UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS INDUSTRIALES

Implementación de control de acceso

MEMORIA DE EXPERIENCIA PROFESIONAL

PARA OBTENER EL TÍTULO DE

LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS INDUSTRIALES

PRESENTA:

SILVESTRE HERNÁNDEZ HERNÁNDEZ

DICTAMINADORES

M. EN C. GENOVEVA RAMÍREZ CASTILLO

DR. CARLOS JIMÉNEZ GALLEGOS

Ciudad de México, marzo de 2021.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

Coordinación de Certificación y Registro

Coordinación de Certificación y Registro

F6 AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, a 25 de febrero de 2021

SILVESTRE HERNÁNDEZ HERNÁNDEZ
Estudiante de la Licenciatura en Ingeniería en Sistemas Electrónicos Industriales
P r e s e n t e

En virtud, de que cuentan con los cuatro votos aprobatorios necesarios para presentar la defensa de su tesis/trabajo recepcional titulado/a **Implementación de control de acceso,** esta Coordinación le autoriza la impresión de su trabajo final.

Por lo que deberá reproducir 6 ejemplares, los cuales **entregará 8 días hábiles antes del examen** uno para cada miembro del jurado y **a esta Coordinación 3 ejemplares, así como 2 discos compactos** con la ***versión electrónica en formato PDF**.

No omito recordarle que no hay prórroga en la entrega de materiales, ya que de ello depende la reconfirmación de fecha de examen.

Sin otro particular, reciba un cordial saludo.

A t e n t a m e n t e

COORDINACIÓN DE CERTIFICACIÓN Y REGISTRO

*Para la Titulación "A distancia" enviar por correo electrónico la versión final de la tesis/trabajo recepcional en versión PDF (tal como aparecerá en el formato impreso que será entregado posteriormente).
El nombre del archivo será: **Nombre del Estudiante_Siglas licenciatura/posgrado**

AGRADECIMIENTOS

Quiero dedicar este trabajo a mis padres;

María Lina Hernández Hernández y Julio Hernández Hernández, por su apoyo incondicional y paciencia, aunque ya no están conmigo físicamente, sé que desde el cielo me cuidan y me guían para que todo marche de la mejor manera.

Gracias a dios por bridarme salud, bienestar y fortaleza para cumplir a todas mis metas trazadas.

Agradezco a mis hermanos por brindarme su apoyo para alcanzar mis objetivos.

Agradezco al Dr. Carlos Jiménez Gallegos y a la Mtra. Genoveva Ramírez Castillo, por aceptar trabajar en conjunto para el desarrollo de este trabajo, por su poyo, confianza, disponibilidad y paciencia, por su importe participación y aporte para el desarrollo de este trabajo por memoria de experiencia profesional.

Gracias a la Universidad Autónoma de la Ciudad de México, mi casa de estudios, en donde pude desempeñarme académicamente, adquirir y poner en práctica múltiples conocimientos, que en la actualidad me son de gran utilidad para mi desempeño en el ámbito laboral

MUCHAS GRACIAS.

SILVESTRE HERNÁNDEZ HERNÁNDEZ

íNDICE

ÍNDICE DE TABLAS Y FIGURAS

ORGANIZACIÓN DEL INFORME

La elaboración de este reporte es de gran importancia debido a que me ha permitido identificar y dar a conocer como he podido llevar a la práctica las habilidades y conocimiento obtenidos a lo largo de mi carrera en una empresa de carácter privado dedicada a brindar servicios de implementación de controles de acceso, de esta manera este trabajo está divido en tres capítulos:

En el Capítulo 1 denominado “Antecedentes”, se describen a grandes rasgos la historia de la empresa IBIX S.A. de C.V. incluyendo sus orígenes, su conformación y las principales actividades que realiza, así como los principales equipos que comercializa, una vez teniendo un panorama general sobre quién es, como está conformada y como funciona IBIX S.A. de C.V.

En el Capítulo 2 denominado “Implementación de controles de acceso”, se presentan sobre los tres tipos de controles de acceso, así como su funcionamiento y su instalación, como parte de las principales actividades que realiza dicha empresa.

Finalmente, en el Capítulo 3 denominado “Conocimientos puestos en marcha en la empresa IBIX S.A. de C.V.”, se presentan sobre los conocimientos obtenidos a lo largo de la carrera Ingeniería en Sistemas Electrónicos Industriales y de cómo los he llevado a la práctica en cada una de las actividades que se realiza en IBIX S.A. de C.V., y como me han sido de gran ayuda para insertarme en el ámbito laboral.

MEMORIA DE EXPERIENCIA PROFESIONAL

INTRODUCCIÓN

En la actualidad los sistemas biométricos han adquirido una importancia significativa en el ámbito laboral, debido a que se han hecho presentes en un gran número de empresas tanto públicas como privadas, con la principal finalidad de tener un mejor control de asistencia de su personal, **IBIX S.A. de C.V.,** se constituye como una empresa encargada de brindar servicio profesional para implementación de controles de acceso, acoplándose a cada una de las necesidades de los usuarios.

Las principales actividades que se llevan a cabo en la empresa **IBIX S.A. de C.V.** consiste en el contacto con el prospecto ofreciendo la mejor opción para sus requerimientos, tales como; el equipo adecuado acorde sus actividades, el software de acuerdo con el número de trabajadores y una póliza de servicio, para brindar instalación, capacitación y soporte en sitio o de forma remota.

Con mi experiencia laboral en el transcurso de estos últimos tres años (2016-2019), he podido llevar a la práctica los conocimientos adquiridos a lo largo de mi formación profesional, algunos como; realizar instalaciones eléctricas y cálculo de corriente de los conductores eléctricos aprendidos en el curso *"seguridad e instalaciones eléctricas industriales"*, comprender el mecanismo de funcionamiento de los electroimanes, conocimiento adquirido en el curso de *"electrotecnia I"*, las materias *"dispositivos electrónicos I y dispositivos electrónicos II*" me proporcionaron las herramientas para identificar el voltaje de corriente alterna y voltaje de corriente directa de una fuente de alimentación, también otros conocimientos que he puesto en práctica son los que obtuve en las materias *de "microprocesadores y periféricos", "aplicaciones de microprocesadores y microcontroladores " y "electrónica aplicada*" enfocados en la configuración de la tarjeta principal de los equipos comercializados de la empresa **IBIX S.A. de C.V.**, estos son solo algunos ejemplos de los conocimientos que he puesto en práctica sin embargo, en el Capítulo 3 se escribe a mayor detalle de ello.

METODOLOGÍA

Para la realización de este reporte, se utilizó una metodología basada en una revisión documental y sistemática de documentos que incluyen; manuales de instalación, manuales de configuración, manuales de funcionamiento, de manera complementaria se realizó una revisión bibliográfica que aportó conceptos importantes que contribuyeron al marco referencial de este reporte.

Este reporte se sustenta en mi experiencia laboral llevada a cabo en la empresa **IBIX S.A. de C.V**., en la que se realizan actividades de implementación de sistemas de control de acceso, que se dividen básicamente en tres etapas, como se puede observar en la figura 1, en una primera etapa, se efectúa un levantamiento sobre las condiciones del lugar donde se instalará el dispositivo, para garantizar una buena instalación, se deben tomar en cuenta las condiciones de la instalación eléctrica especificando que debe de ser regulada y aterrizada, así también la preparación de la instalación de los nodos de red, otro punto importante que se considera es tipo de material de la superficie y las dimensiones donde se colocará el equipo.

En la segunda etapa, una vez teniendo las condiciones óptimas del lugar, se consensa una cita para realizar la instalación del equipo requerido por el cliente, de esta manera se coloca el dispositivo físico, así como también la instalación del software para realizar la interfaz con el dispositivo, además se elabora una estructura de base de datos para posteriormente hacer una carga masiva de datos de los usuarios en el sistema y así poder enviarlos al dispositivo para tener un control de acceso de los trabajadores.

En la tercera etapa, finalmente comprobando que el dispositivo funciona correctamente, se realiza una capacitación con el personal encargado del área de sistemas y de mantenimiento, cuyo principal objetivo es explicar las acciones que deben llevar a cabo para contrarrestar algunas incidencias que el equipo podría presentar (falla de red, bloqueo, falla eléctrica), así también se capacita él personal de recursos humanos abordando temas como; registro del personal, registro de la huellas digitales, rostro o tarjeta de proximidad en el software, generación de turnos

y rotaciones, asignación de áreas y departamentos, registro de conceptos de ausentismo, permisos, días festivos y tipos de reportes que se pueden generar.

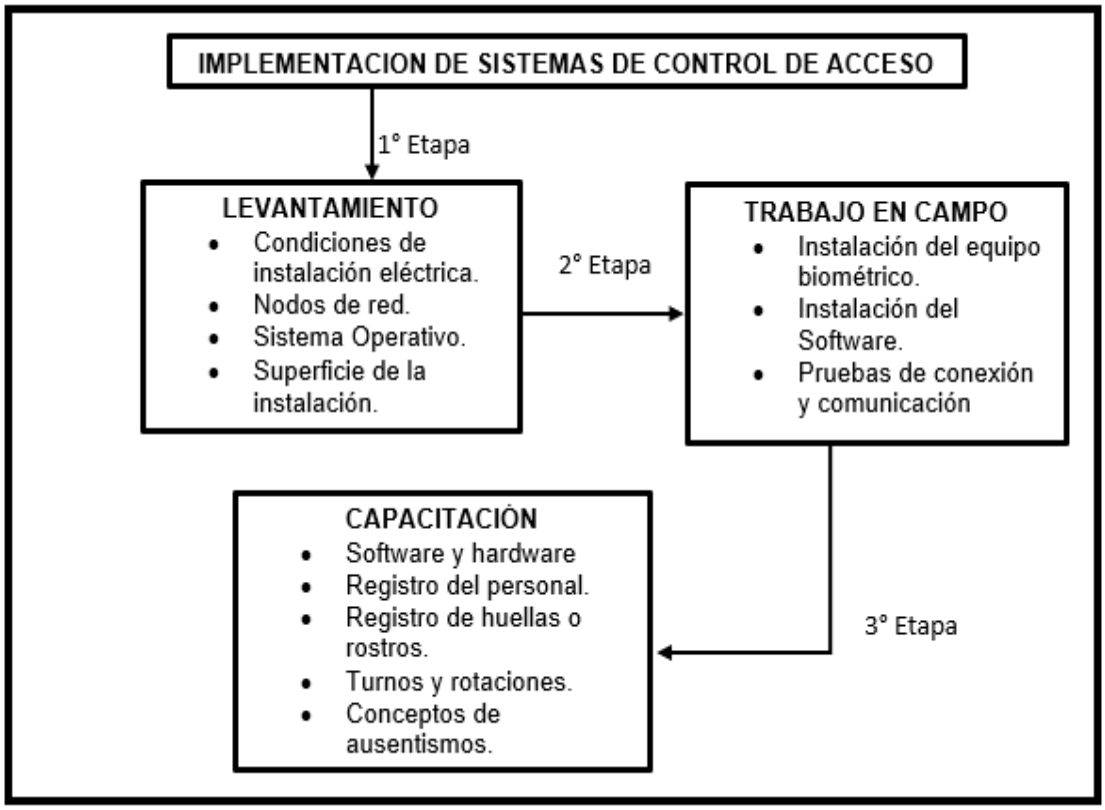


Figura 1. Implementación de sistemas de control de acceso

La elaboración de este reporte se basa en una metodología documental, de carácter sistemática y descriptiva, ya que además de describir las actividades que desempeño en mi ámbito laboral, también se contrastan con los conocimientos adquiridos a lo largo de mi formación profesional, llevados a la práctica con la implementación de los sistemas de control de acceso.

CAPÍTULO 1. ANTECEDENTES

1.1. Historia de la empresa IBIX S.A de C.V

IBIX S.A. de C.V., es una empresa que se fundó el 25 de mayo del año 2000 en Monterrey Nuevo León por profesionistas de sistemas, enfocados específicamente a desarrollar e integrar equipos para captura y validación de datos como; relojes checadores electrónicos, que son utilizados para sistemas de control de asistencia, control de acceso, control de consumos de comedor y control en líneas de producción.

Con el paso de los años, **IBIX S.A. de C.V.**, se ha consolidado como un equipo interdisciplinario en Ingeniería Electrónica e Ingeniería de Sistemas para brindar las soluciones más flexibles y completas, integrando las más variadas e importantes tecnologías emergentes en nuestro campo de acción **[IBIX S.A. de C.V., 2013]** y así responder a las demandas que en la actualidad solicitan las diferentes empresas tanto del ámbito público como privado.

De esta manera IBIX inició sus actividades como una empresa que brindaba servicios específicamente de tecnologías de la información, sin embargo, para el año 2002, respondiendo a las nuevas demandas del mercado se inició con el diseño y desarrollo de hardware y software propio con la fabricación de relojes checadores digitales y el desarrollo del sistema IBIX de control de asistencia y acceso, siendo un plus para la empresa.

Durante el año 2005, IBIX introdujo al mercado los lectores de huella digital de uso rudo, siendo pioneros de este proceso con el desarrollo e implementación del Reloj checador **uControl 6000 Biométrico** (figura 2).

Figura 2. Checador uControl 6000 Biométrico.

El año 2008, fue sin duda un año crucial para la empresa ya que se firmaron alianzas con la Aceleradora de Negocios de la Escuela de Graduados en Administración y Dirección de Empresas, (EGADE) del Tecnológico de Monterrey, para el Desarrollo de Negocios de Base Tecnológica y Evolución a Empresa Gacela, **[IBIX, S.A. de C.V., 2013]** además de que se llevaron a cabo los procesos de certificación bajo la Norma **MOPROSOFT**: Tecnologías de Información, Modelos de Procesos para Desarrollo y Mantenimiento de Software, lo que garantiza la mejor calidad del software desarrollado por IBIX, además de que contribuyó a garantizar la oferta de los servicios de calidad y competitividad a niveles internacionales [Oktaba, 2003]. Dos años más tarde en el 2010 se firmó un acuerdo con el SAP, la compañía mundial número uno en software de negocios, para la promoción e implementación de “SAP Business One” bajo el programa “SAP Member - Extended Business Program”.

Para el año 2010, **IBIX, S.A. de C.V.**, ya contaba con una estructura sólida implementando y poniendo en marcha su propia solución, con alianzas y certificaciones que garantizarían su óptimo funcionamiento frente a las demandas de los usuarios, por lo que se inició una apertura de nuevos mercados con la inauguración de la oficina de ventas en Cintermex, Centro Internacional de Negocios

Monterrey durante este mismo año, posteriormente en el 2010 se inauguró la oficina de ventas y soporte Saltillo Coahuila, después en el año de 2011 se inauguró la oficina de ventas y soporte técnico en World Trade Center de la Ciudad de México, años más tarde en el 2018 se inauguró la oficina de ventas y soporte en león Guanajuato.

Además de la certificación de **MOPROSOFT**, en junio del 2011 se llevó a cabo una verificación realizada por el **NYCE**, **Normalización y Certificación Electrónica, A.C.,** con la cual se alcanzó satisfactoriamente el nivel de madurez dos del modelo MOPROSOFT, aplicando la norma NMX-I-059-NYCE-2005 Tecnología de la Información-Software-Modelos de Procesos y Evaluación para desarrollo y Mantenimiento de Software-Parte 02: Requisitos de Procesos (**MOPROSOFT**). Para noviembre de 2013, fue otorgado el certificado de conformidad con la Norma Oficial Mexicana (NOM) para el reloj checador uControl de IBIX.

