videos y datos, para que esté disponible desde un mismo punto para los usuarios que tengan el permiso de manejar esta información. Con la intervención de este equipo servidor que dispone de todos los datos de los sistemas de seguridad electrónica, será posible la centralización y organización de toda la información de servicios para los usuarios, como consultas de ingreso y salida de personas, registro del tiempo de estadía de un usuario, detección de movimiento por área incluida, imágenes de objetos o personas, registros de video, seguridad de normalidad en áreas incluidas, en cuanto a la nula presencia de humo o fuego; como ejemplo de las funciones del sistema.

2. OBJETIVOS

2.1. Objetivo General

Diseñar e implementar la seguridad electrónica con dispositivos de la marca Bosch, que permita la integración de los diferentes sistemas, tanto los existentes como los nuevos, en la red LAN y a su vez estén centralizados en un servidor, brindando servicios de control de todos los usuarios que ingresan o están presentes y asegurando una respuesta efectiva en el caso de presentarse alguna emergencia por incendio, mediante un sistema de alarmas de incendios.

2.2. Objetivos Específicos

- Ejecutar una revisión física y de mantenimiento preventivo de los equipos existentes en la empresa, para informar cuales equipos son viables a la integración y cuales son obsoletos por su antigüedad o tecnologías diferentes.
- Diseñar e implementar los sistemas de CCTV, de control de acceso, intrusión y de sistema de alarmas de incendios de la marca Bosch, teniendo en cuenta las especificaciones dadas por el contratista.
- Implementar un servidor que permita controlar y gestionar servicios para la red instalada, entre estos centralizar toda la información del área asignada de manera organizada en un solo sitio.

3. DESARROLLO DEL CRONOGRAMA DE ACTIVIDADES

Para la realización de este proyecto se dividió en fases, con esto lo que se espera es que el mismo vaya progresando organizadamente y teniendo en cuenta unos límites de tiempo, además se permite saber que tan avanzado se encuentra el proyecto según la fase en la que se encuentra. Con las fases propuestas se planifico el cronograma de actividades.

Las fases se escogieron teniendo en cuenta los objetivos específicos, por esto mismo se dividirá en cuatro fases y cada una de estas con distintas subfases. Las fases son:

3.1. Fase 1: Revisión del espacio físico

En esta fase se realizó una revisión física y de mantenimiento preventivo de los equipos existentes en la empresa, informando cuales equipos son viables a la integración y cuales son obsoletos por su antigüedad o tecnologías diferentes. Se tienen las siguientes subfases:

3.1.1. Listado de los equipos: se hace un inventario de todos los equipos, máquinas o dispositivos electrónicos de la empresa.

3.1.2. Revisión e identificación: se clasifican los equipos antes listados en, viables o no viables a la integración del sistema.

3.1.3. Mantenimiento: si hay algún equipo que se necesita reparar o cambiar algún componente para que pueda ser integrado, además, se realiza una revisión del software y si es necesario se actualiza.

3.1.4. Cambio de equipos: se presenta una recomendación de los equipos que no son viables al dueño del establecimiento para que los cambie por otros si quiere que estos se puedan integrar al sistema.

3.2. Fase 2: Pruebas

Luego de decidir los equipos que se utilizaran, se realizó diferentes pruebas para implementar y diseñar los diferentes sistemas con los equipos actuales y nuevos de la empresa, para que presten servicios confiables y siempre disponibles en cualquier momento que se requieran. Se tienen las siguientes subfases:

3.2.1. Conexión de los equipos: se realiza la comunicación entre los equipos de la empresa y la nueva red.

3.2.2. Identificación de errores: si surgen errores para la comunicación o la señal recibida o enviada, por algún equipo que no cumple con los estándares en cuanto a calidad de la misma, se encuentra el equipo afectado.

3.2.3. Solución de errores: luego de identificar un error se solucionará discriminando si es necesario una modificación a la red o el quipo no es compatible.

3.2.4. Modificaciones: después de que la red o sistema funcione completamente, se probara si se puede realizar alguna modificación para que sea más eficiente, rápida y consuma menos recursos.

3.2.5. Evaluación: Luego de realizar las modificaciones, se escogerá la versión que mejor haya dado resultados teniendo en cuenta los requerimientos del cliente.

3.3. Fase 3: Implementación

En esta fase se implementó completamente la versión final escogida en la anterior fase, entonces se implementó un servidor que permita controlar y gestionar servicios para la red instalada, entre estos centralizar toda la información del recinto de manera organizada en un solo sitio. Se tienen las siguientes subfases:

3.3.1. Programación: se realiza la programación necesaria en todos los equipos de la empresa y la red de la versión definitiva.

3.3.2. Conexión: se realiza la comunicación entre los equipos de la empresa y la red de la versión definitiva.

3.3.3. Aplicación: se utiliza una aplicación intuitiva que permita controlar y gestionar los servicios de la red, así como también la información de todos los equipos y sistemas.

3.3.4. Evaluación: Luego de implementar completamente los sistemas se realiza una evaluación final para mostrar los resultados de todos los sistemas y demostrar que se han tenido en cuenta los requerimientos del cliente. Esta evaluación también incluye realizar una hoja de datos con las especificaciones de la red implementada y los equipos.

3.4. Fase 4: Socialización

En esta fase se orientó, explicó y se dio acompañamiento al personal para que, luego de la pasantía, puedan sacar el máximo provecho a la solución implementada, además, se realizara la socialización de lo trabajado en la pasantía en la Universidad Distrital para presentarlo como trabajo de grado. Se tienen las siguientes subfases:

3.4.1. Orientación: se explica de forma clara y sencilla el funcionamiento de los sistemas y la aplicación, para que puedan realizar las acciones que deseen.

3.4.2. Resultados: se muestran los resultados de la red implementada y la comparación de lo que se tenía antes, de ser el caso, y la mejora de lo que se desarrolló, evidenciando que se realizó una buena inversión.

3.4.3. Socialización: en la Universidad Distrital se socializará lo desarrollado como modalidad de pasantía.

Fases	Subfases	Mes 1					Mes 2 a Mes 3								Mes 4 a Mes 5						Mes 6		
3.1. Fase1	3.1.1																						
	3.1.2																						
	3.1.3																						
	3.1.4																						
3.2. Fase2	3.2.1																						
	3.2.2																						
	3.2.3																						
	3.2.4																						
	3.2.5																						
3.3. Fase3	3.3.1																						
	3.3.2																						
	3.3.3																						
	3.3.4																						
3.4. Fase4	3.4.1																						
	3.4.2																						
	3.4.3																						

Tabla 3.1. Cronograma de actividades.

En la tabla 3.1. se observa cronograma del desarrollo del plan de trabajo en el cual se incluyen las fases y subfases, todo esto para un periodo máximo de seis meses. Un rectángulo pequeño representa una semana, lo que da un total de 22 semanas.

4. DESARROLLO DE LOS OBJETIVOS

4.1. Revisión física y de mantenimiento preventivo de los equipos existentes en la empresa

Este primer objetivo se relaciona con la fase 1 del plan de trabajo, se presentan los equipos con su respectiva referencia, además, si son viables o no viables para la integración del sistema total, por medio de la siguiente tabla.

