DISEÑO Y ESTRUCTURACIÓN DE UN SISTEMA DE CONTROL DE ACCESO INTEGRADO A LA RED LAN DE UNA EMPRESA

SERGIO ANDRÉS BONILLA CALDERON

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS FACULTAD DE INGENIERIA
PROYECTO CURRICULAR DE INGENIERIA ELECTRÓNICA
COLOMBIA, BOGOTÁ
2016

DISEÑO Y ESTRUCTURACIÓN DE UN SISTEMA DE CONTROL DE ACCESO INTEGRADO A LA RED LAN DE UNA EMPRESA

PROPONENTE:

SERGIO ANDRÉS BONILLA CALDERON

DIRECTOR:
GUSTAVO ADOLFO PUERTO LEGUIZAMON

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS FACULTAD DE INGENIERIA
PROYECTO CURRICULAR DE INGENIERIA ELECTRÓNICA
COLOMBIA, BOGOTÁ
2016

TABLA DE CONTENIDO

INTRODUCCIÓN 4

I. PROPUESTA 5

1. RESUMEN EJECUTIVO 5

1.1. PROPUESTA DE PASANTÍA 5

1.2. TITULO DE LA PASANTÍA 5

2. OBJETIVOS: 7

2.1. GENERAL 7

2.2. ESPECÍFICOS 7

3. JUSTIFICACIÓN: 8

4. ALCANCE Y LIMITACIONES 9

4.1. ALCANCE 9

4.2. LIMITACIONES 9

II. DESARROLLO DEL MANUAL TECNICO 10

5. MANUAL TÉCNICO 11

5.1. ALCANCE Y OBJETIVOS 11

5.2. NORMATIVIDAD 11

5.3. CRITERIOS DE DEFINICIÓN DE REQUERIMIENTOS 12

5.4. CRITERIOS DE SELECCIÓN DE TECNOLOGÍA Y DISEÑO 13

5.4.1. COMPARACION DE MODELOS 14

5.4.2. ÍNDICE DE PROTECCIÓN IPXX 17

5.4.3. ¿QUÉ TECNOLOGÍA USAR? 18

5.5. IMPLEMENTACION DE LOS SISTEMAS DE CONTROL DE ACCESO 19

5.6. CONFIGURACIÓN DEL SOFTWARE 21

5.7. COMENTARIOS 22

6. CASOS DE ÉXITO 23

6.1. FONDO ROTATORIO DE LA POLICÍA. 23

6.2. ITS INFOCOM 25

6.3. ALLIANCE ENTERPRISE 26

7. BIBLIOGRAFÍA 27

INTRODUCCIÓN

En un mercado laboral donde la seguridad electrónica se convirtió en una necesidad habitual en todas las compañías, entidades públicas y zonas residenciales, las empresas que presenten soluciones de este tipo encuentran un foco de ingresos fuerte, donde serán necesarios ingenieros electrónicos cada vez mejor capacitados y con la habilidad de diseñar, presupuestar y ejecutar soluciones acordes a las necesidades específicas de cada cliente. En términos generales, un sistema de control de acceso es un sistema inteligente que permite la integración de tecnologías de identificación biométrica, de tarjetas RF o de teclados matriciales, con el fin de permitir y denegar el acceso a un grupo de usuarios mediante el accionamiento o bloqueo de ingresos y salidas en cualquier tipo de edificación y bajo todas las condiciones de instalación.

I. PROPUESTA

1. RESUMEN EJECUTIVO

1.1. PROPUESTA DE PASANTÍA

El presente documento pretende definir el trabajo a desarrollar durante la pasantía por realizarse en la empresa SERVICIOS Y SOLUCIONES EDC SAS. A cargo del estudiante SERGIO ANDRES BONILLA CALDERON y bajo la dirección académica del Ingeniero GUSTAVO ADOLFO PUERTO LEGUIZAMÓN y la dirección externa del Ingeniero RUBEN DARÍO CLAROS, el cargo que desempeñará el estudiante en la empresa es el de Ingeniero de Preventa de soluciones de seguridad electrónica, desde este puesto, se podrá enfocar en el diseño, la selección de la mejor tecnología y la integración de sistemas de CCTV, detección de incendios y control de acceso, profundizando en este último con el fin de obtener un documento con el soporte correspondiente a la integración de un sistema de control de acceso que involucre biometría y se conecte a la red LAN de cualquier empresa.