Las principales actividades que se desempeñan en IBIX, se rigen bajo un aviso de privacidad con el cual se estipula que **IBIX, S.A. de C.V.** con domicilio en la calle León XIII número 1112, colonia Villa de San Antonio, Guadalupe, Nuevo León México, es responsable de recabar los datos personales, del uso que se le dé a los mismos y de su protección.

En la actualidad **IBIX, S.A. de C.V.**, cuenta con un equipo estable, encargado de la distribución de sistemas biométricos, además de las diferentes áreas que en conjunto se articulan para llevar a la empresa a un estado de funcionamiento acorde a las necesidades del mercado, contando con más de 800 clientes en México debido a su alto grado de compromiso y recomendación de los usuarios, de esta manera, se trabaja para brindar las soluciones más avanzadas y mantener un liderazgo basado en el trabajo de investigación y desarrollo de las diversas soluciones a nivel mundial, tal y como se estipula en la misión y visión de dicha empresa.

Misión

Proveer las más avanzadas soluciones tecnológicas en software y hardware para aplicaciones de control de personal que contribuyan a la productividad y calidad de desempeño de nuestros clientes, así como brindar una plataforma de superación a nuestros colaboradores y accionistas **[IBIX, S.A. de C.V., 2013]**

Visión

Mantener una posición de liderazgo basado en la investigación y desarrollo de soluciones de clase mundial, sirviendo satisfactoriamente a la dinámica de nuestros clientes, expandiéndonos consistentemente a nuevos horizontes geográficos y de retos en el ámbito de las Tecnologías de Información **[IBIX, S.A. de C.V., 2013].**

Una vez teniendo un panorama general sobre la historia de **IBIX, S.A. de C.V.**, en el siguiente apartado se hablará a grandes rasgos sobre las actividades que realiza la empresa, desde el área administrativa, soporte técnico y área de ventas.

1.2. Actividades que desempeña la empresa IBIX S.A de C.V.

Una vez conociendo las generalidades del origen de la empresa **IBIX S.A. de C.V.,** es importante hablar sobre las actividades que se realizan en el interior de dicha empresa, a continuación, se presentan dos figuras en el que se resumen las principales áreas de acción para brindar un servicio de calidad que responda a las necesidades de cada cliente, así como las sucursales que tiene;

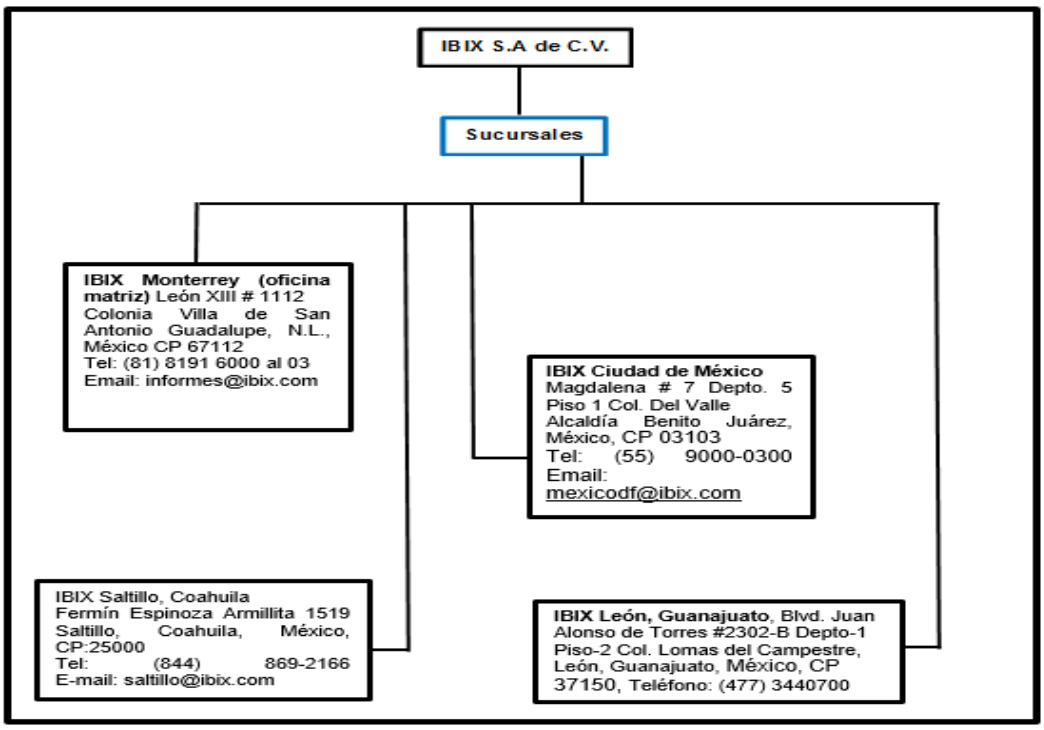


Figura 3. Sucursales de la empresa IBIX, S.A de C.V.

Tal y como se puede ver en la figura 3 anterior, **IBIX, S.A. de C.V.**, es una empresa que cuenta con cuatro sucursales que bridan servicios de atención a clientes en forma remota y presencial, estas son; Monterrey N. L, que es la oficina matriz, Ciudad de México, León Guanajuato y Saltillo Coahuila, además de que articula diferentes áreas para su funcionamiento tales como (figura 4);

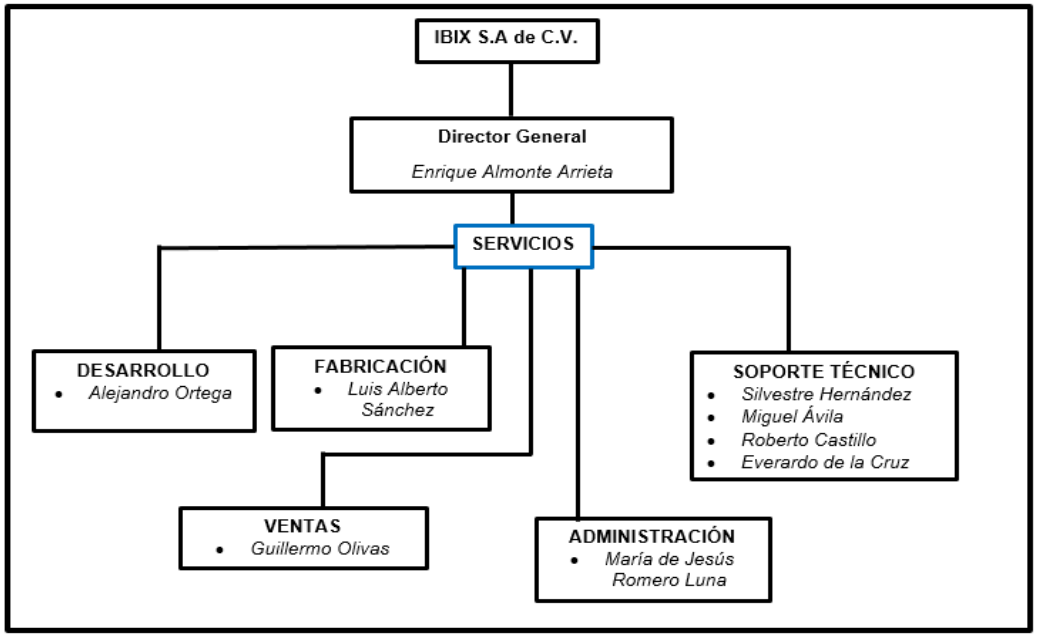


Figura 4. Estructura de la empresa IBIX S.A de C.V.

ÁREA DE DESARROLLO: El área de desarrollo se encuentran ubicada en la oficina matriz, las principales actividades que ahí se realizan son; la implementación y mejoras al sistema **IBIX**, que se define como el software en la cual se lleva un control del registro de los trabajadores de cada uno de los clientes, lo que garantiza el correcto funcionamiento tanto del hardware, otras de las funciones de esta área se enfocan a realizar las interfaces con las diferentes nominas que hay en el mercado **(Aspel Noi, Nomipad, Sap, Apsi** entre otros) además de llevar a cabo interfaces con los nuevos equipos biométricos que salen al mercado.

Aspel Noi: es un sistema de nómina que calcula las percepciones y deducciones de los trabajadores, también genera comprobantes fiscales por internet de los recibos de nómina de cada empresa, con el software **IBIX** maneja una interface por medio de un archivo plano de Excel, la cual se exporta la información de todos los datos de los trabajadores al sistema Aspel Noi como (número del trabajador, nombre completo del trabajador, horas laboradas a la semana o la quincena, tiempos extras, retardos, faltas, vacaciones), esta información son extraídos de los equipos biométricos **[IBIX, S.A. de C.V., 2013]**.

Nomipad: es un sistema para administración y cálculo de las nóminas de los trabajadores, también generan comprobantes fiscales por internet, con el software **IBIX** maneja una interface de acuerdo del diseño proporcionado por parte del proveedor de nómina en donde se exporta un archivo plano de texto continuo con información (código del empleado, número de concepto de ausentismo, tiempos extras dobles, triples, retardos, faltas, horas laborados en días festivos) **[IBIX, S.A. de C.V., 2013]**.

Sap: es un sistema de nómina y ERP (Planificación de recursos empresariales) la cual puede administrar la nómina de los trabajadores y también administrar la producción, logística e inventarios de una empresa, con el software **IBIX** cuenta con una interface donde se genera un archivo de texto con campos separados por tabuladores de cada trabajador la cual exporta los siguientes datos (Fecha de los

marcajes, número del trabajador, clave de área ,clave de departamento, clave del turno, clave de horas laboradas) **[IBIX, S.A. de C.V., 2013]**.

Apsi: sistema de nómina vía web y aplicación móvil para administrar las nóminas de los trabajadores de cada uno de las empresas privadas, con el software **IBIX** cuenta con una interface de forma directa con su base de datos en SQL (lenguaje de consulta estructurada), software **IBIX** se encarga de migrar las checadas de todos los trabajadores recolectados de los equipos biométricos como: las entradas de turnos, salidas/entradas de comidas, retardos de comida y salidas de turnos al sistema **Apsi,** la cual se encarga de calcular las horas laboradas, tiempo extra, vacaciones, conceptos de ausentismos para realizar el pago de nómina de cada trabajador **[IBIX, S.A. de C.V., 2013].**

ÁREA DE FABRICACIÓN: Otra de las áreas es la de fabricación, en la cual se lleva a cabo el ensamblado de gabinete himel, semáforo, cámara y display, así como la fabricación de la tarjeta control y fuente de voltaje, del equipo **IBIX-UCONTROL**, lo que asegura sacar al mercado un equipo de calidad para uso industrial.

ÁREA DE SOPORTE TÉCNICO: El área de soporte técnico, se ha implementado en cada una de las sucursales con el objetivo de obtener el máximo rendimiento del software y sus componentes de hardware además de prevenir riesgos, minimizar problemas por fallas técnicas, optimizar el uso y aprovechamiento del sistema. También se cuenta el apoyo de un ingeniero de soporte cuando se requiere, quien se encarga de realizar la instalación de los equipos para control de acceso, puesta en marcha la base de datos, capacitación de sistema **IBIX**, de los dispositivos de acceso y mantenimiento preventivo y correctivo de los equipos.

Todos estos servicios se hacen a través de una póliza de servicios que se adquiere en el momento que se realiza la comprar de un equipo, sí así lo requiere el cliente, la póliza de servicio incluye:

- Servicio de instalación, capacitación, soporte y asesoría para la operación de los relojes checadores, unidades de control de acceso y software IBIX incluyendo

interface de exportación de prenómina, el módulo de diseño e impresión de credenciales, y en general todos los componentes del sistema IBIX.

- Asesoría remota vía internet, correo electrónico y telefónica.
- Asesoría personalizada en sitio o en nuestras instalaciones.
- Actualizaciones realizadas al sistema **IBIX** incluyendo revisiones y nuevas versiones.
- Servicio de mantenimiento preventivo y correctivo a los relojes checadores y unidades control de acceso componentes del Sistema IBIX, incluyendo mano de obra.
- Refacciones incluidas en equipos **IBIX-UControl** cuando éstas sean requeridas por desgaste bajo condiciones de uso normal excluyendo daños por siniestro o vandalismo, excluyendo también refacciones para dispositivos externos conectados a dichos equipos.
- Dicha póliza tiene una vigencia de un año en los horarios de atención correspondientes (lunes a viernes de 8:30 a 18:30), programando las actividades con anticipación ya sea en sitio o vía remota.

ÁREA DE VENTAS: En esta área se realiza la labor de venta de los productos que comercializa la empresa **IBIX**, iniciando con el contacto con clientes nacionales e internacionales para ofertar dicho productos, una vez que se tiene el contacto se realizan demostraciones del funcionamiento de los equipo y del software, ofreciendo la mejor opción para sus necesidades, a través de una cotización en la que se especifican, los costos, tiempos de entrega, la cantidad y características de los equipos, de esta manera se da paso a la adquisición de los biométricos, complementando con la instalación y la capacitación a cargo del ingeniero de soporte.

ÁREA DE ADMINISTRACIÓN: Esta área es la encargada de llevar un control sobre las facturas correspondientes a los equipos vendidos, además también son los encargados de hacer el envío de los equipos a diferentes puntos donde se encuentre el cliente, dentro de sus principales funciones también se encuentra la consulta de precios de las refacciones y equipos directo con los fabricantes, así

como la asignación de viáticos en el caso de requerirse para la instalación en campo de los equipos.

En general el funcionamiento de la empresa **IBIX, S.A. de C.V.**, gira en torno a un trabajo articulado en equipo en el que se destaca atención primordial al cliente, buscando siempre la forma de asegurar un servicio de calidad que contribuya al mejoramiento de las empresas y que contribuya al mejor control de las actividades que se desempeñan en cada una de ellas.

1.3. Equipos que comercializa la empresa IBIX, S.A. de C.V.

Antes de hablar sobre los equipos que comercializa la empresa **IBIX, S.A. de C.V.**, es importante mencionar que un sistema biométrico consta de componentes tanto hardware como software necesario para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada.

En general un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad, el funcionamiento de estos sistemas implica la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje.

Con el paso del tiempo se han descrito los principales sistemas biométricos existentes, tales como; reconocimiento de la huella dactilar, reconocimiento de la cara, reconocimiento de iris/retina, geometría de dedos/mano, autentificación de la voz y reconocimiento de la firma, de esta manera se afirma que los sistemas biométricos se han desarrollado como respuesta a la creciente demanda de seguridad existente en la actualidad y aunque algunos de ellos son altamente fiables, ningún sistema es efectivo al 100%, y estos sistemas también son susceptibles de ser engañados.

En la actualidad **IBIX S.A. de C.V.** cuenta con una gran variedad de equipos biométricos obtenidos de diferentes fabricantes, con lectores de huella digital y lector de tarjeta de proximidad, reconocimiento facial y tarjeta de proximidad, reconocimiento facial y huella digital, lector de palma de mano y lector de venas y equipos de huella portátiles. De esta manera, se pueden dividir en gama baja, que incluyen terminales biométricas para pequeñas empresas recomendados para no más de 50 usuarios de oficina, los de gama media que son terminales biométricas para medianas empresas recomendados hasta para 200 usuarios, y los de gama alta son equipos recomendados para grandes empresas tipo manufacturas, recomendados para 300 usuarios o más.