Equipo	Referencia	Viable	No Viable	Mantenimiento
Módulo de lazo	LSN 0300A	X		
Módulo de zona	NZM 0002 A	X		
Detector de incendios	FAP-OT 420		X	
Detector lineal de humo	D296	X		X
Pulsador manual	FMC-420RW-GSRRD	X		
Sirena con estrobo	W-HSR	X		
Fuente de alimentación	D9142F	X		
Módulo de entrada	FLM-420-I2-D	X		
Módulo interconexión	FLM-420/4-CON-S	X		
Teclado remoto	FMR-5000-02	X		
Controlador de acceso	APC-AMC2-4WCF	X		
Fuente de poder	APS-PBC-60	X		
Lector de tarjetas	6100CKN0000	X		
Electroimán	E-941SA-600	X		X
Detectores de apertura	ISN-CSM35-W	X		
Panel de control intrusión	D9412GV3-C	X		
Teclado	D1260B	X		
Módulo de interfaz de red	DX4020	X		
Módulo de direccionamiento	D9127U	X		
Detector de movimiento	ISC-PPR1-W16	X		X
Detector de movimiento 360°	DS939		X	
Detector rotura de cristal	DS1101i	X		
Cámara de video domo	VG4-324-ECE1M		X	
Cámara de video domo	NDP-7512-Z30K	X		
Cámara de video 180°	NFN-70122-F1A	X		X
Cámara de video fija	NDN-498V09-22PS	X		
Almacenamiento de video	DLA-AIOL1-08AT	X		

Tabla 4.1. Listado de equipos.

De la tabla 4.1. se observan divisiones horizontales en negrilla que indican elementos de un mismo sistema de seguridad electrónica, algunos dispositivos no eran viables para la integración con el sistema que se quiere implementar, en algunos casos por que son antiguos y el software no es compatible o también porque se encuentran dañados. Los equipos que necesitan mantenimiento, es porque están descalibrados en el caso de los detectores o sucios por acumulación de polvo impidiéndoles su correcto funcionamiento, para estos casos se realiza la tarea correspondiente para que el equipo se pueda integrar en la red y funcione correctamente.

4.2. Diseño e implementación de los sistemas de CCTV, de control de acceso, intrusión y de sistema de alarmas de incendios.

Este objetivo se desarrolla en las fases 2 y 3 del plan de trabajo. Primero, para el diseño de los sistemas se presenta el área donde se trabajó.

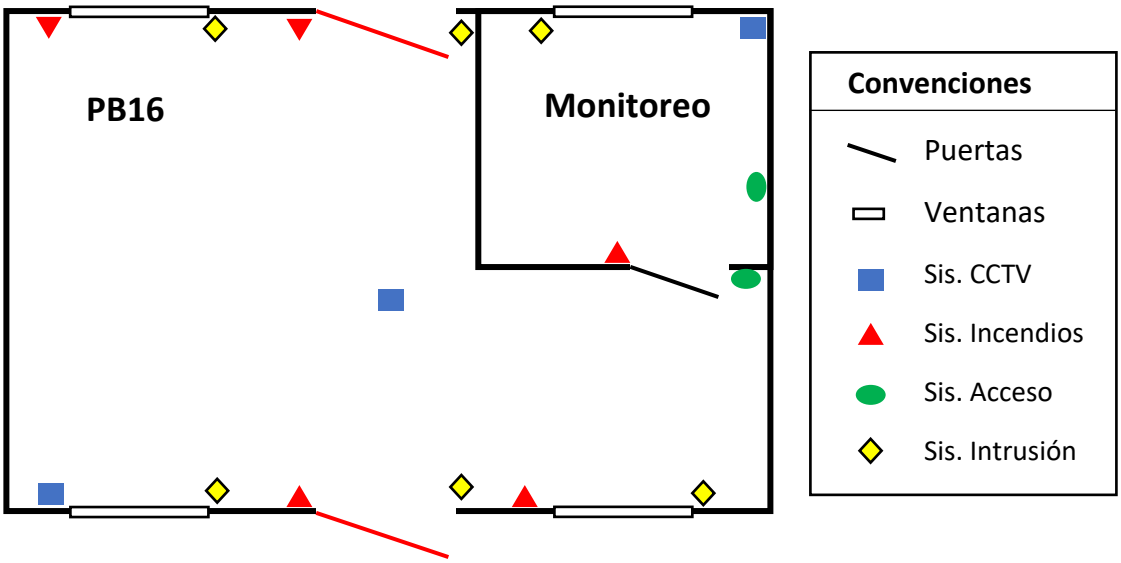


Figura 4.2.1 Plano y sistemas de seguridad electrónica.

En la figura se observa un plano sencillo del área de trabajo (PB16 significa pabellón 16), además como se ve en el cuadro de convenciones también se encuentra la disposición de los elementos que conforman cada uno de los distintos sistemas de seguridad electrónica, siendo este el diseño desarrollado, a continuación, se explicara específicamente la implementación de cada uno de los sistemas.

4.2.1. Sistema de CCTV

La incorporación de Circuitos Cerrados de Televisión (CCTV) dentro de una empresa es una función crítica para cualquier departamento de seguridad. Ha habido muchas mejoras en los equipos de CCTV a lo largo de los años. Las cámaras se han vuelto capaces de extremos mucho más amplios en la iluminación de fondo, lo que hace que las cámaras sean bastante económicas y capaces de obtener imágenes confiables incluso en condiciones de poca luz. Un punto importante es que están disponibles con tecnología de protocolo de información (IP) integrada en la cámara, por lo tanto, todo lo que debe agregarse para permitir que la cámara funcione en Internet es una dirección IP. Además, se han vuelto mucho más robustas y no tan sensibles a la iluminación de alta intensidad que ingresa repentinamente en el campo de visión y hace que la cámara se sature, (Pearson, 2007).

Para este sistema se tienen tres tipos de cámaras de video:

- Cámara de video panorámica de 180°:

- Sensor 12 MP/30 ips para detalles precisos con movimiento fluido
- Corrección de deformación de bordes o en el lado cliente para facilitar la integración
- Descripción general de Intelligent Video Analytics en panorámica completa
- Diseño discreto y elegante para montaje encastrado en techo
- Cubierta embellecedora que se puede pintar fácilmente para una instalación discreta

Figura 4.2.1.1 Cámara de video 180°. Tomada de: Bosch, NFN-70122-F1A.

Esta cámara tiene una visión de 180°, por lo que su posicionamiento es en la parte inferior izquierda del plano de la figura 4.2.1, desde este punto ve toda el área correspondiente al pabellón 16.

- Cámara de video domo PTZ:

- Tecnología Starlight con excelente rendimiento con baja iluminación y Alto rango dinámico de 120 dB para ver detalles en condiciones de iluminación adversas
- Incorpora la última tecnología de compresión de vídeo H. 265 para reducir los requisitos de almacenamiento y ancho de banda
- Intelligent Video Analytics integrado avisa a los operadores en caso de actividad inusual en la escena
- Tecnología inteligente de vanguardia con Intelligent Tracking y detección de objetos, incluso con la cámara en movimiento

Figura 4.2.1.2 Cámara de video domo. Tomada de: Bosch, NDP-7512-Z30K.

La principal ventaja de la cámara tipo domo es que permite el movimiento 360° horizontalmente y 180° verticalmente, por esto se puede enfocar un evento particular, aunque siempre se dejan con un recorrido preestablecido para que pueda observar distintas áreas. Esta cámara se ubico en el centro del pabellón 16.

- Cámara de video fija:

- CCD día/noche de 1/3 de pulgada con exploración progresiva
- tecnología de procesamiento de imágenes de 20 bits
- Amplio rango dinámico, motor 2X-dynamic y SmartBLC
- Transmisión cuádruple
- Opciones de grabación flexibles
- Inteligencia al borde
- ONVIF conformando

Figura 4.2.1.3 Cámara de video fija. Tomada de: Bosch, NDN-498V09-22PS.