1.2. TITULO DE LA PASANTÍA

"Diseño y estructuración de un sistema de control de acceso integrado a la red LAN de una empresa"

1.3. PLANTEAMIENTO DEL PROBLEMA

La seguridad electrónica representa un foco de mercado muy importante en el sector tecnológico de la economía en Colombia, la capacidad de las empresas para brindar soluciones adecuadas a las necesidades específicas de cada cliente, es un factor importante para ser competentes en este mercado. Algo decisivo en el momento de inclinarse por seleccionar un proveedor de soluciones de seguridad electrónica, en este caso, de control de acceso, es la confiabilidad que pueda dar la empresa que ofrece el servicio, la posibilidad de brindar la mejor solución, brindando el personal mejor capacitado y con los criterios más adecuados de diseño y selección de tecnología a integrar.

Esta propuesta va encaminada a elaborar y estructurar el diseño de un sistema de control de acceso con reconocimiento biométrico, que permita ser integrado y administrado a través de la red LAN de una empresa. A partir de los conocimientos adquiridos en las aulas de clases, definir criterios de selección de tecnologías y la forma adecuada de administrar las redes LAN para la integración del hardware. Generar soluciones adaptadas a las necesidades particulares de cada cliente, con la ventaja de poder brindar soporte técnico y personalizar a gusto de cada cliente las soluciones ofrecidas. Todos los procesos, tratando de optimizar el uso de energía.

2. OBJETIVOS:

2.1. GENERAL

Diseñar y estructurar un sistema de control de acceso con reconocimiento biométrico, que permita ser integrado a la red LAN de una empresa.

2.2. ESPECÍFICOS

- Estudiar y analizar las características de las tecnologías disponibles en el mercado para integrar la mejor opción a la solución requerida.

- Desarrollar una solución con la tecnología seleccionada y definir los pasos para que permita integrarse a la red LAN de una empresa.

- Diseñar y estructurar todos los procesos relacionados con el desarrollo del proyecto.

- Definir y documentar estructuras de las soluciones seleccionadas, apoyándose de manuales de instalación de las fábricas con el fin de tener apoyo para el desarrollo de futuras soluciones.

3. JUSTIFICACIÓN:

La estructuración y documentación de un proyecto de integración de un control de acceso dentro de la red LAN de una empresa, permitirá tener una base clara y soportada en el entregable de esta pasantía, que sirva como referencia para el desarrollo de futuros proyectos.

Contar con este soporte, permitirá agilizar el proceso de diseño de futuras soluciones de control de acceso, pues se tendrán claros los criterios de selección de la tecnología más adecuada para cada caso, la forma en la que se debe integrar a la red LAN y los criterios de instalación de los dispositivos.

El desarrollo del proyecto permite aplicar los conocimientos técnicos adquiridos en las áreas de control, telemática, y electrónica, para a partir de éstos, integrar de la mejor manera las soluciones tecnológicas seleccionadas.

En cuanto al impacto social, el desarrollo del proyecto y los beneficios que ofrece para futuras soluciones, tiene un impacto positivo, pues empleará inicialmente a los encargados del desarrollo del proyecto, luego a técnicos encargados de las instalaciones y demás personal requerido.

4. ALCANCE Y LIMITACIONES

4.1. ALCANCE

Durante esta pasantía se pretende modelar y estructurar una solución adecuada de un sistema de control de acceso biométrico, que permita integrarse a la red LAN de una empresa, seleccionando la tecnología apropiada bajo criterios de ingeniería. Al final de la pasantía, al terminar el desarrollo del proyecto se entregará un documento que contenga el registro de los procedimientos realizados para la selección, diseño y ejecución de la integración.