En la tabla 1 se muestra de una forma general los principales equipos que comercializa la empresa **IBIX, S.A. de C.V**; **ZKTECO,** son equipos biométricos considerados de gama baja y media, tal y como se muestra en la siguiente tabla:

ZKTECO GAMA BAJA		ZKTECO GAMA MEDIA	
ZKTeco LX50 Reloj Checador de Huella Digital		**ZKTeco SFace900** ID Reconocimiento Facial y Huella Digital	
ZKTeco K40 Reloj Checador de Huella Digital		**ZKTeco P160** Reconocimiento de Palma-Mano y Huella Digital	
ZKTeco X629-C Reloj Checador de Huella Digital		**ZKTeco MB360** Reconocimiento Facial y Huella Digital	

Tabla 1. Equipos biométricos ZKteco.

ZKTeco UA860 Reloj Checador de Huella Digital		**ZKTeco uFace800** Reconocimiento Facial y Huella Digital	
ZKTeco UA300/MF Reloj Checador de Huella Digital		**ZKTeco inPulse ID** Reconocimiento de Venas	

Continuación: Tabla 1. Equipos biométricos ZKteco.

Los equipos **ZKteco** están disponibles para su distribución como parte de una oferta innovadora diseñada para la aplicación de asistencia de usuarios, con función de acceso simple en el caso de los de gama baja, con respecto a los que son de gama media brindan una gestión de tiempo y asistencia además de aplicaciones de control de acceso mejorado con funciones de reconocimiento facial, huella digital y lectura de palma – mano.

En la tabla 2 se muestran los equipos **SUPREMA BIOMETRICS**, son equipos considerados de gama media, diseñados para ofrecer una solución de autenticación con alto nivel de seguridad.

SUPREMA BIOMETRICS		CARACTERÍSTICAS
X-Station Terminal para Control de Asistencia y Acceso		-Detección de rostro con registro de imagen. -Interfaz TCP/IP
BioEntry Plus Lector Huella Digital de Acceso		**-**Tecnología Biométrica de Huella de Suprema Renombrada a Nivel Mundial. -Interfaz TCP/IP

Tabla 2. Equipos biométricos Suprema Biometrics

Suprema BioLite Net Reloj checador de Huella Digital		**-**Maneja una gran cantidad de datos necesarios para una rápida y precisa verificación, mientras asegura la operación ininterrumpida del dispositivo.
BioStation Reloj Checador de Huella Digital		-Interfaces de comunicación extensivas tales como TCP/IP, RS485, Wiegand, así como salidas de relevador.

Continuación: Tabla 2. Equipos biométricos Suprema Biometrics

Los biométricos **SUPREMA BIOMETRICS**, ofrece interfaces con diferentes sistemas lo que facilita al usuario una interacción con dichos dispositivos, otros aspectos que los caracteriza a la mayoría de estos equipos es que están diseñados con una tecnología que los hace resistentes al agua y al polvo.

Otros de los equipos que distribuye **IBIX, S.A. de C.V,** son los de **RECONOCIMIENTO FACIAL** (tabla 3), característicos de gama alta, soportando métodos de verificación por medio de rostro, huella digital, tarjeta, contraseña y combinaciones entre estas, a continuación, algunos ejemplos:

RECONOCIMIENTO FACIAL		**CARACTERÍSTICAS**
ZKTeco MB360 Reconocimiento Facial y Huella Digital		Terminal MultiBiométrica de Reconocimiento Facial y Huella Digital Pantalla TFT Color de 2.8 Pulgadas Capacidad de 1,200 rostros y 1,500 huellas Capacidad de 100,000 registros de checadas Comunicación en Red TCP/IP y USB

Tabla 3. Equipos biométricos de Reconocimiento Facial

ZKTeco SFace900 ID Reconocimiento Facial y Huella Digital		Nueva Generación SFace con cámara de alto rendimiento apta para instalación exterior Terminal MultiBiométrica de Reconocimiento Facial y Huella Digital Pantalla TFT Touch Color de 4.3 Pulgadas Capacidad de 3,000 rostros, 4,000 huellas, 10,000 tarjetas Capacidad de 100,000 registros de checadas Comunicación en Red TCP/IP, RS232/485, USB
Suprema FaceStation Reloj checador Facial		Terminal Biométrica de Reconocimiento Facial Pantalla WVGA Color de 4.3 Pulgadas Touch Screen Capacidad de Usuarios 10,000(1:1), 1,000(1: N) Capacidad de Eventos 1,000,000 de registros / 10,000 imágenes Comunicación en Red TCP/IP y USB-Host&Slave
ZKTeco uFace800 Reconocimiento Facial y Huella Digital		Nueva Generación Serie uFACE sustituye a la exitosa Serie iFACE Terminal MultiBiométrica de Reconocimiento Facial y Huella Digital Pantalla TFT Touch Color de 4.3 Pulgadas Capacidad de 3,000 rostros y 4,000 huellas Capacidad de 100,000 registros de checadas Comunicación en Red TCP/IP y USB-Host Cámara Infrarroja de Alta Resolución

Continuación: Tabla 3. Equipos biométricos de Reconocimiento Facial

Por último uno de los equipos que comercializa la empresa **IBIX, S.A. de C.V** es el reloj checador **IBIX-UCONTROL** (tabla 4), es un reloj diseñado y fabricado por IBIX para el sector industrial, tiene como principal característica la gran capacidad para adaptarse a los requerimientos de hardware y software, además de su capacidad de programación, validación de turnos, autorización por supervisor, configuración

de dispositivos de lectura a elección de cliente, interconexión con dispositivos externos y software de aplicación de control de asistencia.

IBIX-UCONTROL	CARACTERÍSTICAS
	Reloj Checador de Huella Digital uControl 7000 Ethernet Uso Rudo Lector de Huella Digital BioEntry Suprema con capacidad de 9090 Huellas Digitales en Modo 1:1 o Modo 1: N Identificación Modo 1: N, sólo se requiere poner la Huella Digital Validación Modo 1:1 digitando NIP + validación de Huella Digital Validación Modo 1:1 Opcional con Lector de Proximidad HID Memoria cíclica hasta 12,288 checadas Puerto de Red Ethernet TCP/IP Batería de Respaldo de Datos Display iluminado 16x2 con Mensaje Rotativo

Tabla 4. Equipo biométrico IBIX-UCONTROL

En general, **IBIX S.A. de C.V.**, es una empresa en la que se desempeñan diferentes actividades, de manera que garantice la satisfacción de sus clientes, una de ellas es la comercialización de los diferentes tipos de equipos biométricos acorde a las necesidades de cada uno de ellos, tales como; la cantidad de empleados que maneja, las actividades que desempeñan, los horarios que manejan, entre otras, de esta manera se le da la mejor opción para el uso adecuado del equipo que se solicite, en el capítulo siguiente se muestra de una forma concreta sobre los controles de acceso que son parte importante de las actividades que se llevan a cabo en esta empresa, debido a que los equipos mencionados en este apartado pueden implementarse para realizar este tipo de actividad, además de los controles de acceso.

1.4 Controlador lógico programable (PLC)

Un Controlador Lógico Programable es un equipo electrónico que utiliza una memoria programable para almacenamiento interno, está diseñado para controlar, en tiempo real y en ambiente de tipo industrial con instrucciones diseñadas acorde a las necesidades de cada usuario. En general la función del controlador lógico programable es ejecutar tareas específicas tales como enlaces lógicos, secuenciación, temporización y cálculo para controlar a través de entradas y salidas digitales o analógicas, diversos tipos de máquinas o procesos, el Controlador Lógico Programable y sus periféricos están diseñados de forma que se puedan integrar fácilmente en un sistema de control industrial y ser utilizados en todas las aplicaciones previstas de la manera más sencilla [Valdés, 2012].

A continuación (figura 5) se muestra la arquitectura de un Controlador Lógico Programable, especificando de manera gráfica cada uno de sus componentes para su funcionamiento, tales como; fuente de alimentación, bus de datos, módulo de unidad central de proceso, módulo de entradas y salidas digitales, módulo de entradas y salidas analógicas, de esta manera el Controlador Lógico Programable es considerado uno de los principales componentes en el funcionamiento de los controles de acceso [Valdés, 2012].

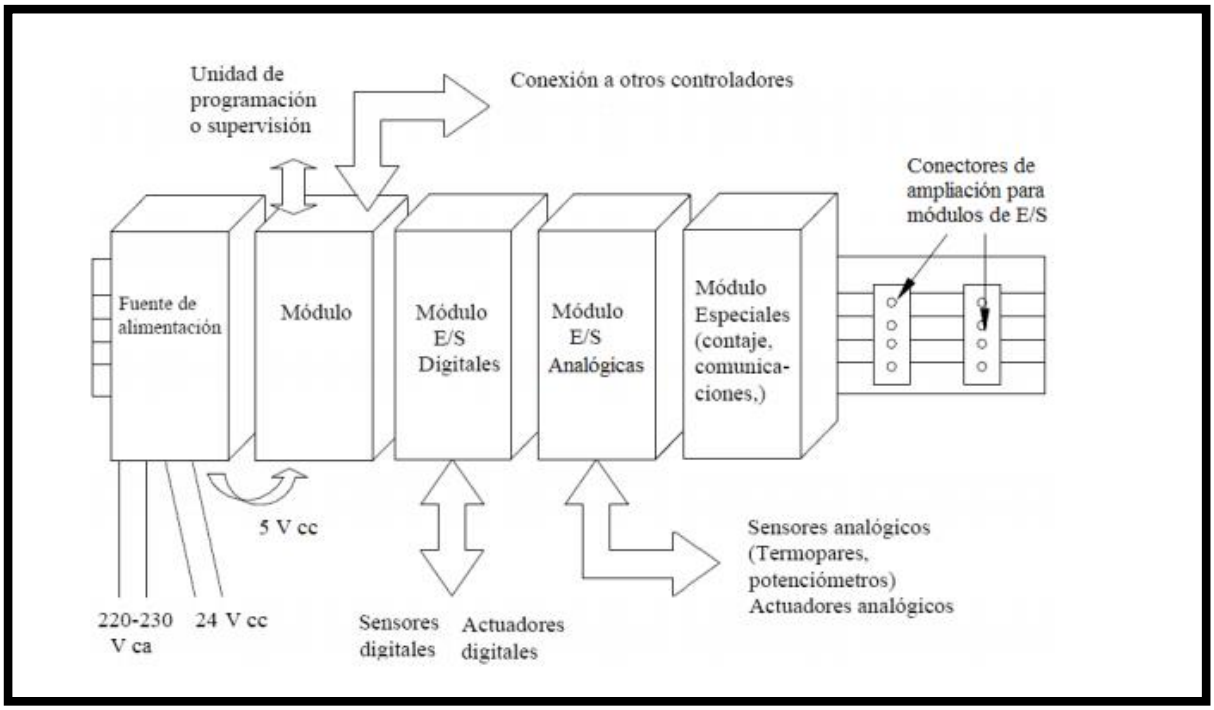


***Figura 5. Arquitectura de un Controlador Lógico Programable** [Valdés, 2012].*

1.5 Cerradura electromagnética

En general se define una cerradura electromagnética como un dispositivo de bloqueo que desde hace mucho tiempo se ha incorporado a puertas como un dispositivo de seguridad que permite u obstruye el acceso a algún sitio. El principio de funcionamiento de la cerradura electromagnética consiste en un electroimán que atrae a un conductor con una fuerza producida por un campo magnético que evita que la puerta se abra [Gutiérrez, Serrano, 2016].

El campo magnético es producido cuando un solenoide se envuelve alrededor de un núcleo ferromagnético, cuando el solenoide esta energizado fluye una corriente en el embobinado que genera el campo magnético, el cual se denomina inducción magnética, esta inducción es la fuerza con la que se atrae el núcleo del imán, cuando se corta la energía se pierde el campo magnético y las placas se separan [Gutiérrez, Serrano, 2016].

Figura 6. Cerradura Electromagnética

1.6 Servidor Web

El Servidor Web es un sistema operativo que permite controlar y administrar recursos físicos y lógicos de otras computadoras que se encuentren en el mismo segmento de red, para llevar a cabo este procedimiento se tiene que estructurar un modelo que es denominado Cliente – Servidor [Olvera, Rizo, 2013].

Un cliente, es una computadora de escritorio que brinda una interfaz sencilla para el usuario, para tener acceso a la utilización de aplicaciones como software, base de datos, procesadores de texto hojas de cálculo entre otros. El servidor se encarga de compartir los servicios, programas y accesos a la misma estructura de base de datos [Olvera, Rizo, 2013].

El modelo Cliente - Servidor se basa en un protocolo solicitud - respuesta, la cual debe realizarse en el mismo segmento de red de interconexión, el cliente realiza él envió de un mensaje al servidor para solicitar un servicio determinado, el servidor realiza la tarea solicitada y regresa los datos pedidos o un código de error que muestre la razón por la cual no se logró llevar a cabo el proceso, en la siguiente figura 7 se muestra la comunicación Cliente- Servidor [Olvera, Rizo, 2013].

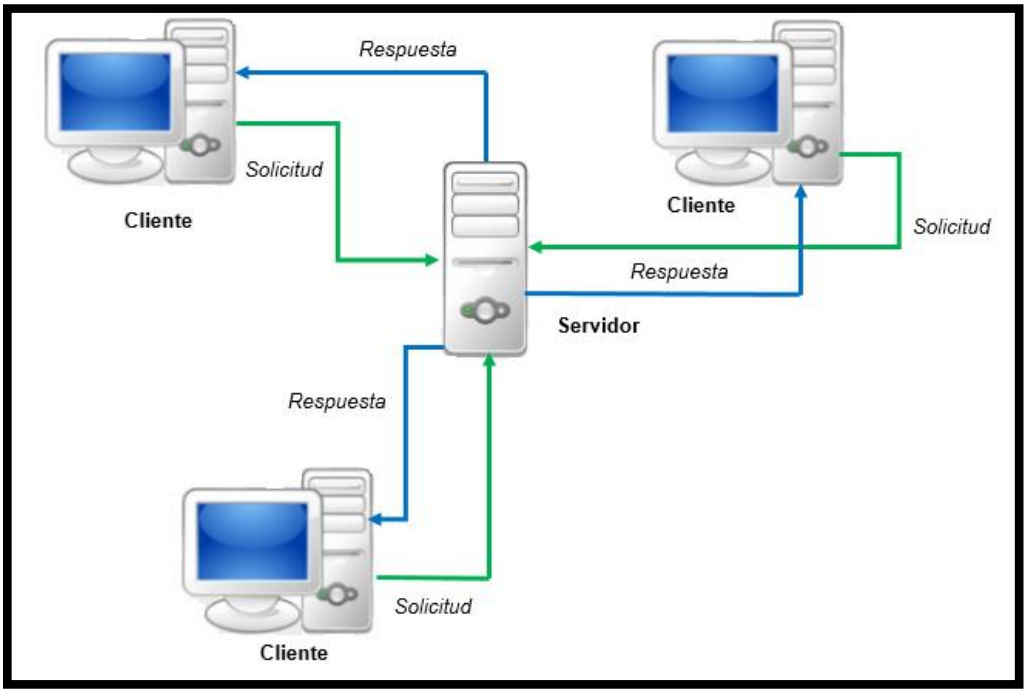


Figura 7. Comunicación del Cliente - Servidor

Un servidor es muy importante para una empresa industrial ya que permite centralizar todos los programas y base de datos para todas las computadoras, si un equipo cliente se daña es posible quitar y agregar sin afectar el funcionamiento del servidor.