Se utiliza en la zona de monitoreo, ya que es un cuarto pequeño, principalmente tiene que estar apuntando a la puerta, pero con esto alcanza a grabar todo el cuarto, esta en la parte superior derecha en el cuarto de monitoreo de la figura 4.2.1.

- Implementación

Con la distribución mencionada de estas cámaras se cubre toda el área asignada, se le asignan direcciones IP a cada una para poderlas reconocer en la red LAN y observar su información, la configuración se realiza por medio del software de Bosch BVMS (BVMS Bosch, 1886) y Configuration Manager, para observar las cámaras en directo o las grabaciones se utiliza la aplicación Operator Client.

a) Cámara 180°

b) Cámara domo PTZ

c) Cámara fija

Figura 4.2.1.4 Implementación física de cámaras de video.

Una vez instaladas se procede a realizar la configuración teniendo en cuenta que estas cámaras pertenecen a un mismo grupo, a continuación, un ejemplo de la programación de una cámara.

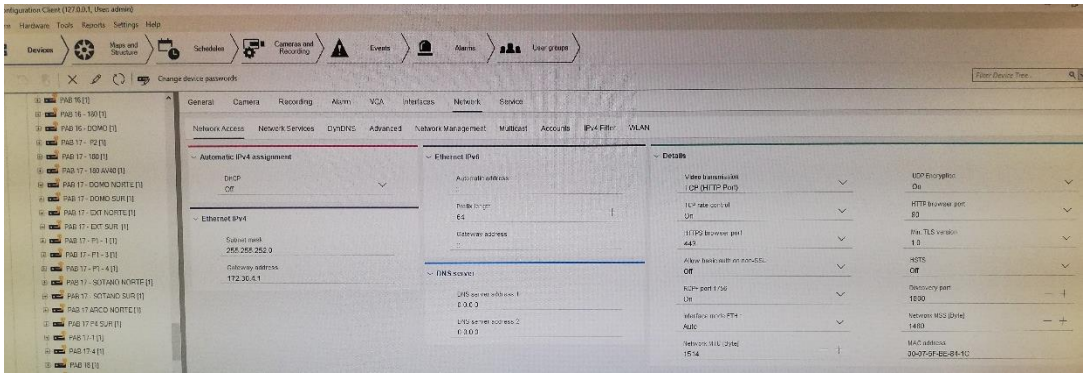


Figura 4.2.1.5 Programación de cámaras de video.

Lo necesario para que una cámara entre en la red y se pueda visualizar el video es, crear una contraseña, ingresar un dirección IP en la cual se encuentre la red LAN, la máscara de subred, la dirección de la puerta de enlace (en este caso no se contaba con un servidor DHCP, por esto es necesario esto), número de puerto HTTP, nombre por el cual se identifica la cámara y asignar el grupo al cual va a pertenecer.

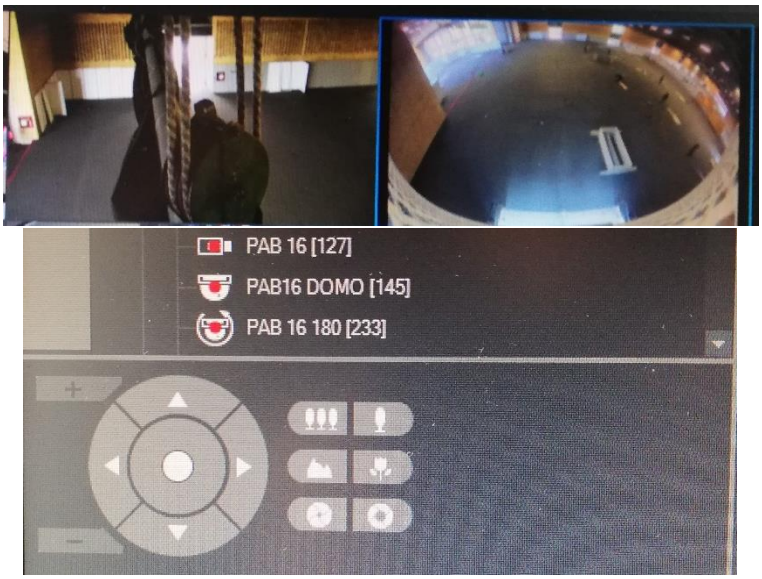


Figura 4.2.1.6 Video en directo de las cámaras.

Como se ve en la figura 4.2.1.6 las cámaras programadas se encuentran funcionando correctamente, se observa la vista de la cámara tipo domo PTZ, a esta se le incluyó un recorrido predeterminado que realiza siempre que no se este operando manualmente con los controles, también se observa la vista en vivo de la cámara tipo panorámica de 180°.

4.2.2. Sistema de control de acceso

Es el componente más expuesto de un programa de seguridad electrónica, ya que va a ser el primero con el que se va a encontrar cualquier usuario al querer ingresar a un recinto. Los empleados, contratistas, clientes y visitantes conocen su sistema de control de acceso electrónico, porque normalmente, los empleados utilizan el sistema a través de una credencial todos los días para acceder a su área de trabajo (Pearson, 2007). Por esto las empresas que implementan sistemas de control de acceso, hoy en día clasifican a los diversos grupos de personas que visitan o trabajan en sus instalaciones como empleados y no empleados.

- Lector de tarjetas sin contacto

Se decidió usar un lector de tarjetas sin contacto para el ingreso al cuarto de monitoreo, las otras dos puertas en rojo no son de acceso son puertas de emergencia por esto tienen ese color, como se ve en la figura 4.2.1.

Dimensiones
1,9" x 4,1" x 0,9" (4,8 cm x 10,3 cm x 2,3 cm)
Admite tarjetas inteligentes sin contacto de 13,56 MHz.
iCLASS Seos®, iCLASS SE, iCLASS® estándar, MIFARE® Classic y MIFARE DESFire®EV1
Protocolo
Modo de protocolo abierto de dispositivo supervisado (OSDP)
Modos Wiegand o de "reloj y datos" (clock & data)
Garantía
Garantía contra defectos en los materiales y mano de obra durante un año. (Consulte todos los detalles en la póliza de garantía).

Figura 4.2.2.1 Lector de tarjetas sin contacto. Tomada de: HID, HID® iCLASS SE® R10.

Se implementaron dos lectores de tarjetas inteligentes en la puerta de monitoreo, uno para la entrada y otro para la salida, como se observa en la figura 4.2.1, ya que esta es un área importante y en la cual se debe restringir el acceso, teniendo en cuenta que es donde se concentra toda la información de los sistemas de seguridad electrónica.

- Implementación

Para la configuración de los dispositivos se utiliza el software Access Engine (ACE), en el cual se programan las tarjetas del personal autorizado para ingresar, teniendo en cuenta que toda la información pasa antes por el controlador de acceso (*Engineered Solutions-AMC2: Controlador Modular de Acceso AMC2: Controlador Modular de Acceso*, n.d.) que incluye la fuente de alimentación de la lectora.

Figura 4.2.2.2 Controlador de acceso implementado.

Figura 4.2.2.3 Lectores de tarjetas de entrada y salida, implementado.

Con los equipos instalados se procedio a realizar la configuración del sistema de control de acceso.