4.2. LIMITACIONES

Se pretende entregar un documento únicamente con procesos de diseño, selección de tecnología y ejecución de la integración. Sin embargo, no se entregarán equipos ni prototipos físicos, debido a los costos que esto implica.

Se soportará el trabajo realizado mediante registros fotográficos que demuestren la instalación de las tecnologías seleccionadas.

II. DESARROLLO DEL MANUAL TECNICO

5. MANUAL TÉCNICO

5.1. ALCANCE Y OBJETIVOS

El objetivo de este manual técnico es el facilitar el proceso de diseño y estructuración de la solución más adecuada de sistemas de control de acceso y definir la forma en la que se debe integrar a una red LAN. El manual no profundiza en la teoría, ni define un catálogo de productos o marcas, se presenta en cambio como una guía práctica para definir de acuerdo a las necesidades del cliente, la selección de más adecuada de equipos.

El dimensionamiento de un sistema de control de acceso requiere el conocimiento de numerosos factores relativos, por ejemplo: el tipo de identificación que se requiere (huella, clave o tarjetas RF), los equipos instalados, el número de usuarios que recurrirán al sistema, la cantidad de puertas o dispositivos que se necesitan, requerimiento de generación de reportes, etc. El manual pretende dar la mejor opción de acuerdo a la combinación de esos factores.

El manual técnico constituye un instrumento adecuado para todos aquellos que se ocupan de diseñar e implementar sistemas de control de acceso.

5.2. NORMATIVIDAD

Todos los diseños deben cumplir con la normatividad técnica:

- Norma Técnica Colombiana NTC 2050 Código Eléctrico Colombiano [1].
- RETIE Reglamento Técnico de Instalaciones Eléctricas y las normas y apartes de las normas exigidas por dicho reglamento, (según última actualización de agosto de 2013) [1].
- ANSI/TIA/EIA-568-B.1, Estándar de Cableado de Telecomunicaciones de Edificios Comerciales, Parte 1: Requerimientos Generales, Abril de 2001.
- ANSI/TIA/EIA-568-B.2, Estándar de Cableado de Telecomunicaciones de Edificios Comerciales, Parte 2 Componentes de Cableado de par trenzado balanceado, Abril de 2001.

5.3. CRITERIOS DE DEFINICIÓN DE REQUERIMIENTOS

Al momento de decidir cuál es la mejor tecnología para instalar, es importante conocer información básica con el fin de dimensionar que tipo de sistema de control de acceso requiere el cliente, para lo cual, el primer paso sería hacer el siguiente cuestionario, con el fin de dar la solución más acorde a las requerimientos.

Cuestionario inicial, requerimientos del cliente

1. ¿Qué tipo de autenticación requiere?
    - Huella
    - Tarjeta
    - Clave
2. ¿Cuántos empleados tiene la empresa?

    _____
3. ¿Cuántas puertas va a controlar?

    _____
4. ¿Requiere control de visitantes?

    _____
5. ¿Cuántos visitantes estima por día?

    _____
6. ¿Requiere electroimanes para puertas, o sistemas de bloqueo como molinetes? ¿Cuántos?

    _____
7. ¿Quiere tener reportes y registros de entrada y salida del personal?

    _____
8. ¿Requiere un software de gestión de visitantes?

    _____
9. ¿Cuenta con un centro de datos? ¿tiene puertos Ethernet libres o requiere un switch?

    _____
10. ¿Quién y cómo se administra la red LAN de su empresa? ¿Tiene algún tipo de bloqueo? ¿tiene VLANS?
11. ¿Qué categoría de cable usan para las redes de su empresa?

    _____

Esta información es importante, debido a que con ella se empieza a dimensionar el tamaño y la complejidad del proyecto, la primera pregunta ya define una línea de

dispositivos, la decisión de trabajar por huella, tarjeta o clave es del cliente, de acuerdo a gustos o experiencias anteriores. Evidentemente la biometría por huella dactilar es la más segura, pero no siempre es la más recomendada para instalar, hay otros factores importantes como el tipo de empresa, una fábrica con trabajos de manufacturación puede representar la perdida de huellas dactilares, en casos como este sería mejor utilizar tarjetas RF.