1.7 Nodo de red RJ45

Es un cableado estructurado compuesto por un cable llamado UTP (Unshielded Twisted Pair - par trenzado sin blindaje) que se compone de cuatro cables trenzados y dos conectores RJ45 uno en cada extremo, también conocido como patch cords, se utiliza para transportar información, datos, recursos físicos sin importar donde se encuentre la localización física de los dispositivos, haciendo que un recurso compartido por un sistema remoto funcione como de forma local [Fabla, Vélez, Moran, 2011].

Para el funcionamiento el nodo de red RJ45 el cable va conectado de la PC o a dispositivos que tengan salidas para internet y a un switch para la interconexión, por

lo general se utiliza un cable con configuración directa, el cableado tiene que cumplir con la norma estándar EIA/TIA 568 A.

La norma estándar EIA/TIA 568 A establece que el cable UTP debe contar con 8 hilos, los cuales se dividen en 4 pares y 2 conectores Rj45 que cuentan con 8 pines cada uno, de esta manera van conectados a cada extremo; blanco/naranja de pin 1 a pin 1, naranja de pin 2 a pin 2, blanco/verde de pin 3 a pin 3, azul de pin 4 a pin 4, blanco azul de pin 5 a pin 5, verde de pin 6 a pin 6, blanco/café de pin 7 a pin 7 y café de pin 8 a pin 8, [Castellón, 2014] como se muestra en la siguiente figura 8.

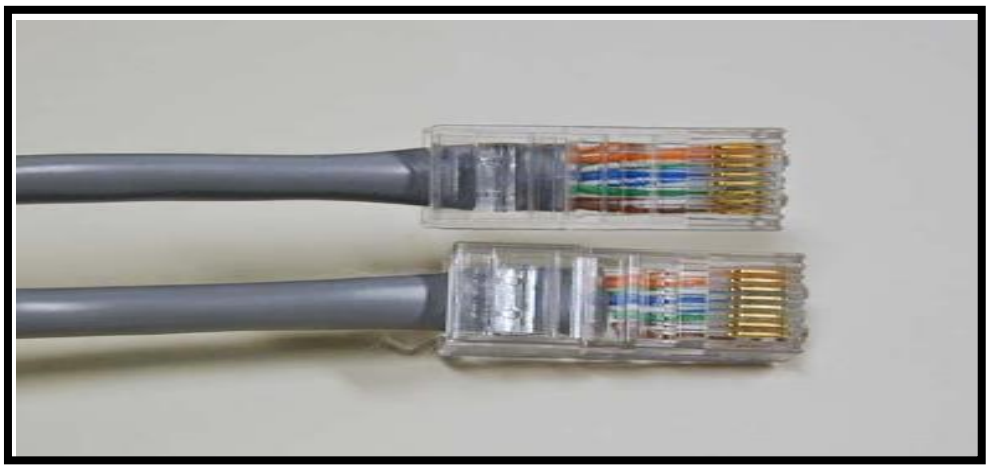


Figura 8. Conexión de cable UTP con RJ45

Este tipo de cableado estructurado solo se emplea para conectores RJ45, de esta manera es una toma única que debe servir para conectar los equipos de cómputo a la red con dispositivos que tienen salidas a internet que van conectados a un switch.

1.8 Switch

El Switch es un dispositivo electrónico de interconexión de redes de ordenadores que opera para el nivel de enlace de datos, un switch interconecta dos o más segmentos dentro de una red local, es un accesorio que se utiliza para conectar múltiples redes, fusionándolas a una sola, además de que sirve para eliminar la interferencia en las comunicaciones y logrando la seguridad de transferencias de

datos de una forma rápida y segura. Para su funcionamiento el switch debe contar con un router para conectarse a una red, es un dispositivo que proporciona conectividad a nivel de red por medio de cables UTP conectado en conjunto con el switch [López, 2008]

Para el acceso al internet que brinda el router tiene que venir configurado por medio de un IP que el fabricante asigna al dispositivo, la dirección IP (Protocolo de Internet) se describe en cuatro números decimales separados por puntos, cada punto es un byte de dirección y cada interfaz debe tener una dirección IP única, conceptualmente cada IP es una par (id red, id anfitrión), donde id red es la que identifica a una red, e id anfitrión es la que identifica a un anfitrión dentro de la red, por ejemplo la dirección IP 192.168.1.150 el anfitrión que se idéntica es el 150 que está dentro de la red 192.168.1.0, un anfitrión puede ser cualquier dispositivo conectado a internet por ejemplo una computadora, impresora, un equipo biométrico, etc., de esta manera se pueden interconectar hasta 254 dispositivos la misma red [Montaño, 2006].

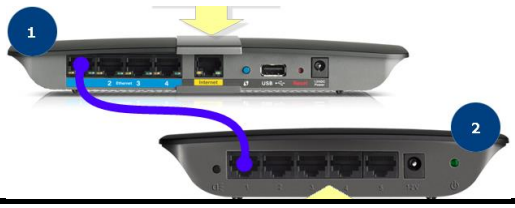
EQUIPOS DE RED		CARACTERÍSTICAS
Switch		-Fuente de alimentación de entrada de 120 VCA con salida de 48 VCD a 1.25 A - 8 puertos salida con RJ 45
Router		-Fuente de alimentación entrada 120 VCA con salida 12VCD a 0.5 A - Banda de 2,4 y 5 GHZ - 4 puertos Ethernet.
CONEXIÓN ROUTER-SWITCH		
La siguiente imagen con el número 1 es el router que va conectada con un cable de red RJ45 macho en uno sus puertos de salida que interconecta con el switch conectando a su puerto de entrada para la distribución del Ethernet, imagen con número 2. 		

Figura 9. Conexión Switch- Router

En general los componentes mencionados anteriormente, forman parte importante del funcionamiento de los controles de acceso, que se articulan con otros componentes de una forma complementaria para garantizar una correcta puesta en marcha de los sistemas biométricos de los cuales se hablara a mayor detalle en el siguiente capítulo.

CAPÍTULO 2. IMPLEMENTACIÓN DE CONTROLES DE ACCESO

2.1. Control de acceso implementado con puertas

Una vez conociendo los antecedentes históricos de la empresa **IBIX, S.A. de C.V.**, así como su estructura funcional y los principales equipos biométricos que comercializa, en este apartado se pretende dar a conocer cómo se lleva a cabo la implementación de controles de acceso implementados con puertas, torniquetes y barreras vehiculares, que forman parte de las principales actividades que se realizan en dicha empresa.

Antes de describir la implementación de los controles de acceso es importante mencionar que un control de acceso se ha definido como un sistema electrónico que restringe o permite acceso de un usuario o grupos de usuarios a un área específica, validando la identificación por medio de diferentes mecanismos, ya sea por tarjetas de proximidad, por biometría, entre otros, y a la vez controlando varios tipos de dispositivos [Mora, 2016]

Hace algunos años para restringir el acceso a ciertas áreas de las empresas se hacía a partir de accesorios mecánicos como; cerrojos, llaves, entre otros, sin embargo, hoy en día han sido sustituidos por un sistema de control más fiable, como son los equipos electrónicos. En la actualidad, la implementación de controles de acceso, forman parte de una necesidad primordial para las pequeñas y grandes empresas, ya que de esta manera logran tener un mayor control sobre los trabajadores, así como restringir el acceso a áreas específicas, además de que con los nuevos mecanismos de seguridad que se manejan, evita que alguien pueda suplantar la identidad de algún otro trabajador.

Para la instalación de un control de acceso implementado con puertas, en primer lugar, se tiene que saber el tipo de puerta a controlar, comúnmente las puertas abatibles están instaladas con bisagras, giran 180 grados con movimiento hacia afuera o hacia adentro, también es importante definir de qué lado se va abrir la puerta para su comodidad y seguridad, una vez teniendo claro este requerimiento, se necesitará; cable múltiple con calibre de 16 AWG (American Wire Gauge), dos

fuentes de voltaje, dos batería de respaldo, dos chapas electromagnéticas, dos soportes L/z, dos equipos biométricos con parámetros de control de acceso, Controlador Lógico Programable, una fuente de voltaje para el Controlador Lógico Programable , un servidor, un switch, nodos de red (ver tabla 5).

MATERIAL		CARACTERÍSTICAS
Cable múltiple con calibre de 16 awg (american wire gauge)		Resistente a la humedad 13 Amper Cable de cobre blando con aislación de PVC Temperatura de operación a 80°
Fuente de voltaje		Convierte el voltaje de corriente alterna (VCA) a voltaje de corriente directa (VCD) Capacidad de 4 Ampere Salida de 12 VCD
Batería de respaldo		Batería de respaldo de 7 Ampere. Duración de 5 horas Voltaje de 12 VCD
Chapa electromagnética		Fuerza de sujeción de 280kg (600 lbs) Voltaje de 12/24 VCD Dimensiones del imán 250x51.8x27.9mm Dimensiones de la placa 180x38.8x13mm Peso 2 kg
Soporte L/Z		Aluminio reforzado Medida soporte L 250x48.8x30.4mm Medida de soporte Z 180x50x50mm
Equipo Biométrico		Lector de huella y tarjeta de proximidad Capacidad de 5000 huellas Comunicación por TCP/IP

Tabla 5. Material para el control de acceso implementado con puertas

Fuente de voltaje del PLC		Voltaje de entrada de 120 VCA Voltaje de salida de 24 VCD Corriente de 4.2 A Voltaje ajustable de 24 a 29 VCD
Controlador lógico programable (PLC)		8 entradas digitales 6 salidas digitales 24 VCD Indicadores de led de Run o Stop Puertos de comunicación Ethernet/ RS485 Módulo de 8 entradas digitales Módulo de 8 salidas digitales
Cable de red		Cable de red con RJ45 macho Color azul

Continuación: Tabla 5. Material para el control de acceso implementado con puertas

Para llevar a cabo la instalación del control de acceso de una puerta abatible, es necesario que el cliente proporcione una instalación eléctrica de 120 VCA regulada y aterrizada, así como una instalación de los nodos de red con RJ45 macho, y servidor disponible para la base de datos, es necesario que esté realizada la instalación del switch para proceder a la implementación del control de acceso.

De igual forma se sugiere al cliente que la instalación eléctrica debe de ser de un circuito independiente, esto para garantizar la protección de sobre corriente, protegida con interruptores magnéticos de 15 A, calibre de cable 12 AWG, para la alimentación del Control Lógico Programable, es importante puntualizar que para los equipos biométricos con huellas dactilares el Control Lógico Programable tiene que ser instalado y programado por un proveedor independiente, indicado cuales son las entradas digitales y salidas digitales para el control de la puerta, algo complementario a la implementación del control de acceso es incluir un botón de emergencia, para deshabilitar las puertas en caso de alguna contingencia.

Una vez teniendo las condiciones óptimas de la instalación eléctrica, se realiza la colocación del gabinete en cada puerta (de entrada y salida) el cual está compuesto

por una fuente de voltaje con entrada de 120 VCA y voltaje de salida de 12 VCD, también incluye una batería de respaldo de 7 A con una duración de 4 a 5 horas, siendo de gran apoyo en el caso de alguna emergencia por falla de la energía eléctrica (figura 10).

Figura 10. Regulador de voltaje con batería de respaldo

Con la instalación del gabinete, se procede a instalar las cerraduras electromagnéticas de 600 lbs (figura 11), para puertas abatibles de metal, se fijan los electroimanes en el marco de la puerta y la placa metálica va instalada directamente en la puerta, se instalan también los brazos mecánicos para que realicen el cierre de las puertas y de esta manera funcionen adecuadamente, algo muy importante es que deben de estar alineados de forma paralela. Las cerraduras requieren una alimentación de 12 VCD y una corriente de 250 mA la cual se obtiene de los reguladores de voltaje instalado anteriormente, el cableado para las cerraduras es de calibre 16 AWG, para evitar una caída de voltaje se recomienda que la fuente no se encuentre a más de 30 metros de la cerradura electromagnética, algo muy importante que se debe tener presente es que el equipo está diseñado para instalaciones solamente en interiores.

Figura 11. Instalación de la cerradura electromagnética en una puerta

Posteriormente, se hace la instalación de los dispositivo biométricos de lector de huella digital (figura 12) a una altura de 1.20 m sobre nivel del piso, realizando también la conexión eléctrica, verificando la polaridad positivo (+) y negativo (-) de la salida de la fuente de voltaje de 12 VCD, se conecta el nodo de red RJ45 macho a la entrada del nodo de red RJ45 hembra de cada uno de los dispositivos biométricos, una vez que está instalado el dispositivo, se procede a la configuración de la dirección IP, mascara de red y puerta de enlace para poder enlazar el equipo al sistema de red del cliente y se pueda controlar desde el servidor de este.

La dirección IP es un número único para cada equipo, representado por cuatro cifras separadas por puntos quedando determinado el número 254 como límite, por ejemplo 192.168.1.15 es la dirección de la máquina del usuario y a la red que pertenece [Estrada, 2004].

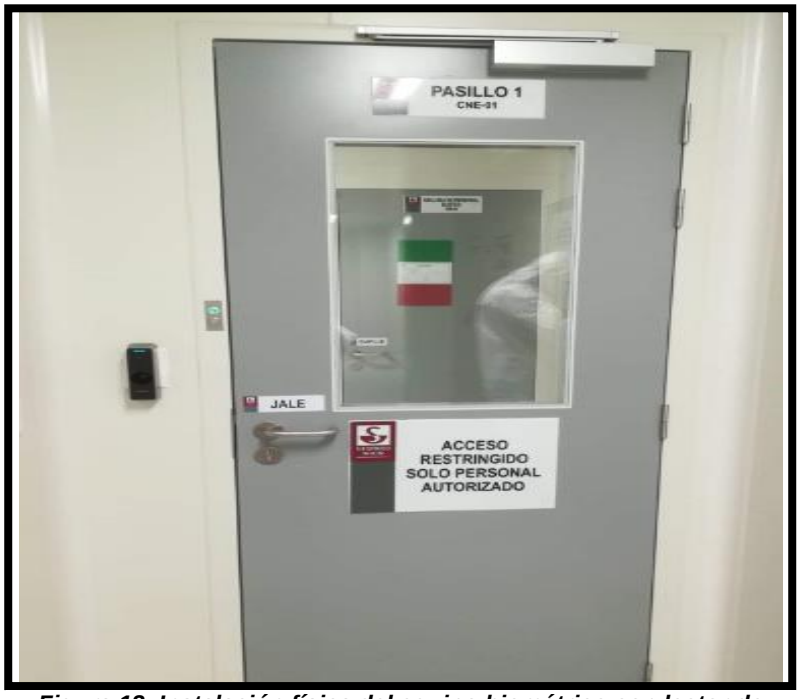


Figura 12. Instalación física del equipo biométrico con lector de huella digital

2.1.1 Conexión y funcionamiento del Controlador Lógico Programable con las cerraduras electromagnéticas

Para la instalación de un control de acceso implementado con puertas, una vez colocando los equipos biométricos y las chapas electromagnéticas en los lugares estratégicos, para su funcionamiento se procede a realizar la conexión eléctrica del Controlador Lógico Programable.