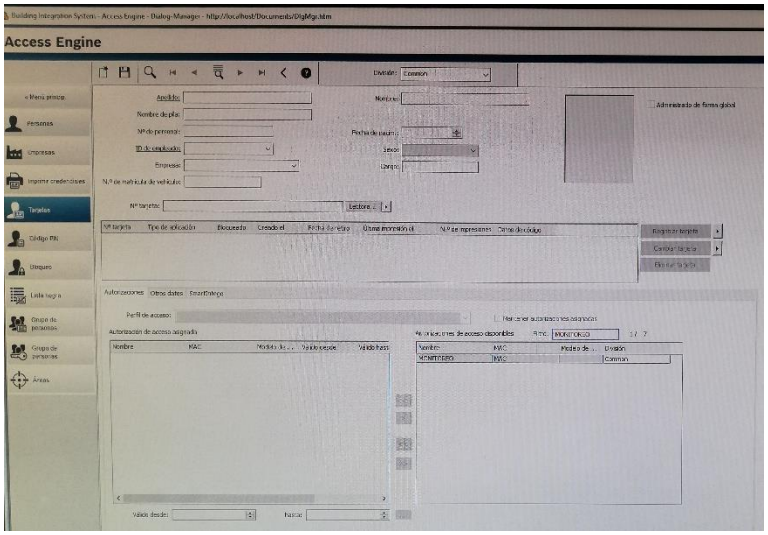


Figura 4.2.2.4 Configuración sistema de control de acceso.

Por medio del software Access Engine (*Access_Engine*, n.d.), una vez conectado se escanea para detectar el controlador y su información, se asigna a un grupo y se programan las tarjetas necesarias para los usuarios que necesitan acceder por esta puerta. En la figura 4.2.2.4 se observa la ventana en la cual se crean los usuarios, además, se le dan los permisos de las áreas correspondientes para que pueda ingresar, según indica el jefe se seguridad de la empresa.

4.2.3. Sistema de intrusión

Existen muchas opciones posibles, pero hay cuatro tecnologías ampliamente utilizadas en cuanto a la lectura de credenciales: banda magnética, Weigand, proximidad y tarjeta inteligente sin contacto. Dependiendo de la tecnología implementada se verá en consecuencia una diferencia en la manipulación y uso de los servicios que ofrece el lector. Con banda magnética y tecnología Weigand, la credencial debe pasarse físicamente tocando el lector. Con las tecnologías de tarjetas inteligentes de proximidad y sin contacto, la credencial se puede colocar a una corta distancia frente al lector sin llegar a tener contacto. La tecnología utilizada también afectará otros aspectos, como el costo, la facilidad de falsificación, el equipo de codificación de credenciales y las ubicaciones de montaje del lector, (Pearson, 2007).

- Detector de movimiento

- Cobertura estándar de 18 m x 25 m (60 pies x 80 pies); cobertura de corto alcance seleccionable de 8 m x 10 m (25 pies x 33 pies)
- Tecnología de fusión de datos de los sensores
- Tecnología de óptica trifocal
- Supresión activa de la luz blanca
- Compensación dinámica de temperatura
- Prueba de paseo remota
- Memoria de alarmas
- Inmunidad contra corrientes e insectos
- Altura de montaje de 2 m a 3 m (de 7 pies a 10 pies); no se necesitan ajustes

Figura 4.2.3.1 Detector de movimiento. Tomada de: Bosch, ISC-PPR1-W16.

Los detectores se instalan cerca a las puertas, esto porque es un punto clave teniendo en cuenta una intrusión, porque es el lugar por el que se puede entrar o salir al área asignada, es decir son puntos de convergencia de actividad, que son fuentes importantes de información ante cualquier eventualidad (*ISC_PPR1_W16_Data_sheet*, n.d.). Se instalan dos detectores de movimiento cada uno cerca a cada puerta de emergencia, como se observa en la figura 4.2.1, en el cuarto de monitoreo no se instalan ya que siempre tiene que haber una persona en este recinto, se tiene una cámara que observa completamente el cuarto, además, para el ingreso se necesita una tarjeta inteligente porque existe una restricción de entrada por lector de tarjetas, por lo que se decide no poner un detector de movimiento en monitoreo.

- Detector de rotura de cristal

Figura 4.2.3.2 Detector de rotura de cristal. Tomada de: Bosch, DS1101i.

Los detectores de rotura de vidrio se instalan en todas las ventanas y en las puertas de emergencia ya que estas también tienen cristal, en total se implementan seis como se observa en la figura 4.2.1 (*Intrusion Alarm Systems | DS1101i Series Detectores de Roturas de Cristal*, 2016). Teniendo en cuenta los detectores de movimiento antes instalados, otro punto clave para detectar una intrusión son las ventanas, que son un punto débil de la estructura, porque es la segunda forma de entrar o salir más fácil en caso de una intrusión.

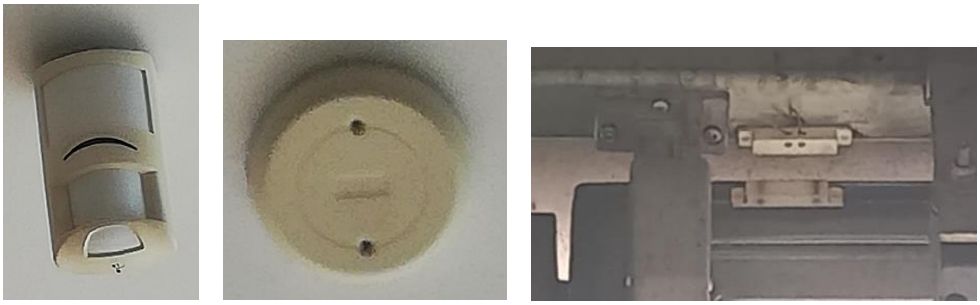
- Detector de apertura de puerta

Figura 4.2.3.3 Contactos. Tomada de: Bosch, ISN-CSM35-W.

Se utilizan contactos como se ven en la figura 4.2.3.3, como detectores de apertura de puerta. Se instalan en cada puerta que se observa en la figura 4.2.1 (por esto no se señalan, considerando una saturación de información en la figura), se implementaron un total de tres contactos.

- Implementación

Una vez instalados todos los dispositivos necesarios se procede a realizar la programación, esto por medio del software RPS de Bosch (*Intrusion Alarm Systems-Software de Programación Remota*, 2023), en donde se leerán todos los detectores conectados a la central desde donde se está programando y se podrán asignar a áreas o grupos dependiendo de los requerimientos solicitados.



a) D. movimiento b) D. rotura de cristal c) D. apertura

Figura 4.2.3.4 Implementación física de detectores de intrusión.

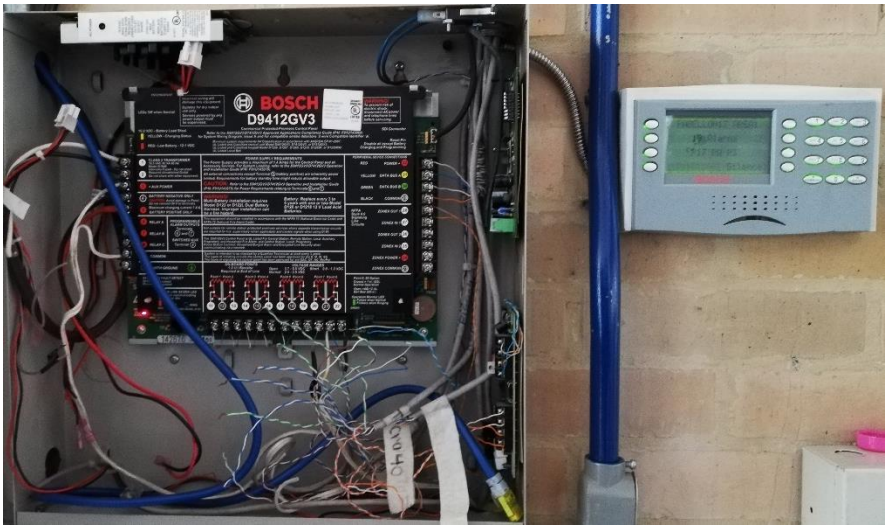


Figura 4.2.3.5 Implementación de la central del sistema de intrusión.