Tanto el número de empleados como el número de visitantes, implica definir la capacidad de almacenamiento de usuarios, huellas o tarjetas, en la memoria de los dispositivos.

El requerimiento de software de administración de visitantes implica la compra de licencias adicionales para esta función.

La pregunta sobre quién y cómo administran la red LAN es importante debido a que los equipos requieren ser agregados al mismo segmento de red del computador que se va a comportar como servidor.

Una vez se obtenga esta información, se puede comenzar a evaluar cuál es la mejor opción para ofrecerle al cliente.

5.4. CRITERIOS DE SELECCIÓN DE TECNOLOGÍA Y DISEÑO

Los criterios de selección de tecnología, van relacionados con los requerimientos del cliente, pues a partir de éstos, se dimensionan las capacidades de los sistemas de control de acceso.

El paso a seguir es evaluar opciones, tecnologías y marcas, con el fin de ofrecer la mejor solución. Debido a la gran cantidad de opciones o posibilidades que hay en el mercado, se tomarán tres opciones, de tres marcas reconocidas, que autentifiquen mediante huella o tarjeta a los usuarios, que permitan conectarse a la red LAN, para evaluarlas y definir característica, ventajas y desventajas de cada una.

5.4.1. COMPARACION DE MODELOS

Opción 1: Suprema INC.

Es una empresa coreana con 16 años en el mercado, especializada en biometría:

- Clasificada entre las primeras 50 principales compañías de seguridad por ASMAG en 2011, 2012, 2013 y 2014.
- Premio Detektor para el mejor producto y la mejor innovación en 2009, 2010, 2012.
- Algoritmo de desempeño superior de acuerdo con la prueba MINEX realizada por NIST.
- Clasificado en los primeros lugares en la Competencia de Verificación de Huella en 2004, 2006 y 2010.
- Certificación FBI para enrolamiento y autentificación de escáner de huella viva [2].

El dispositivo a evaluar es el BIOENTRY PLUS:

Biometric	Fingerprint	
IP Rating	N/A	
RF Option	125KHz EM	
	125KHz HID Prox	
	13.56MHz Mifare/DesFire	
	13.56MHz iClass	
Capacity	**Max. User**	5000
	Max. Datos	10000
	Max. Registros	50000
	WiFi	-
	TCP/IP	Yes
	RS-485	1ch Host or 1ch Slave
Interface		(Selectable)
	RS-232	-
	Wiegand	1ch In or 1ch Out
		(Selectable)
	Input	2 Inputs
	Relay	1 Relay
	USB	-
	SD Card Slot	1ch H+D15 or 1ch Slave

Tabla 1, ficha técnica Bioentry Plus



Figura 1. Controladora Bioentry plus

Opción 2: Soyal

Es una empresa que ha estado en el mercado desde 1993, Localizada en Taiwan, se caracteriza por tener los dispositivos más antiguos en el mercado, con certificaciones internacionales en biometría y seguridad electrónica.

El dispositivo a evaluar es el AR837 EF

Teclado y clave	yes	
Biometric	Fingerprint	
IP Rating	N/A	
RF Option	125KHz EM	
	125KHz HID Prox	
	13.56MHz Mifare/DesFire	
	13.56MHz iClass	
Capacity	**Max. User**	9000
	Max. Datos	9000
	Max. Registros	32000
	WiFi	-
	TCP/IP	Yes
Interface	**RS-485**	1ch Host or 1ch Slave
		(Selectable)
	RS-232	-
	Wiegand	1ch In or 1ch Out
		(Selectable)
	Display	yes
	Relay	1 Relay
	USB	-
	Antipassback	yes

Tabla 2, ficha técnica AR 837EF



Figura 2. Controladora AR 837EF

Opción 3: ZKTeco

Empresa fundada en 1985, tiene su sede principal en China, actualmente se encuentra en más de 200 países, liderando con soluciones económicas e innovadoras, el mercado de los sistemas de control de acceso y la biometría, crearon un algoritmo propio de identificación biométrica, el cual han mejorado con el paso de los años.