Tal y como se puede observar en la figura 13 -1, el Controlador Lógico Programable cuenta con una fuente de voltaje con entrada de 120 VCA y salida de 24 VCD necesarias para que este dispositivo se mantenga encendido, por lo regular para este tipo de control de acceso se utilizan dos entradas y dos salidas del Controlador Lógico Programable, las dos salidas (Q0.0, Q0.1) van conectadas a las cerraduras electromagnéticas (Cerradura de entrada V+ - Q0.0 y Cerradura de salida V+ - Q0.1), las dos entradas del Controlador Lógico Programable (I0.0, I0.1), van conectadas van conectadas a lose quipos biométricos (I0.0 – PIN1del biométrico de entrada y I0.1 – PIN1 del biométrico de salida), así también se realiza una conexión

llamada común (COM) PIN2 – M de cada uno de los biométricos cuya funciones cerrar el circuito, adicionalmente se coloca un botón de emergencia que va conectado al Controlador Lógico Programable (I0.2 – NO y M - COM), dicho botón se puede accionar manualmente en caso de que se presente alguna emergencia para liberar las puertas.

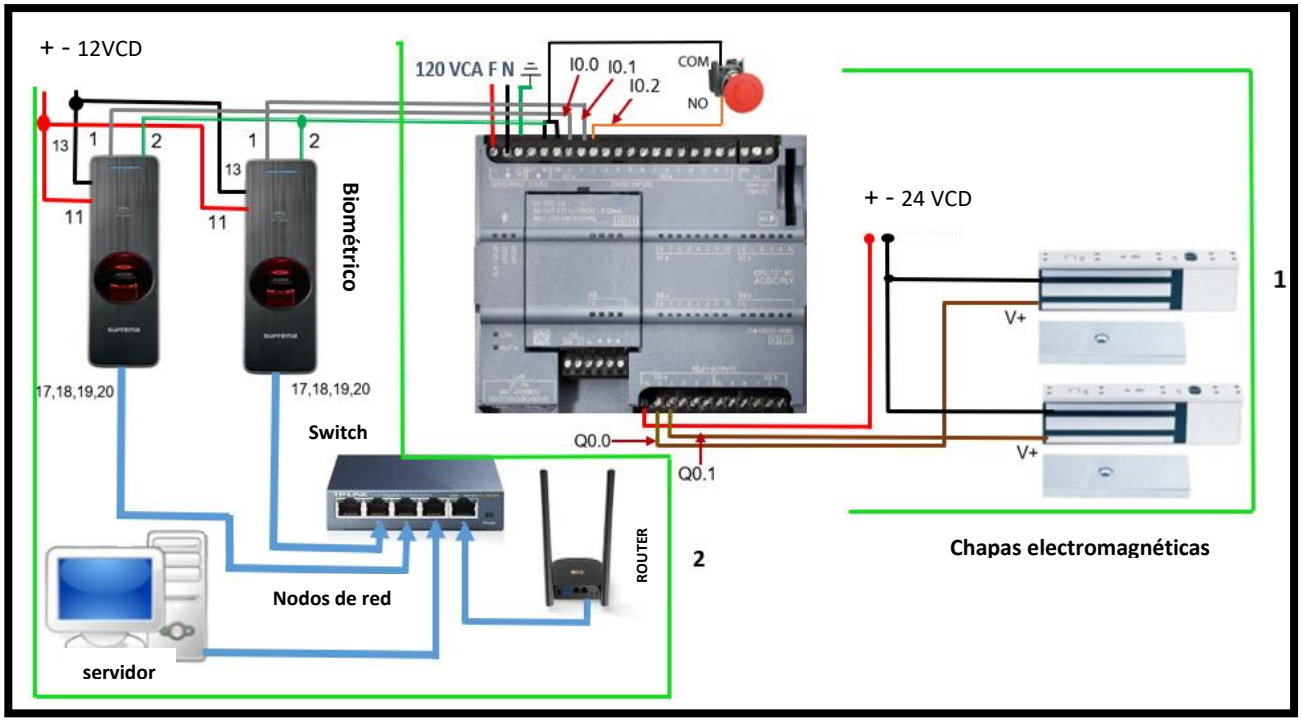


Figura 13. Diagrama eléctrico de un control de acceso implementado con puertas

Una vez contando con las conexiones de entradas y salidas del Controlador Lógico Programable con las cerraduras electromagnéticas, así como con los equipos biométricos, el funcionamiento inicia cuando el equipo biométrico detecta una señal de lectura de huella ya sea de entrada o salida, el equipo biométrico genera una señal de salida que se direcciona hacia la entrada del Controlador Lógico Programable, de esta manera una vez que el controlador detecta la señal ejecuta la programación cargada previamente por un proveedor externo, una vez terminando este proceso se envía una señal de salida a la cerradura electromagnética dando acceso al usuario.

En el apartado 1 de la figura 13 se puede visualizar el proceso descrito anteriormente, sin embargo, para el funcionamiento del control de acceso

implementado con puertas también es importante la ejecución de otros elementos complementarios como el nodo de red, el switch y el servidor, que se articulan para lograr concluir el proceso de acceso a través de puertas.

2.1.2. Conexión y funcionamiento de los nodos de red, el servidor y del switch con los equipos biométricos.

Para el funcionamiento de los controles de acceso implementados con puertas, además de la conexión del Controlador Lógico Programable con la cerradura electromagnética y los biométricos, también es importante la conexión y el funcionamiento que deben tener los biométricos con el nodo de red, switch y el servidor.

De esta manera los nodos de red son cables estructurados cuyo funcionamiento es trasferir información, en el caso específico de los controles de acceso implementados con puertas, los nodos de red son de gran importancia debido a que son el medio de comunicación entre los equipos biométricos, el switch y el servidor, es decir transporta datos como; los nombres de los trabajadores, huellas digitales, fotografías y registros de checadas de los trabajadores.

Para el funcionamiento de este tipo de control de acceso se debe iniciar asignando una IP fija para cada equipo biométrico de esta manera permitirá que los equipos se puedan mantener en el mismo segmento de red, así también se debe precargar la información de los trabajadores en el servidor creando una base de datos. Una vez teniendo los equipos biométricos en red, así como la base de datos precargada en el servidor, en ese momento inicia el funcionamiento de los nodos de red, que son los encargados de llevar la información del servidor a los equipos biométricos, siendo un proceso importante debido a que, si no se cuenta con esta información en los equipos biométricos, los usuarios no podrán ingresar como se muestra en la (Figura 13) aparado 2 marcado de color verde.

El switch es otro componente importante ya que en conjunto con el router se encarga de generar y mantener fijas las IP´S tanto para los equipos biométricos como para el servidor, como podemos observar en la figura 13-2 el switch va conectado con el router, con el servidor y con los equipos biométricos por medio de

nodos de red, estas conexiones garantizan que tanto los equipos biométricos y el servidor se mantengan en una red local con una IP fija para cada equipo y de esta manera se puedan transferir información del servidor a los equipos biométricos, es decir el switch en conjunto con el router son los dispositivos que brinda la estabilidad de comunicación entre los equipos biométricos y el servidor.

Por su parte el servidor siendo un sistema operativo encargado de ejecutar programas, almacenar datos y transferir información, en el caso del control de acceso implementado con puertas, funciona como un medio de almacenamiento de la base de datos, así como del software IBIX control de acceso, siendo de gran importancia ya que una vez teniendo esta información en el dispositivo se puede realizar él envió de datos de los trabajadores a los equipos biométricos, así como recolección de checadas, consulta de reportes de las checadas de los usuarios.

En la figura 14 se muestra el proceso de funcionamiento del control de acceso de manera sistemática implementado con puertas, describiendo los pasos de funcionamiento del envió de la información al Control Lógico Programable con las chapas electromagnéticas, los biométricos y componentes complementarios que son esenciales para la ejecución del control de acceso.

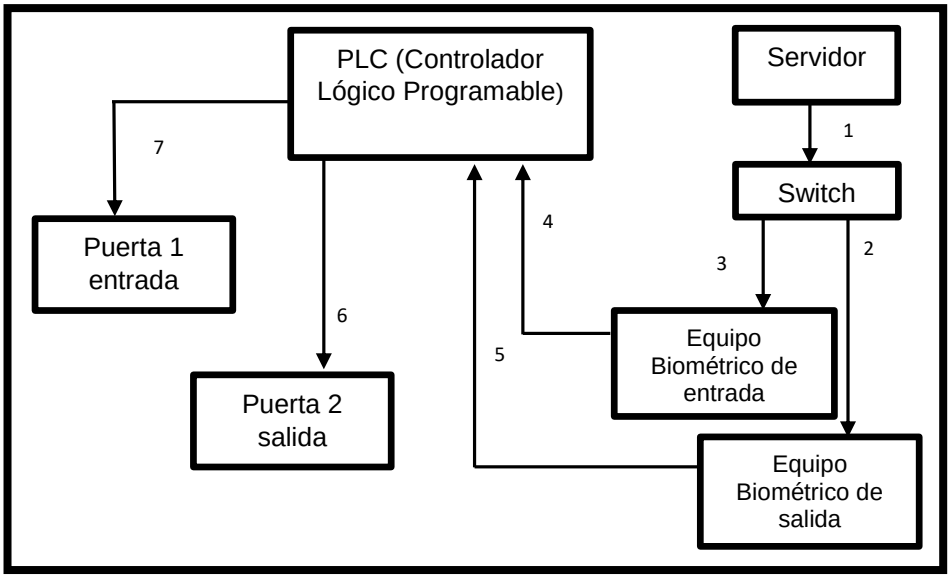


Figura 14. Proceso de funcionamiento de control de acceso con dos puertas

Una vez que se tiene la carga de la base de datos con la información de los trabajadores en el servidor (paso 1, figura 14); nombre completo, número de trabajador, área, departamento al que pertenece y la huella digital se envían los datos y el swich se encarga de distribuir en cada uno de los equipos biométricos.

Los equipos biométricos cuentan con una memoria interna en la que una vez transferidas las huellas digitales, se almacenan, de esta manera cuándo el trabajador coloca la huella en los lectores de entrada o salida (paso 2 o 3, figura 14), estos se tardan entre 2 a 3 segundos en verificar la huella almacenada, posteriormente comparar la huella obtenida en el momento de realizar la checada con la que ya tiene almacenada anteriormente, si estas coinciden permite el acceso, de lo contrario, se niega el acceso en los equipos, si el acceso es positivo los equipos biométricos manda una señal al controlador PLC, (paso 4 o 5, figura 14) para habilitar la puerta 1 o la puerta 2 (paso 6 o 7, Figura 14), brindando acceso en la puerta de entrada o de salida.

Teniendo la instalación eléctrica de los diferentes componentes así como del software sistema ibix, se imparte la capacitación sobre el software al personal de recursos humanos incluyendo los siguientes temas; dar de alta un trabajador en el software, captura el turno y rotación, captura de concepto de ausentismo, como dar de alta las huellas desde un biométrico de escritorio, transferir las huellas a los equipos biométricos instalados para el control de acceso, extraer checadas a la base de datos instalado en el servidor y los reportes de entradas y salidas de los trabajadores.

En la siguiente figura 15 se muestra la instalación del software ibix, el sistema se ejecuta como administrador para no tener incidencia de permisos o sea bloqueado por el antivirus. Para la instalación del software ibix control acceso, en primer lugar, se instala el aplicativo del sistema que tiene que ser en el disco duro para posteriormente ejecutarlo, posteriormente registra la empresa colocando datos como: la razón social, número de instalación, número de licencia y el número de nómina, por último, una vez teniendo registrada la empresa se procede a dar de alta el equipo biométrico colocando el número de licencia y la IP asignado.

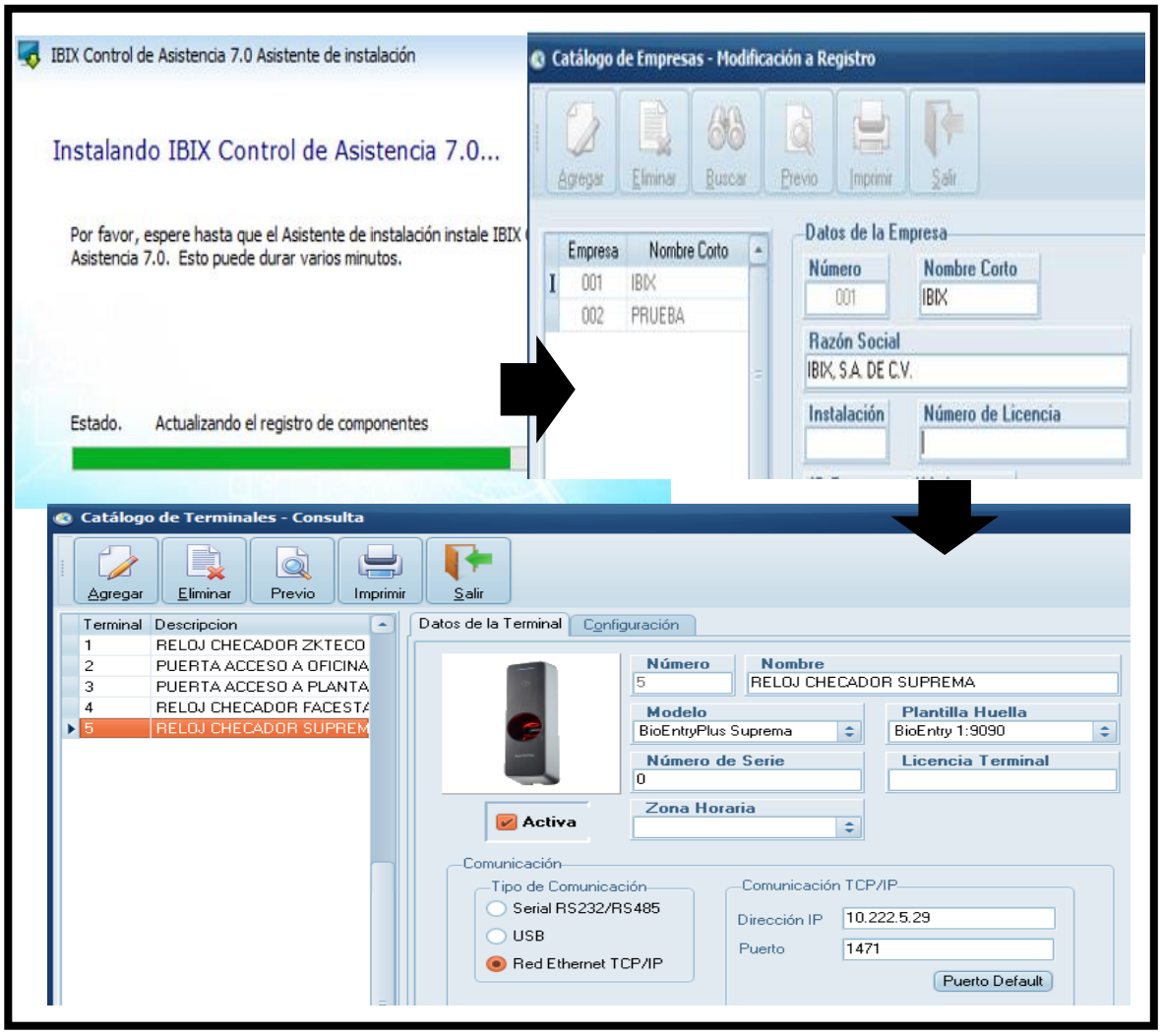


Figura 15. Instalación del software Sistema IBIX

En la figura 16 se puede observar cómo se da de alta un trabajador, una vez dado de alta el equipo biométrico se puede dar de alta un trabajador en el sistema, para esto se ingresa al catálogo de trabajadores, posteriormente se agrega el número de trabajador, Nombre, área y departamento al que pertenece, categoría, tipo de empleado y centro de trabajo.