En las figuras antes mostradas se encuentran en general todos los dispositivos más importantes para el funcionamiento del sistema de intrusión. Para realizar la programación, se necesita realizar una comunicación mediante red, teniendo en cuenta la finalidad de este proyecto que es realizar la centralización de la información de todos los sistemas, por esto se presenta a continuación la configuración del módulo de interfaz de red y luego la configuración de la central de intrusión.

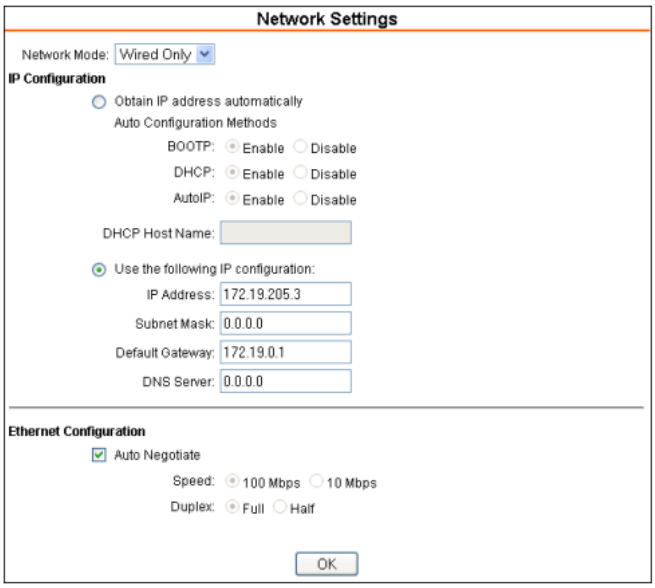


Figura 4.2.3.6 Configuración módulo de interfaz de red.

En esta primera parte se realiza la comunicación entre el modulo de red y el computador, para esto previamente es necesario ajustar los parámetros de asignación de dirección IP, mascara de subred, puerta de enlace, número de puerto, entre otros, esto se realiza en la ventana de comandos.

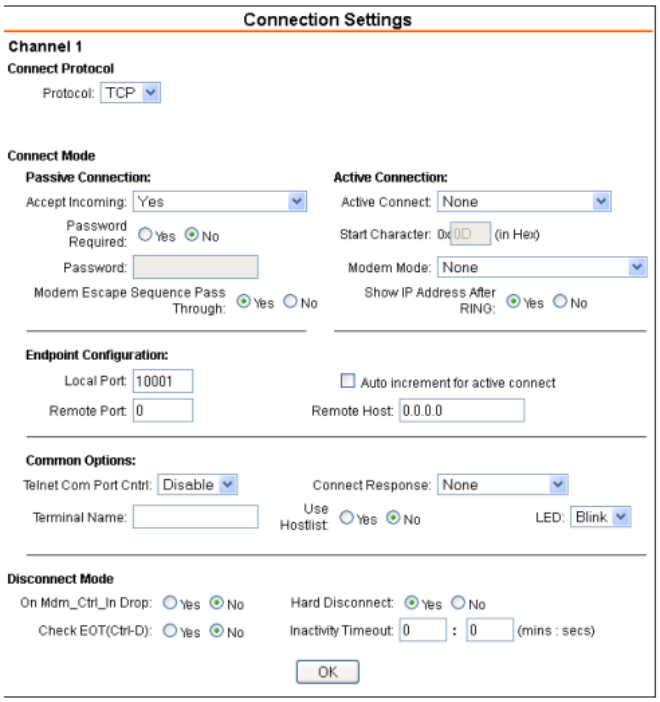


Figura 4.2.3.7 Configuración módulo de interfaz de red, opciones de conexión.

Después de se ingresa por medio de la red LAN con la IP asignada a las configuraciones de red mostradas en la figura 4.2.3.6 y figura 4.2.3.7 (Lantronix, 2018), en estas se ingresa

nuevamente la dirección IP, la máscara de subred y en general las mismas configuraciones realizadas en la ventana de comandos, pero hay opciones adicionales de red que hay que configurar, como lo son las opciones seriales o las opciones de conexión (figura 4.2.3.7) que para este proyecto el protocolo es TCP. Con esto ya se puede realizar la programación del panel de intrusión y sus dispositivos conectados.

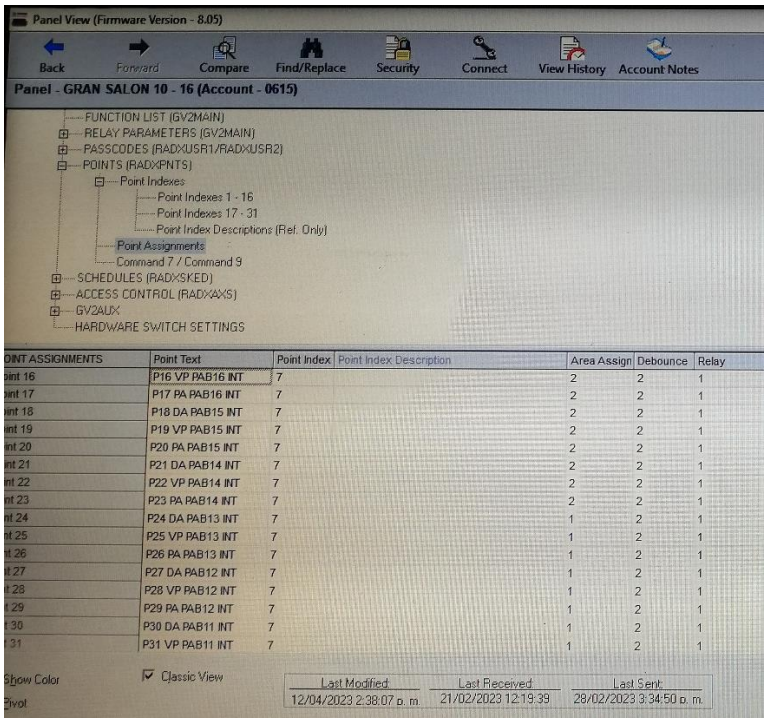


Figura 4.2.3.8 Configuración sistema de intrusión.

Realizada la conexión, se puede acceder al software RPS y detectar la central de intrusión por conexión mediante red, porque la que utilizamos en el futuro para integrar todos los sistemas. En este programa se asignan nombres a cada dispositivo emparejandolo con su dirección IP asignada, tambien se asignan grupos, permisos o configuraciones especiales como tiempo de funcionamiento, entre otros. La figura 4.2.3.8 muestra la configuración realizada para los dispositivos del pabellón 16 y monitoreo.

4.2.4. Sistema de alarmas de incendio

La respuesta a incendios y emergencias es importante para cualquier empresa o recinto y debería ser una obligación para garantizar la seguridad del personal. Los dispositivos iniciadores para este tipo de sistema independiente son detectores de humo, detectores de calor, estaciones manuales, detectores de humo de conducto, detectores de humo de haz y varios otros dispositivos especiales. El siguiente grupo son los dispositivos anunciadores o, como se denominan en el código, dispositivos de notificación. Estos son los dispositivos que notifican a los ocupantes del área que hay una alarma. Están disponibles en varias formas. Pueden ser campanas, bocinas, sirenas, altavoces y/o luces estroboscópicas, (Pearson, 2007).

Los dispositivos audibles deben cumplir con el código. El código requiere que existan tres señales o tonos audibles distintos para los diferentes tipos de alarmas: uno para problema, uno para supervisión y otro para incendio.