El dispositivo a evaluar es ZK F16

Biometric	Fingerprint	
IP Rating	65	
RF Option	125KHz EM	
Capacity	**Max. User**	3000
	Max. Datos	3000
	Max. Registros	100000
	WiFi	-
	TCP/IP	Yes
	RS-485	1ch Host or 1ch Slave
Interface		
	RS-232	Yes
	Wiegand	1ch In or 1ch Out
		(Selectable)
	Display	yes
	Relay	1 Relay
	USB	-
	Antipassback	yes

Tabla 3, ficha técnica ZKTeco F16



Figura 3. Controladora ZKTeco F16

Las anteriores son tres opciones vigentes en el mercado actual, con las cuales se han tenido casos de éxito en instalaciones durante el último semestre, sin embargo hay factores que diferencian y facilitan la selección de los dispositivos, uno de ellos es el software, de esta manera, mientras que para ZKteco y Soyal las licencias de software para estos dispositivos son gratuitos y sin limitaciones, en Suprema, la versión gratuita limita el número de dispositivos que se pueden controlar a 22. La interfaz del software es más intuitiva y amigable para el cliente final en ZKteco, la de Suprema es aceptable pero la de Soyal es obsoleta e incómoda para el trabajo

del cliente final, todas generan reportes y manejan base de datos de los clientes en SQL.

5.4.2. ÍNDICE DE PROTECCIÓN IPXX

Otro factor importante para decidir la selección de los dispositivos es la protección que tienen contra los factores ambientales como agua, polvo o humedad, esta se mide mediante el índice de protección [3], el cual es un número de dos dígitos, donde el primer digito representa la protección contra el ingreso de objetos solidos como el polvo y el segundo representa el índice de protección contra el ingreso de objetos líquidos como el agua. En el caso de las biométricas evaluadas, observamos que la única que garantiza índice de protección es la ZKTeco F16, indicando que éste dispositivo es IP65, lo que significa que bajo ningún motivo le puede ingresar polvo u otro objeto sólido y que soporte chorros de agua directos sin afectar su funcionamiento. La tabla 4 muestra el significado de cada número de los índices de protección.

Cuerpos sólidos		Agua	
0	No está protegido contra el ingreso de cuerpos extraños.	0	Sin protección.
1	Protegido contra el ingreso de cuerpos extraños de hasta 1 mm de diámetro.	1	Protección contra el goteo de agua condensada.
2	Protegido contra el ingreso de cuerpos extraños de hasta 1 mm de diámetro.	2	Protección contra el goteo hasta 15º de la vertical.
3	Protegido contra el ingreso de cuerpos extraños de hasta 1 mm de diámetro.	3	Protección contra lluvia con un ángulo inferior a 60º.
4	Protegido contra el ingreso de cuerpos extraños de hasta 1 mm de diámetro.	4	Protección contra salpicaduras en cualquier dirección.
5	Protección contra depósito de polvo.	5	Protección contra chorreo de agua en cualquier dirección.
6	Protección contra el ingreso de polvo.	6	Protección contra ambientes propios de las cubiertas de los barcos
		7	Protección contra inmersión temporal.
		8	Protección contra inmersión indefinida.

Tabla 4, índices de protección

5.4.3. ¿QUÉ TECNOLOGÍA USAR?

En este caso, al analizar las tres opciones, todas son buenas alternativas, sin embargo, si la cantidad de huellas por registrar es mayor a 3000, se descarta esta referencia de controladora ZKTeco, de ser mayor a 5000, se descarta la controladora Suprema, en el caso de ser mayor a 9000, ZKteco tiene otra línea de productos de alto rendimiento que puede cubrir estos requerimientos.