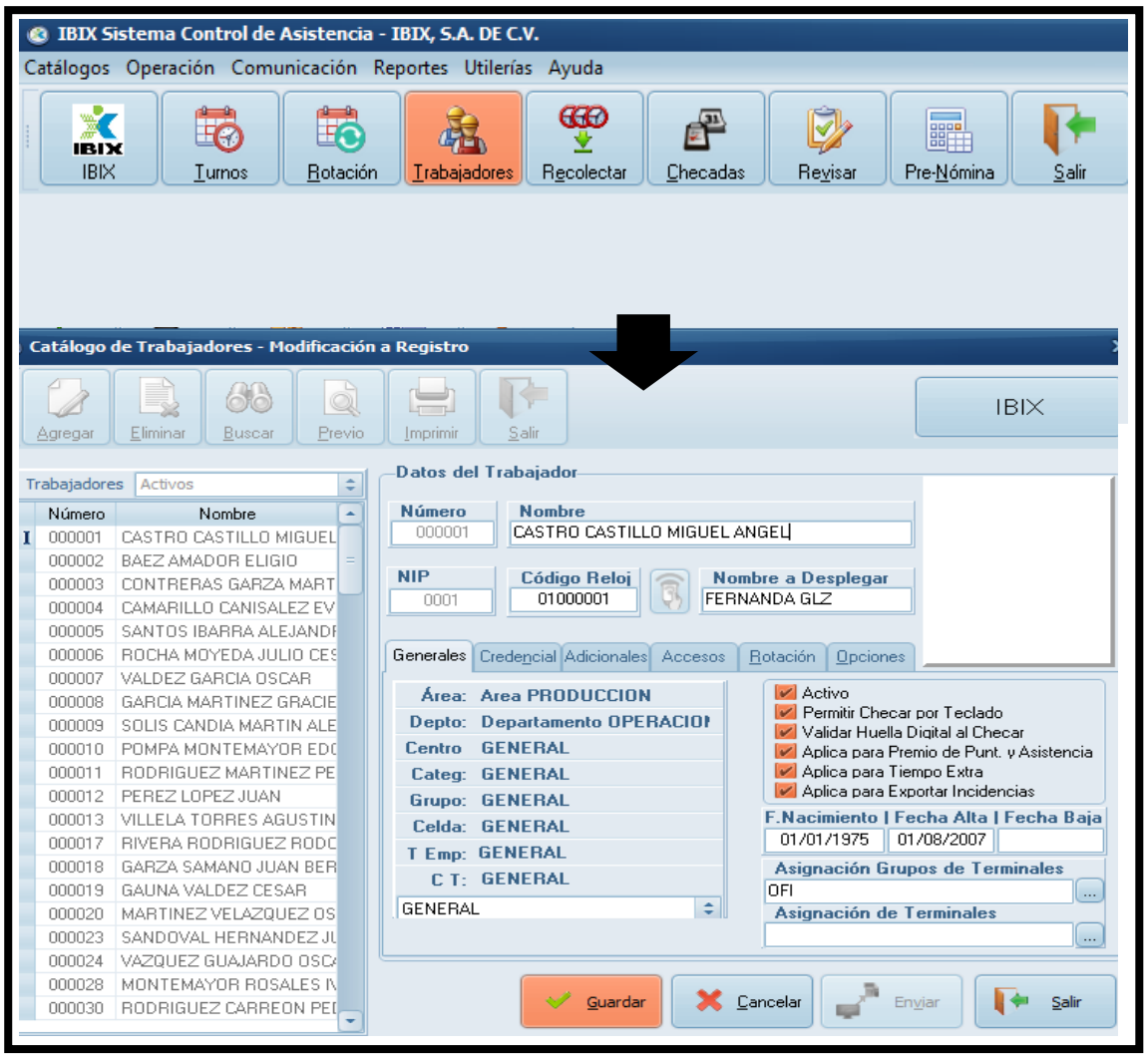


Figura 16. Dar de alta un trabajador en el Sistema IBIX

Una vez teniendo el registro de los trabajadores en el sistema, para dar de alta sus huellas desde el software con el equipo biométrico de escritorio, se sugiere dar de alta dos huellas digitales de cada empleado, una vez hecha la captura de la huella digital se seleccionan los trabajadores que estarán autorizados para entrar y salir en la puerta 1 o en la puerta 2, se transfiere la información capturada a los equipos biométricos instalados para el control de las puertas (figura 17).

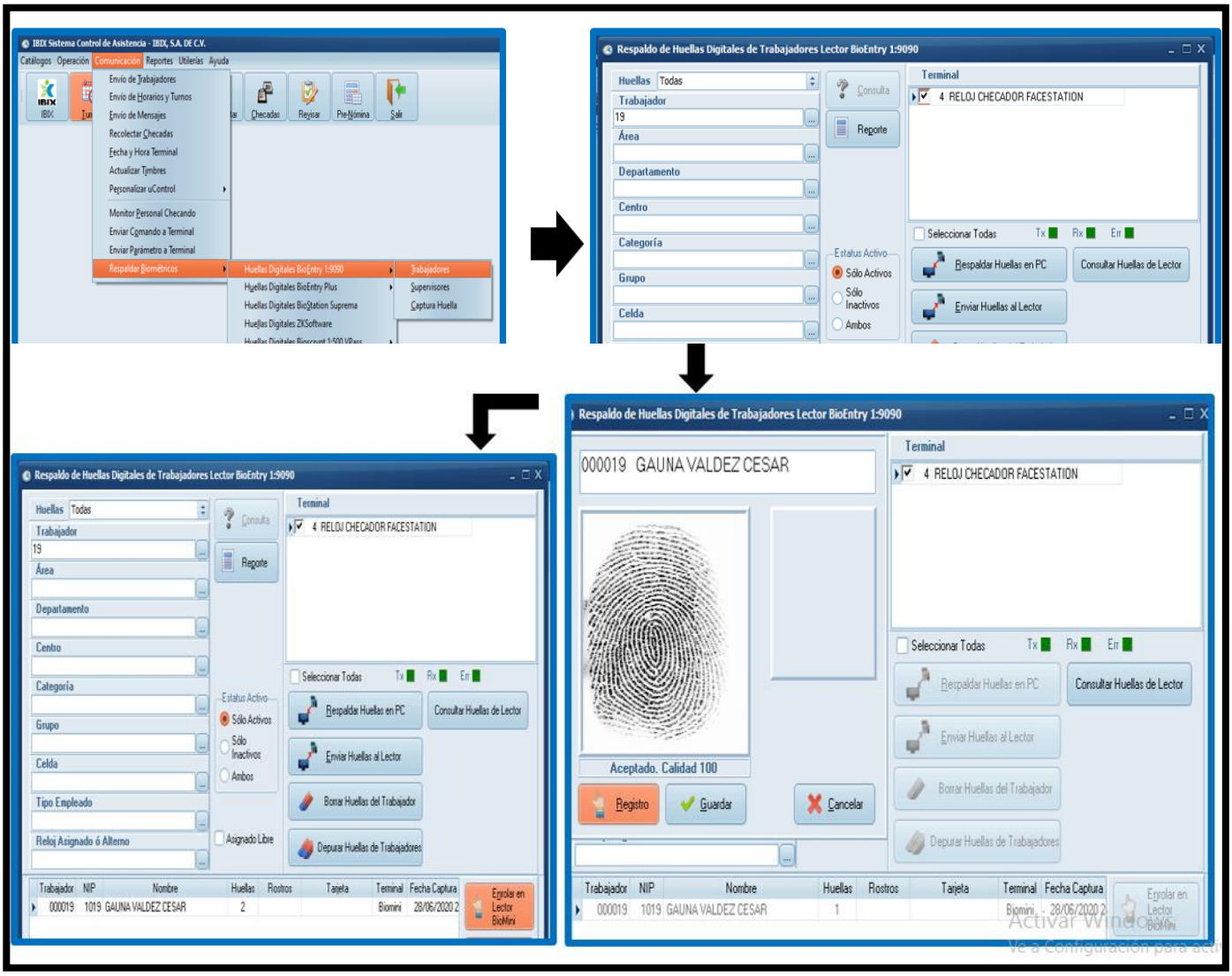


Figura 17. Dar de alta la huella de un trabajador en el sistema IBIX

A continuación, se muestra en la figura 18 la simulación de funcionamiento de un control de acceso de dos puertas.

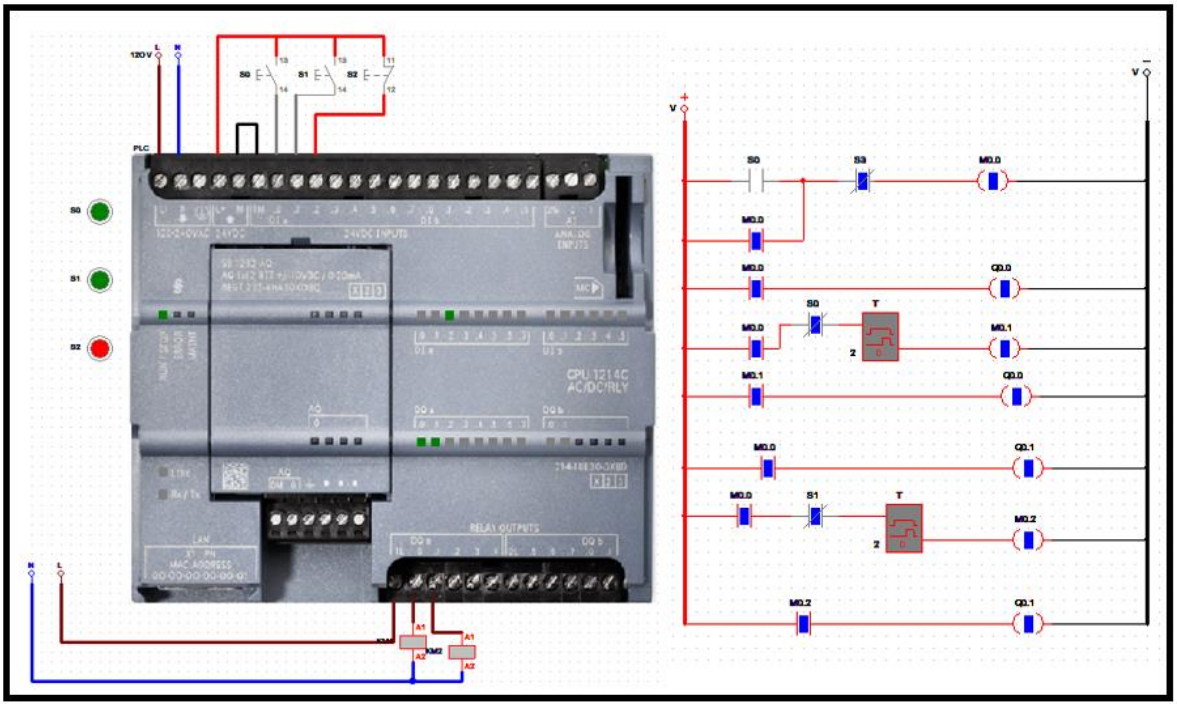


Figura 18. Simulación del funcionamiento de un control de acceso con dos puertas

El funcionamiento del control de acceso inicia en el momento en el que se instala el software en el servidor y se carga la base de datos en los equipos biométricos con la información de los trabajadores: nombre completo, número de trabajador, área, departamento al que pertenece y la huella digital.

En la figura 18 se muestra la simulación de la estructura del diagrama de escalera, con su secuencia lógica de funcionamiento utilizando contactos normalmente abierto, contactos normalmente cerrados, temporizadores y salidas utilizadas como memoria de almacenamiento. De esta manera este diagrama simula a partir de que le trabajador coloca la huella en el lector (S0, S1), este se tarda entre 2 a 3 segundos en detectarla, posteriormente la compara con la huella almacena anteriormente, si estas coinciden permite el acceso, de lo contrario se restringe el paso a través de la puerta, si el acceso es positivo el biométrico manda una señal al Controlador Lógico Programable (I0.0 o I0.1) para habilitar la puerta 1 (Q0.0) o la puerta 2 (Q0.1). Así también cuenta con un botón de emergencia (S2) que se acciona en caso de una situación anormal cuyo funcionamiento es deshabilitar las cerraduras

electromagnéticas para la liberación de las puertas y los usuarios puedan entrar o salir libremente.

El control acceso implementado con puertas es uno de los más comunes en las pequeñas y grandes empresas, debido a que garantiza por un lado la seguridad del trabajador, y por otro lado proporciona múltiples beneficios a las empresas teniendo un mayor control sobre los horarios y actividades desempeñadas en el lugar de trabajo, es importante mencionar que en este campo hay una diversidad de opciones que el cliente puede seleccionar de acuerdo a sus necesidades, es decir se pueden utilizar equipos biométricos con huella digital, tarjeta de proximidad, reconocimiento facial o palma de mano, en el caso de **IBIX, S.A. de C.V.**, es muy frecuente la puesta en marcha con detección de huella digital y tarjeta de proximidad.

2.2. Control de acceso implementado con torniquetes

Tal como se mencionó en el apartado anterior los controles de acceso se pueden implementar ya sea con puertas, torniquetes o barreras vehiculares, en este apartado se hablará sobre la puesta en marcha de un control de acceso con torniquetes, siendo uno de los más usables para empresas industriales. De esta manera **IBIX, S.A de C.V**, comercializa diferentes modelos de torniquetes para responder a las necesidades de cada cliente, a continuación, se muestran los más solicitados (figura 19).

Catrax Fit	Catrax Master	Catrax Clip
		
• Tapa superior con abertura (opcional) para lector de código de barras y tapa de acero inoxidable que facilita la configuración para montar display, teclados, lectores de proximidad o biométricos. • Espacio interno con soporte para montaje de placas de control. • Angulo de abertura de brazos de 81°. • Cuenta con dos electroimanes. • Molinete triple brazo de acero inoxidable. • Extensión de los brazos de 47cm.	• Accionamiento de trabas por medio de electroimanes • La tapa superior posee una combinación de chapa de acero inoxidable y terminación con piezas de plástico inyectado de alto impacto • No hay tornillos aparentes. Para acceder a la parte interna del torniquete es necesario usar una llave de seguridad. • En caso de emergencia, si falta energía, el torniquete funciona libre para los dos sentidos. • Permite la instalación de proximidad o Smart Card en las dos extremidades superiores de la tapa. • Fuente de entrada 90 a 250 VAC y salida 12 VDC/2A.	• Terminación externa de acero de carbono y pintura electrostática. • Angulo fuertemente redondeado para evitar heridas o daños a los usuarios. • Brazo tipo clip de acero inoxidable. • Movimiento mecánico. • Sistema bidireccional con posibilidad de traba. • Sistema con dos sensores ópticos para identificación de sentido de pasaje. • Accionamiento de trabas a través de electroimanes. • Ausencia de tornillos aparentes. • Modelo tipo columna

Figura 19. Modelos de torniquetes

Los torniquetes son dispositivos que cuentan con un sistema de giro bidireccional, ya sea con giros o movimientos horizontales, cuentan con dos electroimanes de 12 VCD, dos sensores ópticos y una tarjeta controladora, los sensores ópticos

suministran señales para accionar las trabas de los dos electroimanes, para realizar el acceso; si se intenta el paso a través del torniquete sin que el usuario presente su huella o tarjeta de proximidad, un electroimán será accionado e impedirá el acceso, el equipo emitirá una señal accionando el pictograma de color rojo en la parte frontal [**IBIX, S.A de C.V, 2013].**

En general este dispositivo se utiliza para llevar a cabo el control de acceso de todo el personal de una empresa pública o privada, autorizando sólo a usuarios que tienen acceso a dicho edificio y restringiendo a personas que no están autorizadas, hay varias formas de permitir el acceso con los biométricos, por ejemplo, con tarjeta de proximidad, lector de huella, reconocimiento facial, entre otros. A continuación, se describirá el proceso de implementación utilizando un equipo biométrico con lector de reconocimiento facial.