Se utilizan los siguientes componentes:

- Detector de humo lineal

- Funciona a distancias de entre 9 m y 107 m.
- Seis niveles de sensibilidad seleccionables mediante un conmutador
- Miras de alineación y protección antisabotaje integradas
- Ajuste automático del rango, sincronización de señal y ajuste de contaminación
- La placa indicadora remota anuncia el estado del detector y proporciona puntos de prueba para monitorizar la tensión

Figura 4.2.4.1 Detector de humo lineal. Tomada de: Bosch, D296.

Se eligió este tipo de detector de humo teniendo en cuenta el espacio. Como el área a cubrir es mayor a sesenta metros cuadrados, estos detectores permiten cubrir largas distancias en línea recta. Se compone de un transmisor y un receptor, por lo que es necesario calibrar tanto el objetivo del transmisor para que apunte directamente al receptor y también variando el conmutador se elige la distancia efectiva del detector (*Datasheet_D296_Data_sheet*, n.d.). Teniendo en cuenta la ventaja de distancia alcanzada del detector solo se necesitaron tres detectores compuestos de un par transmisor y receptor, en la figura 4.2.1 solo se señala al transmisor sabiendo que el receptor se encuentra directamente al frente.

- Pulsadores de incendio

- Activación de la alarma pulsando la señal o rompiendo el cristal
- Protección contra daños con cristal laminado y pegatina
- LED indicador de alarma activada o de inspección
- Identificación individual del pulsador de alarma de incendio
- Rutinas de consultas de pulsadores de alarma de incendio con evaluación y transmisión múltiple
- Mantiene las funciones del bucle LSN en caso de interrupción de los cables o de cortocircuito gracias a dos aisladores integrados

Figura 4.2.4.2 Pulsadores de incendio. Tomada de: Bosch, FMC-420RW.

Se instalan los pulsadores de incendios al lado de las puertas como se observa en la figura 4.2.1, por lo que se utilizan tres pulsadores en total, se utilizan solo de color rojo. Estos pulsadores cuando se activan se cambia el papel blanco que se ve en la pequeña abertura rectangular, para dejarlo normal nuevamente es necesaria una llave especial.

- Bocinas con luz estroboscópica

Figura 4.2.4.3 Bocinas con luz estroboscópica. Tomada de: Bosch, W-HS.

Las bocinas con estrobo se instalan encima ,por lo menos a dos metros de la estación manual, en la figura 4.2.1 tienen la misma ubicación de los pulsadores, por lo que se representa por el mismo símbolo, se implementaron tres bocinas cada una cerca de una puerta. Se activan inmediatamente cuando se pulsa una estación manual, se detecta humo o se activan directamente desde monitoreo.

- Módulos de interconexión

Figura 4.2.4.4 Módulos de interconexión. Tomada de: Bosch, FLM-420/4-CON.

Estos módulos se utilizan para integrar en el lazo a los detectores de incendios lineales y poder reconocerlos individualmente por medio de tres dígitos, con el fin de identificar de donde proviene el fuego en caso de incendio. Por esto se utilizan tres módulos en la misma posición de los detectores lineales. Además, estos módulos reportan falla en caso de cortocircuito, funcionamiento erróneo del detector o circuito abierto por daño en los cables.

- Implementación

Se realiza la conexión de todos los dispositivos con el cable especial para interconexión de elementos para alarmas de incendio, en este caso se usó cable Rojo (305m) 5220UL-0021000 Belden. Después de instalar los equipos, lo primero que se trabajara es la calibración de los detectores de incendios lineales, para estos se necesita primero calibrar mecánicamente la posición para que el transmisor se encuentre con el receptor, luego se ajusta precisamente con el multímetro midiendo voltaje.

Figura 4.2.4.5 Calibración detectores de humo.

De la hoja de datos se obtiene el rango de funcionamiento correcto para el detector de incendios lineal, este va desde 3.8 hasta 4.2 voltios (*Datasheet_D296_Data_sheet*, n.d.), por lo que se observa que todos los mostrados en la figura 4.2.4.5 están bien calibrados.

Figura 4.2.4.6 Implementación pulsadores de incendio y sirena con estrobo.

Se observa la implementación de las estaciones manuales de incendio y la sirena con estrobo en la figura 4.2.4.6, para activar el pulsador se presiona donde indican las flechas negras.

Figura 4.2.4.7 Central de incendios implementada.

Se observa la central del sistema de alarmas de incendio, recibe toda la información de los detectores de incendio, pulsadores y módulos de interconexión, también permite activar o desactivar las sirenas de incendio o desactivar cualquier dispositivo (*FMR_5000_C_Data_sheet*, n.d.). Ahora se presenta la programación que se realiza por medio del software FSP-5000-RPS.

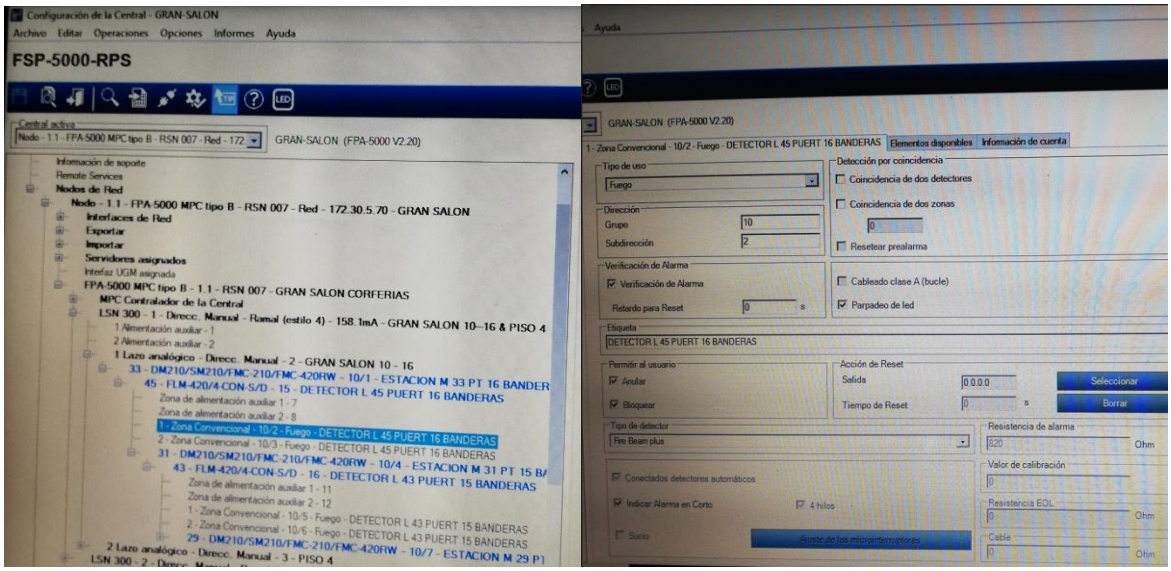


Figura 4.2.4.8 Programación detector de humo lineal.

En la configuración se ingresa el grupo y subdirección del detector elegido, esto es para ubicarlo y activarlo con el mismo conjunto que el ingresado, se selecciona el tipo de uso, fuego para este caso y dependiendo de los requerimientos se selecciona como dispara la alarma y cuanto retraso es necesario para activarla.