Si las biométricas estarán sometidas a condiciones de agua o polvo, por el índice de protección es recomendable la ZKTeco F16.

Si la integración debe llevar más de 22 dispositivos, por costos de licenciamiento de software, es recomendable eliminar la controladora como opción.

Estos son algunos ejemplos de criterios de selección de tecnología, sin embargo no son los únicos, dependiendo del gusto del cliente, del presupuesto, de la integración con otro tipo de tecnologías como CCTV o alarmas, se pueden expandir las opciones o reducir las posibilidades que cubran los requerimientos puntuales de cada cliente.

5.5. IMPLEMENTACION DE LOS SISTEMAS DE CONTROL DE ACCESO

Una vez definidas las referencias de los equipos a instalar y el diseño, se procede a la implementación de la solución. La figura 4 ilustra una opción de sistema de control de acceso, con el fin de definir y aclarar conexiones y funcionamiento de los componentes del sistema, a continuación se explicara éste caso específico.



Figura 4, estructura de sistema de control de acceso

- La estructuración de un sistema de control de acceso se centra en el dispositivo biométrico, que en este caso, a su vez funciona como controlador, es decir, tiene un relé interno que activa o desactiva el electroimán, para permitir la apertura de la puerta.

- El botón de salida, en este caso un no touch, se conecta directamente a la biométrica. En los datasheet definen los pines de conexión como NO (normalmente abierto), NC (normalmente cerrado) y COM (común), se conecta el NO o el NC dependiendo del funcionamiento del botón y de la configuración que se haga desde el software a la biométrica.

- La alimentación de la controladora se hace con una fuente de 12 Voltios a 3 amperios, desde la controladora se energiza el electroimán, sin embargo

existe un botón de emergencia que funciona normalmente cerrado para que en un caso extremo, se presione y pase a normalmente abierto, cortando la energía del electroimán y liberando la puerta.

- Cada dispositivo controla una puerta, el botón de salida puede ser reemplazado por un dispositivo biométrico esclavo, que se conectaría por RS 485 a la controladora, su única función seria leer los datos de huellas o tarjetas, pero no habilita directamente el electroimán, eso solo es posible a través de la controladora.

- La controladora tiene un puerto TCP/IP, al cual llega un cable UTP categoría 5e o mayor, que lo conecta con un switch en el centro de datos y lo enlaza a la red LAN.

- El computador se encuentra en la misma red LAN, es importante que se encuentre en el mismo segmento de Red de las controladoras, y de ser utilizadas, en la misma VLAN, sin ningún tipo de restricción o firewall.

- El computador debe tener unas características mínimas de recursos físicos, para el correcto funcionamiento del software.

- El enrolador de huellas se conecta vía USB al computador en el cual se va a administrar el software y se van a registrar los usuarios.

- El brazo hidráulico solo es un equipo mecánico de cierra, no implica ningún cableado ni conexión eléctrica.

- Cuando se requiere uno o más molinetes, el principio es el mismo, la diferencia está en que el relé de las biométricas no va a activar el electroimán, sino el paso en un sentido del molinete.

- Los cableados deben cumplir las normas de las instalaciones eléctricas RETIE.

- El cable UTP se poncha de acuerdo a la norma TIA/EIA 568

5.6. CONFIGURACIÓN DEL SOFTWARE

Una vez terminada la instalación física de los equipos, la asignación de direcciones IP, el cableado, se procede a la instalación del software y al enlace con los dispositivos. Para esto se recomienda seguir los siguientes pasos.

a. Desde el computador ejecutar el instalador del software como administrador.
b. Seguir los pasos de instalación, crear el directorio de instalación, de backup y de la base de datos.
c. Una vez terminada la instalación hacer ping a cada una de las controladoras para comprobar la conexión.
d. Agregar las controladoras al software.
e. Asignar a cada controladora una puerta dentro del software.
f. Definir distribución de puertas
g. Definir departamentos, grupos de usuarios, horarios y demás requerimientos acordes a las necesidades del cliente.
h. Hacer el enrolamiento y registro de usuarios dentro del software, con tarjetas o huellas.
i. Sincronizar los datos de usuarios entre el computador y las controladoras.
j. Definir niveles de acceso para cada usuario, es decir definir a que puertas se le permite acceder.
k. Probar el monitoreo en tiempo real
l. Generar reportes.