Para dicha instalación se recomienda contar con piso firme, además de acondicionar el lugar con las medidas exactas acordes a las del torniquete, una alimentación eléctrica de 120 VCA debidamente protegida y regulada, en caso de que se presente una falla de corriente eléctrica se puedan seguir haciendo uso de los controles de acceso, así también se requiere de nodos de red con RJ45 macho, contar con un servidor disponible y un switch con entradas RJ45 hembra.

En la siguiente tabla (6) se muestra el material que se utiliza para llevar a cabo la instalación en campo.

MATERIAL		CARACTERÍSTICAS
Torniquete Catrax Fit		Accionamiento por electroimanes Señales de confirmación de giro por sensores ópticos. Fuente de voltaje. Tarjeta de control.
Biométrico de reconocimiento Facial		Terminal Biométrica de Reconocimiento Facial Pantalla WVGA Color de 4.3 Pulgadas Touch Screen Capacidad de Usuarios 10,000(1:1), 1,000(1: N) Comunicación en Red TCP/IP
Cable múltiple con calibre de 16 awg (american wire gauge)		Resistente a la humedad 13 Amper Cable de cobre blando con aislación de PVC Temperatura de operación a 80°
Cable de red		Cable de red con RJ45 macho Color azul

Tabla 6. Material para la instalación de un torniquete

Adicional al material mencionado anteriormente se requiere de un taladro, brocas de metal, brocas para concreto, desarmadores, un multímetro, martillo, juego de dados, tornillos de expansión, un flexómetro y un nivelador de burbuja.

Una vez contando con el espacio acondicionado y el material, se procede a realizar la instalación, en primer lugar, se realizan las mediciones pertinentes, se fijan los taquetes de expansión para la colocación del torniquete, preferentemente se tienen que hacer algunas pruebas para corroborar que el dispositivo quede perfectamente colocado en el lugar solicitado, así como algunas pruebas de giro bidireccional, en la figura 20 se muestra la colocación de un torniquete, en un tipo de piso firme.

Figura 20. Torniquete instalado físicamente

Una vez fijado el torniquete, se verifica que haya una fuente de energía para la alimentación de la tarjeta de control y los nodos de red estén instalados correctamente, posteriormente se instala el equipo biométrico en una pared con un brazo movible de izquierda y derecha de una altura de 1.20m en el lugar solicitado por el cliente con su fuente de voltaje de salida de 12 VCD, se conectan las salidas de relevador normalmente abierto y la tierra (NO/GND) del dispositivo biométrico de reconocimiento facial a la entrada digital de la tarjeta controladora del torniquete, de esta manera, se utiliza un solo equipo para la entrada y salida de los trabajadores, como se muestra en la (figura 21).

Figura 21. Torniquete instalado con equipo biométrico de reconocimiento facial

Una vez contando con la colocación del torniquete y la instalación del equipo biométrico, se programa una dirección IP para conectar el dispositivo a la red del cliente, teniendo ya la comunicación y verificando que esta funcione adecuadamente, se procede a la instalación del software en el servidor del cliente, así como la creación y carga de una base de datos que concentra la información de los trabajadores como; número de trabajador, nombre, área o departamento al que pertenece.

Algo que me parece importante mencionar, es que para este tipo de equipo biométrico se tienen que dar de alta los rostros de cada uno de los usuarios con un número de empleado asignado directamente en el dispositivo.

2.2.1. Conexión y funcionamiento del torniquete con el equipo biométrico

Una vez colocado el equipo biométrico con las especificaciones solicitadas, así como el torniquete que dará acceso de entrada y salida de los usuarios, se realiza la conexión eléctrica de 120 VCA para la alimentación del torniquete, dicha conexión debe de estar debidamente protegida, regulada y aterrizada, posteriormente se hacen las conexiones del torniquete al equipo biométrico que van de la entrada de la tarjeta controladora del torniquete PIN2 HBA1,PIN5 HAB2 a la salida del equipo biométrico NO PIN 4, de igual forma se hace la conexión de la salida a tierra que va de la entrada GND del torniquete a la salida del equipo biométrico COM PIN3, de igual forma las salidas del torniquete deben tener una conexión del PIN10 al positivo del solenoide 1 y el PIN9 tiene que ir conectado al GND del solenoide 1, el solenoide 2 positivo va conectado de la salida controladora del torniquete en el PIN11, el negativo del solenoide 2 va conectado en el PIN9 ver figura 22 apartado 1.

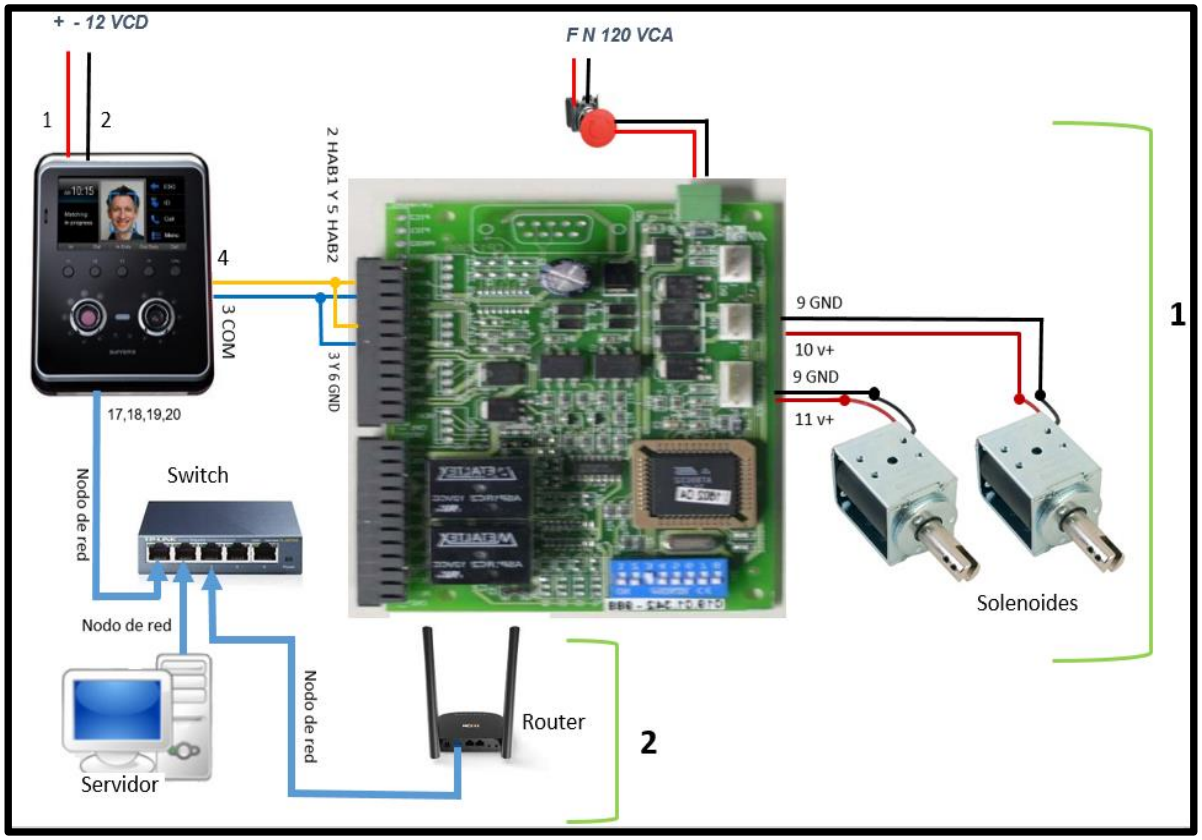


Figura 22. Diagrama eléctrico de conexión de un control de acceso implementado con torniquete.

Teniendo las conexiones mencionadas, el funcionamiento del torniquete con el equipo biométrico inicia cuando el usuario se presenta a una distancia de 40 cm a 50 cm del equipo biométrico, este dispositivo realiza la lectura de reconocimiento facial, después de 2 a 3 segundos, si la lectura es correcta envía una señal de salida a la entrada controladora del torniquete, de esta manera al recibir la señal el torniquete la procesa habilitando los solenoides de entrada o salida con tiempo aproximado de 3 a 5 segundos permitiendo el paso al usuario, en caso de que la recepción del reconocimiento facial sea incorrecta, el equipo biométrico restringe el paso automáticamente.

2.2.2. Conexión y funcionamiento de los nodos de red, servidor y switch con el equipo biométrico.

Para el funcionamiento del control de acceso implementado con torniquete, además de la correcta conexión del torniquete con el equipo biométrico, también es importante el papel que juega los nodos de red, el servidor y el switch tal como podemos observar en la figura 22 apartado 2, los nodos de red tienen una conexión simultánea con el servidor, switch, equipo biométrico y el router, con la finalidad de mantener en red los dispositivos mencionados, así como transferir información del servidor al switch y del switch al equipo biométrico.

Por su parte el switch en conjunto con el router se encargan de mantener una IP fija para el equipo biométrico y el servidor, de esta manera se mantenga en el mismo segmento de red para no perder la comunicación.

El servidor es el equipo encargado del almacenamiento de los datos de los trabajadores, de esta manera para su funcionamiento se tiene que realizar una estructura de base de datos, a la cual posteriormente se le importa la información de los trabajadores tales como: el número de empleado, nombre, área, rostros y turnos, una vez teniendo la base de datos de forma correcta, se carga en el servidor y se envía al equipo biométrico a través de los nodos de red, dicha información se queda almacenada tanto en el servidor como el equipo biométrico. Para complementar los datos se hace el registro de los rostros de los trabajadores directamente en el equipo biométrico.

Además de hacer el envío de la base de datos al equipo biométrico, en el servidor se puede realizar la recolección de las checadas de los usuarios, así como llevar un control de asistencia verificando los retardos, los tiempos extras, las faltas, días de vacaciones, así como los conceptos de ausentismos como; incapacidad por riesgo de trabajo y permisos, todos estos procesos se llevan a cabo con el software Ibix control de acceso.

La implementación de este tipo de control de acceso se resume en la instalación adecuada del torniquete y del equipo biométrico, así como la carga de los datos de los trabajadores y el registro de los mismos, complementario a este procedimiento se llevan a cabo pruebas técnicas de funcionamiento, con la finalidad de verificar de que el sistema esté funcionando correctamente.

Por último, se lleva a cabo la capacitación del personal de recursos humanos que incluye temas cómo; como dar de alta un trabajador en el software, registrar turnos y rotaciones, dar de alta áreas, departamentos, dar alta conceptos de ausentismo y asignación de conceptos a los trabajadores, tipos de reportes de asistencia, así como crear perfiles de usuarios para administrar el sistema.

En la siguiente figura (23) se muestra el proceso de funcionamiento del control de acceso implementado con torniquete.

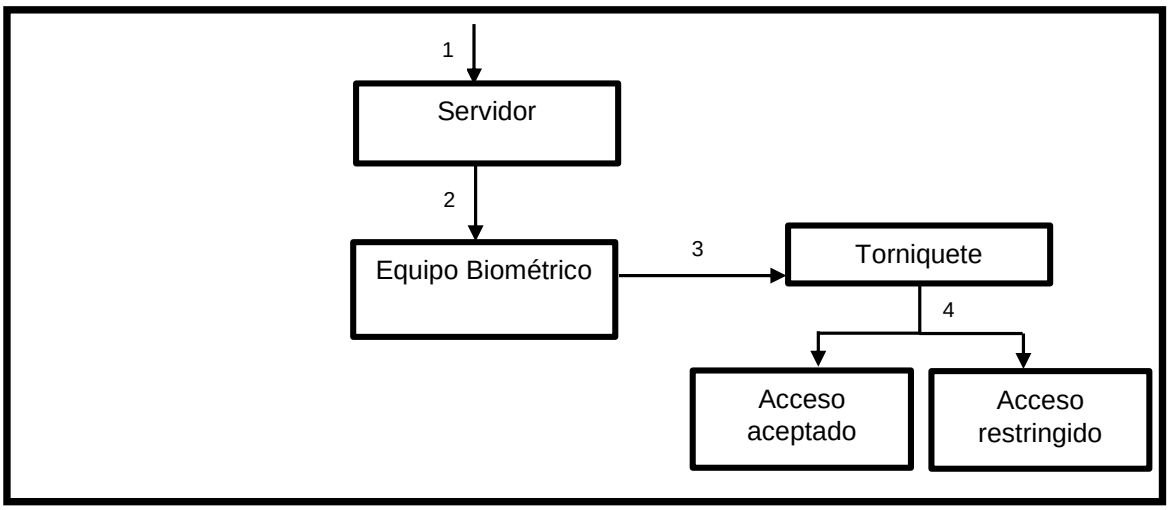


Figura 23. Funcionamiento de un control de acceso implementado con torniquete.

El funcionamiento del control de acceso inicia en el momento en el que se carga la base de datos de los trabajadores al servidor (figura 23, paso 1), posteriormente a través del software se envían el nombre y el número de trabajador al equipo biométrico (figura 23, paso 2), teniendo un almacenamiento interno se puede realizar el registro de los rostros de cada uno de los trabajadores, para este proceso; se identifica el número de trabajador en el biométrico de forma manual, corroborando sus datos para proceder a hacer la captura de los rostros, una vez teniendo todos los datos en el dispositivo el empleado puede acceder a través del torniquete, se tiene que presentar frente al reloj checador a una distancia aproximada de 40 cm a 50 cm, (figura 23, paso 3), el equipo biométrico realiza la lectura del rostro del usuario almacenado en el equipo, realiza la comparación de la información en un tiempo de 2 a 3 segundos, de esta manera envía una señal al torniquete, si la información es correcta el torniquete da acceso, de lo contrario restringe el paso (figura 23, paso 4).

El control de acceso con torniquetes es un sistema en el que se integran diferentes dispositivos para tener un control sobre el personal debido a que es un excelente mecanismo que no solamente funciona para el control de acceso de los usuarios sino también para llevar un control de asistencia, lo que contribuye a llevar un adecuado registro sobre la nómina, es por esto que en la actualidad a adquirido una mayor demanda en el mercado sobre todo para empresas de gran tamaño.

2.3. Control de acceso implementado con Barreras Vehiculares

En los apartados anteriores se ha descrito el proceso de implementación de controles de acceso con puertas y torniquetes, a continuación, se hablará sobre el proceso de implementación un control de acceso efectuado con barreras vehiculares, que también forma parte importante de las actividades que realiza la empresa **IBIX, S.A. de C.V.**

Las barreras vehiculares son dispositivos electrónicos normalmente metálicos para uso en exteriores, pueden ser colocadas tanto en entradas y salidas de estacionamientos, unidades habitacionales o en calles cerradas, los sistemas con

barreras vehiculares están formados por una barra horizontal que se manipula con una palanca para elevarla o descenderla o pueden ser controlados por motores, sensores y herramientas de control, tal es el caso de **IBIX, S.A. de C.V.** que implementa este tipo de control de acceso con equipos biométricos que funcionan con tarjetas de proximidad permitiendo o restringiendo el paso de vehículos, así como el registro de las entradas y salidas de los usuarios.