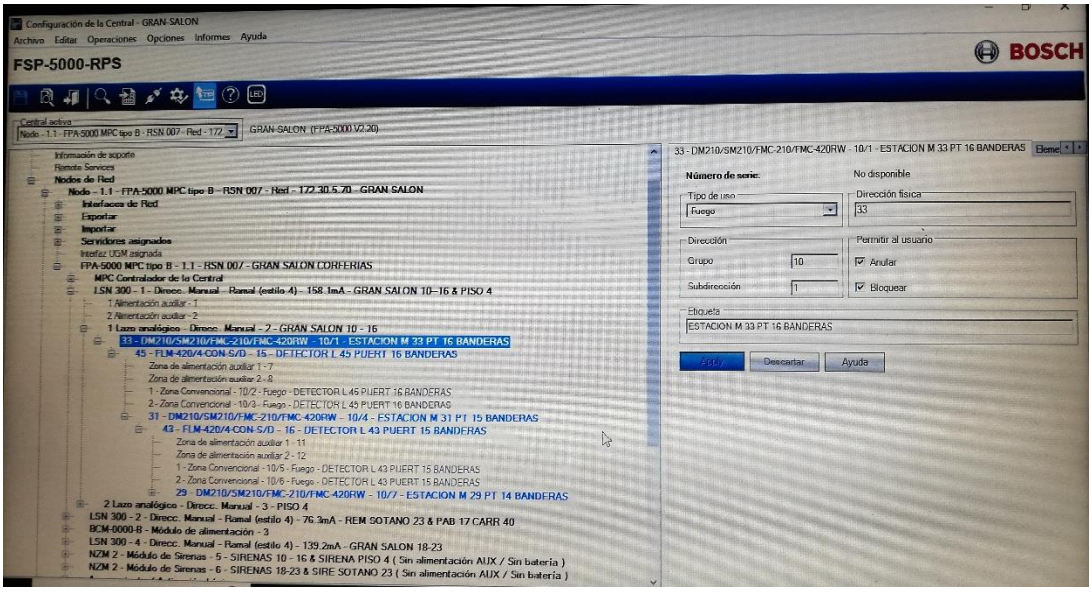


Figura 4.2.4.9 Programación pulsador de incendio.

Para una estación manual se configura el tipo de uso, fuego, la dirección física e igualmente el grupo y la subdirección, como se esta programando estos dispositivos en una misma zona (pabellón 16), se ingresa el mismo grupo (10), para la subdirección dentro de un mismo grupo no puede haber dos dispositivos con el mismo valor, para diferenciarlos.

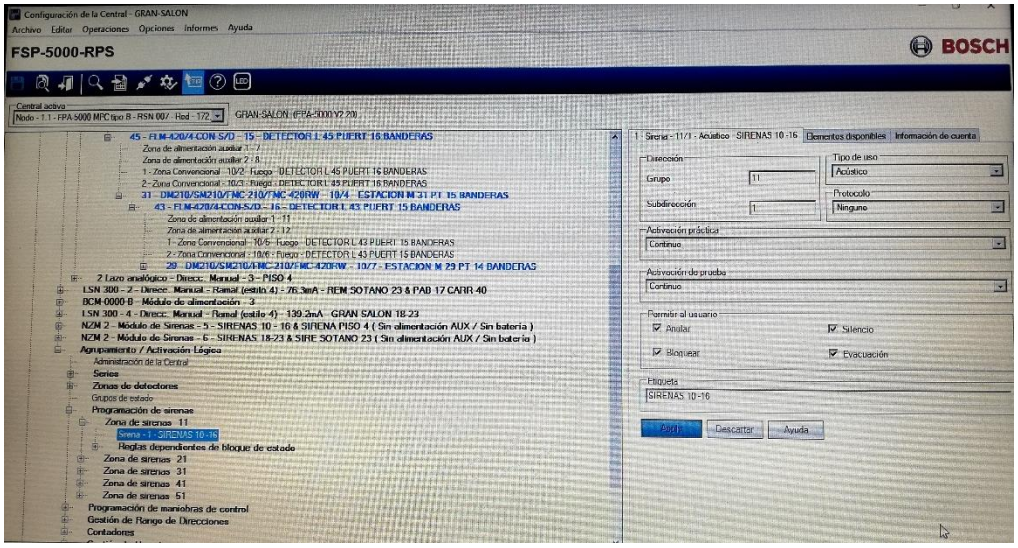


Figura 4.2.4.10 Programación activación de sirenas.

En la figura 4.2.4.10 se observa la programación de las sirenas, en donde se ingresa un valor de grupo diferente para identificar a todas las sirenas de ese mismo grupo y se dan permisos para que el usuario pueda ejecutar diferentes acciones como anular, silenciar o bloquear.

4.3. Implementación del sistema de integración

El desarrollo de esta sección es igual de importante que la anterior, porque es la segunda componente fundamental de este proyecto, en la cual se implementara el sistema de integración para centralizar la información de todos los sistemas expuestos en la sección 4.2, en un servidor, permitiendo una lectura general del estado y de cualquier advertencia o alarma por parte de cualquiera de los sistemas de seguridad electrónica en uso. Este objetivo se desarrolla en las fases 2 y 3 del plan de trabajo.

En general para este proyecto como requerimiento se solicito trabajar con la marca Bosch y esta nos ofrece una solución para el problema planteado, el sistema BIS, Bosch Building Integration System (BIS) es un software que administra diferentes sistemas de seguridad electrónica de Bosch, como el control de acceso, videovigilancia, alarmas de incendios o sistemas de intrusión, en una única plataforma, tomado de (BIS Bosch, 1886). Por lo que al utilizar los productos y programas de la marca Bosch en todos los sistemas implementados anteriormente, solo queda reunir los sistemas bajo el sistema BIS.

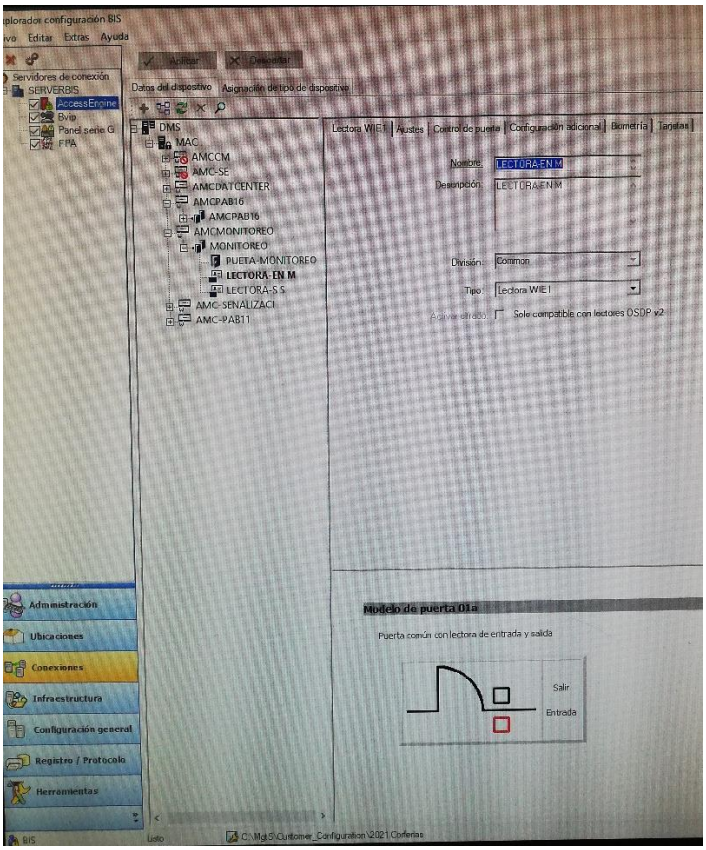


Figura 4.3.1 Programación del software Access Engine en BIS.