Figura 5, ejemplo de software de control de acceso ZKAccess 3.5

Nota: El éxito del proceso de configuración del software, radica en la capacidad de explicarlo el cliente, con el fin de que éste conozco todas las funciones y quede satisfecho con la administración del proceso.

5.7. COMENTARIOS

La información entregada en este manual no es absoluta, son casos específicos tomados como ejemplo para retroalimentar el proceso de aprendizaje durante la pasantía.

Los dispositivos tomados como ejemplo, fueron instalados en diferentes proyectos durante el transcurso de la pasantía y hoy son considerados casos de éxito.

La biometría y los sistemas de control de acceso son escalables, es decir, se puede aplicar a macroproyectos, de más de 20000 usuarios, con software especializado de control de visitantes, con la posibilidad de integrar otros sistemas como los circuitos cerrados de televisión, las alarmas, el acceso a ascensores, de modo que se pueden administrar todos desde el mismo software. ZKTeco tiene un ejemplo con su nueva línea de producto, de la serie Green Label [4].

La integración a la red local de las empresa también se puede hacer de manera inalámbrica, vía WIFI, solo cambiaría la referencia de las controladoras, lo cual incrementaría costos.

6. CASOS DE ÉXITO

6.1. FONDO ROTATORIO DE LA POLICÍA.

Diseño, suministro, e instalación de sistema de control de acceso, para 14 torniquetes (dos controladoras por cada uno) y 10 puertas, en las dos sedes de FORPO en Bogotá.

Dispositivos biométricos marca Suprema.



Figura 6, Instalación de torniquetes con controladoras Suprema Bioentry Plus



Figura 7, Instalación de torniquetes con controladoras Suprema Bioentry Plus

6.2. ITS INFOCOM

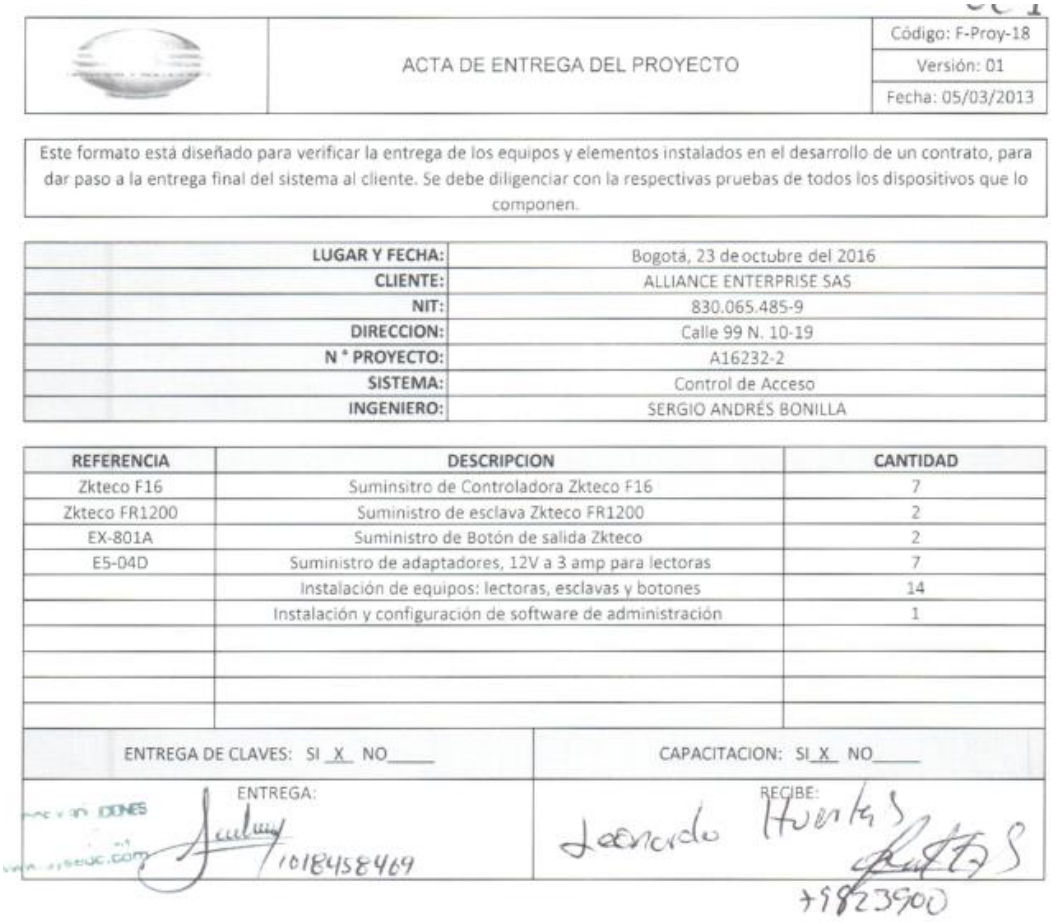
Diseño, suministro e instalación de sistema de control de acceso, para 3 puertas y circuito cerrado de televisión con cámaras IP.