Se observa en la figura 4.3.1 la integración del software del sistema de acceso Access Engine, en este caso el programa se esta ejecutando desde la plataforma BIS por lo que esta seria una aplicación para cliente, se programo para que desde esta entrada se puedan registrar nuevos usuarios en la lectora de monitoreo como se observa en la figura 4.3.1.

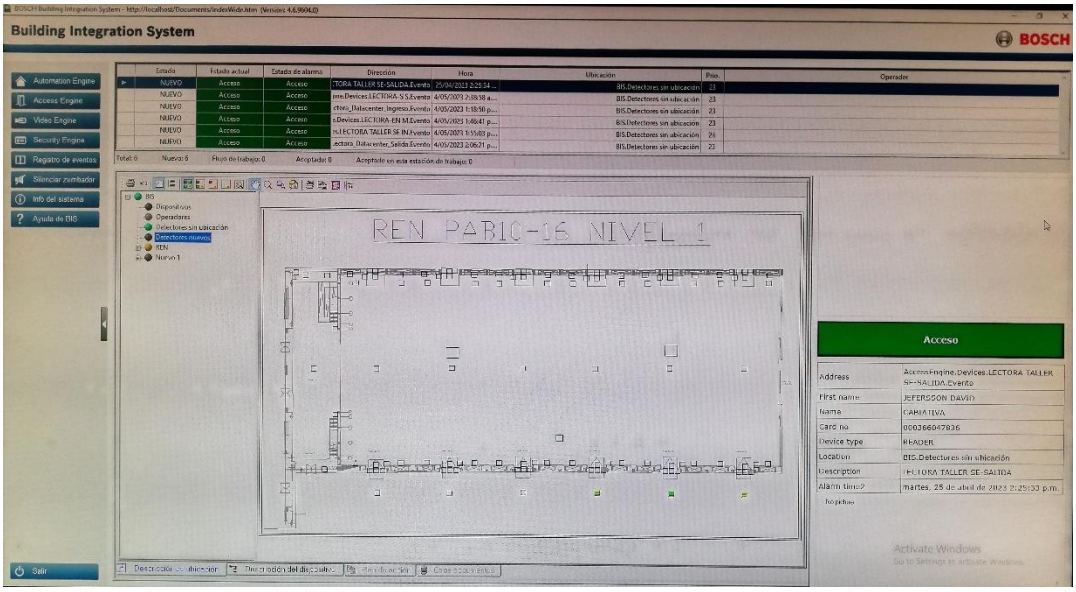


Figura 4.3.2 Vista general plataforma BIS.

Los sistemas de intrusión, alarmas de incendios y CCTV, se integran ingresando las configuraciones de los equipos existentes teniendo en cuenta que tienen que estar relacionadas a las realizadas en cada uno de los programas individuales para cada sistema. Realizando esto en el sistema BIS ya se pueden recibir las alarmas o indicadores de todos estos sistemas, como se observa en la figura 4.3.2 en la parte superior llegan las notificaciones de los distintos sistemas. Ahora el sistema BIS permite subir planos realizados en el software AutoCAD, como se observa en la figura 4.3.2 debajo del cuadro de las notificaciones se observa el plano para los pabellones del 10 al 16, para observar de manera grafica la activación de las alarmas o los sucesos que ocurren en directo, como la lectura de una tarjeta inteligente, notificación del sistema de control de acceso. De esta manera los usuarios capacitados pueden observar y registrar cualquier alarma que se reciba desde cualquiera de los sistemas de seguridad electrónica implementados: Sistema CCTV, de control de acceso, de intrusión y de alarmas de incendio.

5. CONCLUSIONES Y RECOMENDACIONES

La seguridad electrónica es fundamental para cualquier recinto, como también explorar los diversos sistemas y componentes disponibles para lograr un sistema robusto que asegure el perímetro ante cualquier irrupción. Lo mínimo recomendable es tener los siguientes cuatro sistemas de seguridad: Sistema de CCTV, con las diversas cámaras y transmisión de imágenes en las zonas designadas, además con un monitoreo a distancia de las imágenes procesadas, que son archivadas. Sistema de control de acceso, registrando entradas y salidas del recinto se tendrán diferentes controles como el usado en el proyecto, lector de tarjetas inteligentes sin contacto, este sistema procesa y almacena los datos de registro de los usuarios y asigna permisos a cada uno según la zona. Para el sistema de intrusión, detecta la presencia de una persona no permitida en un área específica, por medio de detectores de movimiento, ruptura de cristal y de apertura de puertas. Por último, el sistema de alarma contra incendios, da respuesta a emergencias, como fuego, humo o aumento de la temperatura, para este sistema se utilizan elementos especiales que tengan mayor resistencia a los cambios drásticos de temperatura, así como también a altas temperaturas.

Para conjuntos de sistemas que tienen diferentes funciones, pero trabajan bajo el mismo espacio, es importante integrarlos. Por esto, una red que integra todos los sistemas, teniendo como elemento central un servidor, permite controlar y activar servicios de cada uno de los sistemas implementados, también una base de datos que almacenara por separado la información provista por cada uno de los sistemas para en caso de ser necesario se pueda consultar fácilmente. Al estar centralizada la información, se pueden realizar comparaciones con los demás sistemas para obtener un resultado más completo y objetivo, detectando rápidamente si se violó el perímetro asignado y de ser así realizar un seguimiento en tiempo real de la ruta seguida.

Se recomienda analizar exhaustivamente el área de trabajo, esto permite tomar decisiones acertadas para escoger los equipos y elementos que se integraran al sistema de seguridad final. Para este proyecto, como ejemplo, se decidió usar detectores de humo lineales con haz largo alcance, esto teniendo en cuenta que el recinto tiene un área considerable, de usar detectores de humo individuales se necesitarían muchos más comparado con los usados, esto también incrementa gastos monetarios y energéticos. Por lo que, una planificación y selección de los dispositivos como de su ubicación, incrementa la rápida detección de alarmas o indicadores de los sistemas de seguridad, disminuye el tiempo de identificación del evento y el accionar para actuar según la situación, además que aprovecha al máximo las capacidades y ventajas de los dispositivos incorporados al elegirlos para la situación específica del recinto.

6. BIBLIOGRAFÍA

- *Access_Engine*. (n.d.). Retrieved May 7, 2023, from https://commerce.boschsecurity.com/xl/es/BIS-Access-Engine-ACE-4-4/p/26808595467/
- BIS Bosch. (1886). *Bosch Building Integration System*. https://www.boschsecurity.com/xl/es/soluciones/software-de-gestion/building-integration-system/
- BVMS Bosch. (1886). *BVMS*. https://www.boschsecurity.com/es/es/soluciones/software-de-gestion/bvms/
- Compañía Internacional de Integración S.A. (n.d.). *Ci2*. Retrieved November 17, 2022, from https://ci2.co/
- *Datasheet_D296_Data_sheet*. (n.d.).
- *Engineered Solutions-AMC2: Controlador Modular de Acceso AMC2: Controlador Modular de Acceso*. (n.d.).
- *FMR_5000_C_Data_sheet*. (n.d.).
- *Intrusion Alarm Systems | DS1101i Series Detectores de roturas de cristal*. (2016). www.boschsecurity.com
- *Intrusion Alarm Systems-Software de programación remota*. (2023). www.boschsecurity.com/xc/en/contact/
- *ISC_PPR1_W16_Data_sheet*. (n.d.).
- Lantronix. (2018). *XPort Device Server User Guide*. http://patents.lantronix.com;
- Pearson, R. L. (2007). *Electronic security systems : a manager's guide to evaluating and selecting systems solutions* . Elsevier.