Figura 8, Instalación de control de acceso con dispositivos Soyal

6.3. ALLIANCE ENTERPRISE

Diseño, suminsitro e instalación de sistema de control de acceso, con dispositivos marca ZKTeco.



	ACTA DE ENTREGA DEL PROYECTO	Código: F-Proy-18 Versión: 01 Fecha: 05/03/2013

Este formato está diseñado para verificar la entrega de los equipos y elementos instalados en el desarrollo de un contrato, para dar paso a la entrega final del sistema al cliente. Se debe diligenciar con la respectivas pruebas de todos los dispositivos que lo componen.

LUGAR Y FECHA:	Bogotá, 23 de octubre del 2016
CLIENTE:	ALLIANCE ENTERPRISE SAS
NIT:	830.065.485-9
DIRECCION:	Calle 99 N. 10-19
N ° PROYECTO:	A16232-2
SISTEMA:	Control de Acceso
INGENIERO:	SERGIO ANDRÉS BONILLA

REFERENCIA	DESCRIPCION	CANTIDAD
Zkteco F16	Suminsitro de Controladora Zkteco F16	7
Zkteco FR1200	Suministro de esclava Zkteco FR1200	2
EX-801A	Suministro de Botón de salida Zkteco	2
E5-04D	Suministro de adaptadores, 12V a 3 amp para lectoras	7
	Instalación de equipos: lectoras, esclavas y botones	14
	Instalación y configuración de software de administración	1

ENTREGA DE CLAVES: SI X NO____ CAPACITACION: SI X NO____

ENTREGA: 1018458469 RECIBE: Leonardo Huertas 7823900

Figura 9, Acta de entrega de proyecto, sistema de control de acceso marca ZKTeco con biométricas F16 y esclavas FR1200

7. BIBLIOGRAFÍA

[1] Ministerio de minas y energía. “Reglamento técnico de instalaciones eléctricas”. Agosto de 2013. Extraído de: http://www.ccenergia.org.co/upload/default/products/6894392baeb62fb2a6af7e72c41dcc42.pdf

[2] Suprema INC. Información acerca de suprema. Extraído de: https://www.supremainc.com/es/node/102

[3] ANSI/IEC 60529-2004, “Degrees of Protection Provided by Enclosures”. Noviembre de 2004, Extraído de: https://www.nema.org/Standards/ComplimentaryDocuments/ANSI-IEC-60529.pdf

[4]Zkteco Latinoamérica. “¿Qué es Green label?”. Septiembre del 2016. Extraído de: http://www.zktecolatinoamerica.com/productos