En **IBIX, S.A. de C.V.**, se comercializan dos modelos de barreras vehiculares, como podemos observar en la figura 24.

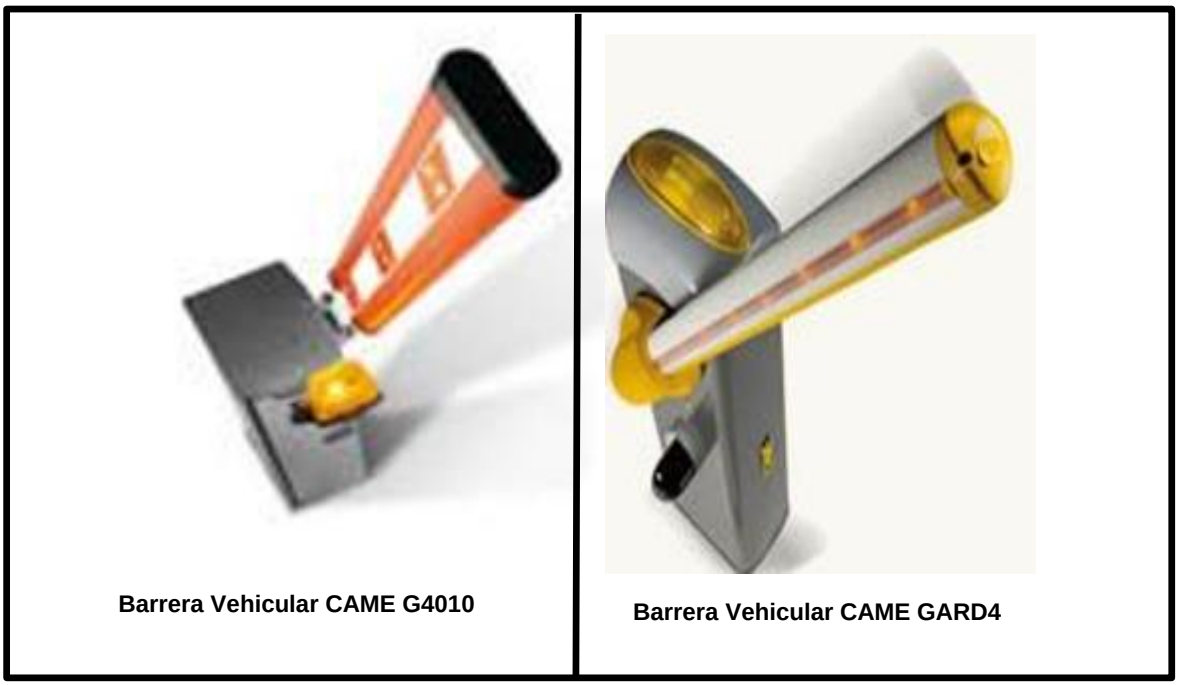


Figura 24. Modelos de barreras vehiculares.

Estos tipos de barreras vehiculares pueden implementarse con equipos biométricos con lectores de tarjeta de proximidad para exteriores. Para llevar a cabo la instalación, se le indica al cliente que debe tener una preparación especial para la fijación de los componentes de la barrera, una base de concreto anclada con la placa de la barrera para la fijación del equipo, un registro sobre el piso 1m*2m*10cm para la instalación del sensor inductivo, de igual forma debe contar con la instalación de 2 tuberías con medidas de ¾” una para la alimentación eléctrica de 120 VCA

que debe estar debidamente protegida y regulada, la otra es para la instalación del nodo de red, además de que debe contar con un servidor disponible y un switch.

En el siguiente Tabla (7) se muestra el material que se utiliza para llevar a cabo la instalación en campo.

MATERIAL		CARACTERÍSTICAS
Barrera Vehicular GRD4		Barrera de 4 metros Alimentación de 120 VCA Motorreductor de 24 VCD Nivel de protección IP54 Potencia de 300 w, 1,3 A. Tarjeta de control.
Biométrico		Terminal Biométrica de lector de tarjeta de proximidad Alimentación de 12 a 24 vcd Comunicación R232 y Rj45
Cable múltiple con calibre de 16 awg (american wire gauge)		Resistente a la humedad 13 Amper Cable de cobre blando con aislación de pvc Temperatura de operación a 80°
Cable de red		Cable de red con RJ45 macho Color azul

Tabla 7. Material para la instalación de una barrera vehicular

Como complemento para la instalación se requiere de herramienta mecánica como: pinzas de corte, pinzas de electricista, pinzas de punta, pinzas de presión, juego de desarmadores, flexómetro, nivelador de burbuja, taladro, brocas de metal y para concreto, arco, martillo y multímetro.

Una vez contando con el espacio acondicionado y el material mecánico, se procede a realizar la instalación; se inicia con el cableado de las tuberías para la alimentación eléctrica de 120 VCA y para el nodo de red que dará comunicación del switch hasta el equipo biométrico, una vez teniendo estas instalaciones se fija la barrera con tuercas y arandelas en la base de concreto solicitada al cliente la cual está anclada con la placa, de igual forma se fija el mástil sobre la base de la barrera, una vez colocada, se instala el biométrico con lector de tarjeta de proximidad en una base de pedestal, dicho dispositivo va conectando a la tarjeta de control de la barrera.

Finalmente se instala el sensor inductivo sobre la superficie a una distancia aproximada de 1 m de la barrera, este debe ir conectando a la tarjeta controladora de la barrera (figura 25).

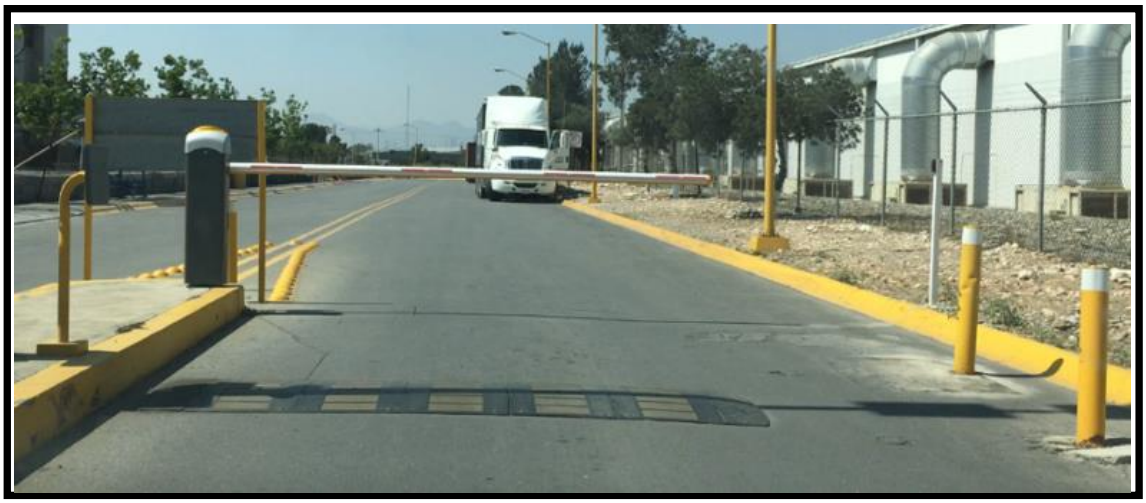


Figura 25. Instalación de la barrera vehicular

Una vez teniendo la instalación de la barrera, el equipo biométrico y del sensor, se lleva a cabo la capacitación al personal de recursos humanos con el objetivo de dar a conocer el funcionamiento del sistema, específicamente se muestra cómo dar de alta un trabajador en el software, cómo dar de alta las tarjetas de proximidad para cada uno de los usuarios y cómo enviar la información de los usuarios al equipo biométrico.

2.3.1 conexión y funcionamiento de la barrera vehicular con el equipo biométrico

Para el funcionamiento del control de acceso implementado con barrera vehicular, una vez teniendo la instalación física de la barrera y del equipo biométrico, se procede hacer la conexión eléctrica como podemos observar en la figura 26 apartado 1, se realizan dos conexiones que van de la salida PIN4 del equipo biométrico a la entrada de la tarjeta controladora de la barrera vehicular PIN3 y de la salida del equipo biométrico PIN5 COM que a la entrada PIN2 de la tarjeta controladora de la barrera Vehicular y también va conectado en paralelo un botón inalámbrico del PIN4 – PIN3 de tarjeta controladora de la barrera vehicular y PIN5 del botón inalámbrico al PIN 2 de la tarjeta controladora de la barrera vehicular.

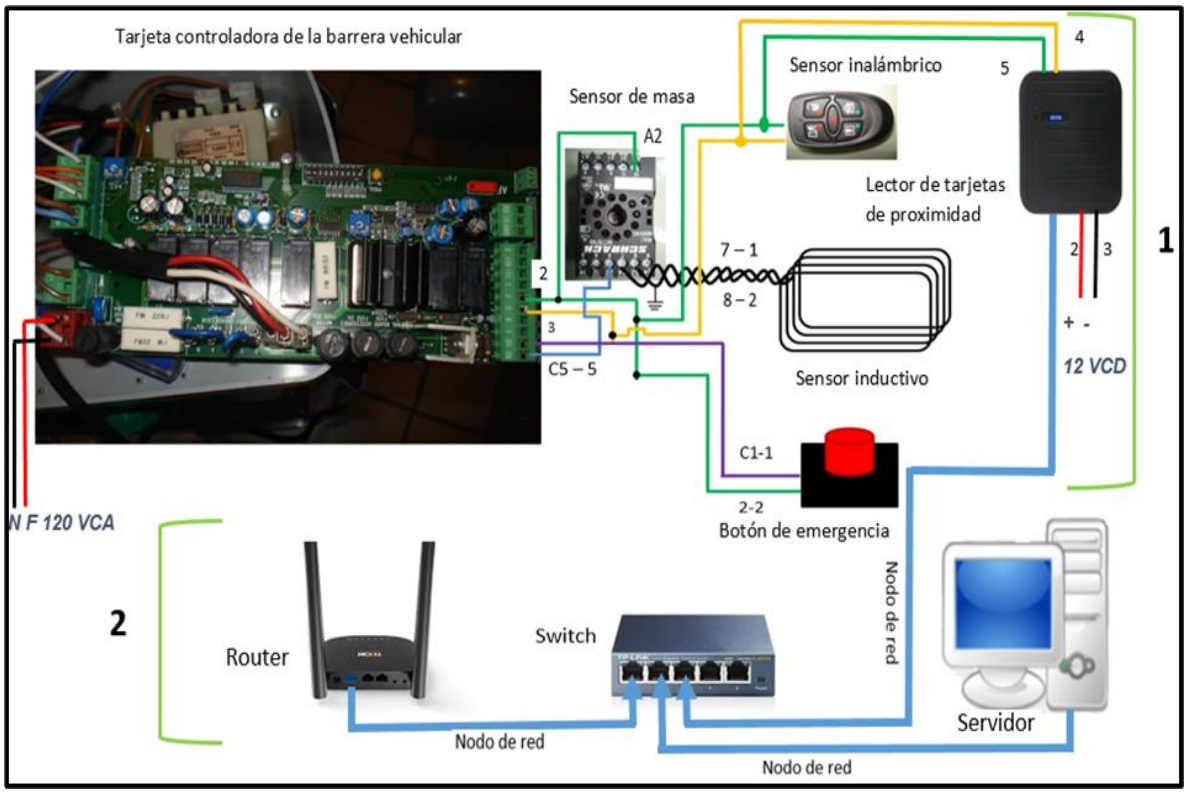


Figura 26. Diagrama eléctrico de conexión de un control de acceso implementado con barrera vehicular

Además de las conexiones mencionadas anteriormente, también se realiza una conexión adicional que es el sensor inductivo que se conecta al sensor de masa en el PIN7- PIN1 del sensor inductivo que es alimentado con 24 VCD, sensor de masa del PIN8 – PIN2 del sensor inductivo van que va aterrizado a tierra, de igual forma se realiza la conexión que va del sensor de masa PIN A2 a la entrada de la tarjeta controladora de la barrera PIN2, además para cerrar el circuito se realiza la conexión del sensor de masa PIN5 a la entrada de la tarjeta controladora de la barrera PIN CN5, por último, se realiza la conexión del botón de emergencia que va al PIN2 al PIN2 de la tarjeta controladora de la barrera vehicular y PIN1 del botón de emergencia va al PIN C1 de la tarjeta controladora de la barrera vehicular.

Una vez teniendo las conexiones necesarias el funcionamiento de la barrera vehicular con el equipo biométrico inicia cuando el usuario presenta la tarjeta de proximidad al equipo biométrico a una distancia de 20 cm a 30 cm, el equipo biométrico realiza la lectura en un tiempo aproximado de 2 a 3 segundos, posteriormente manda una señal a la tarjeta controladora de la barrera vehicular accionando el motorreductor lo que permite que el mástil se eleve a 90°, para el descenso del mástil, una vez que el vehicula pasa sobre el sensor inductivo, este genera un campo magnético hacia el sensor de masa, siendo el encargo de convertir y enviar la señal a la tarjeta controladora de la barrera vehicular para que descienda el mástil.

Cuando el botón de emergencia es activado, este envía una señal a la tarjeta controladora de la barrera vehicular, esta a su vez eleva el mástil sin dejar descender de manera que permite el libre paso de los vehículos.

2.3.2. Conexión y funcionamiento de los nodos de red, switch y servidor con el equipo biométrico

Para el funcionamiento del control de acceso implementado con barrera vehicular, además de las conexiones de la barrera vehicular con el equipo biométrico y las conexiones adicionales que se realizan con el sensor e masa y el botón de emergencia, también es importante la conexión de los nodos de red, el servidor y el switch con el equipo biométrico, tal como podemos observar en la figura 26

apartado 2, los nodos de red tienen una conexión simultánea con el servidor, el switch, el equipo biométrico y el router, de manera que estos dispositivos se mantengan en red para transferir información del servidor al switch y del switch al equipo biométrico.

El switch en conjunto con el router se encargan de mantener una IP fija para el equipo biométrico y el servidor, de manera que se mantengan en el mismo segmento de red para no perder la comunicación.

El servidor es el equipo encargado del almacenamiento de los datos de los trabajadores, para su funcionamiento se tiene que seguir un proceso similar al del control de acceso implementado con puerta y con torniquete, de esta manera realiza una estructura de base de datos, con información de los usuarios tales como: el número de empleado, nombre, área y número de tarjeta , una vez teniendo la base de datos de forma correcta, se carga en el servidor y se envía al equipo biométrico a través de los nodos de red, dicha información se queda almacenada tanto en el servidor como el equipo biométrico.

De igual forma en el servidor se puede realizar la recolección de las checadas de los usuarios, así como llevar un control de asistencia verificando los retardos, los tiempos extras, las faltas, días de vacaciones, así como los conceptos de ausentismos como; incapacidad por riesgo de trabajo y permisos, todos estos procesos se llevan a cabo con el software Ibix control de acceso.

En la figura 27 se muestra el proceso de funcionamiento del control de acceso implementado con barrera vehicular.

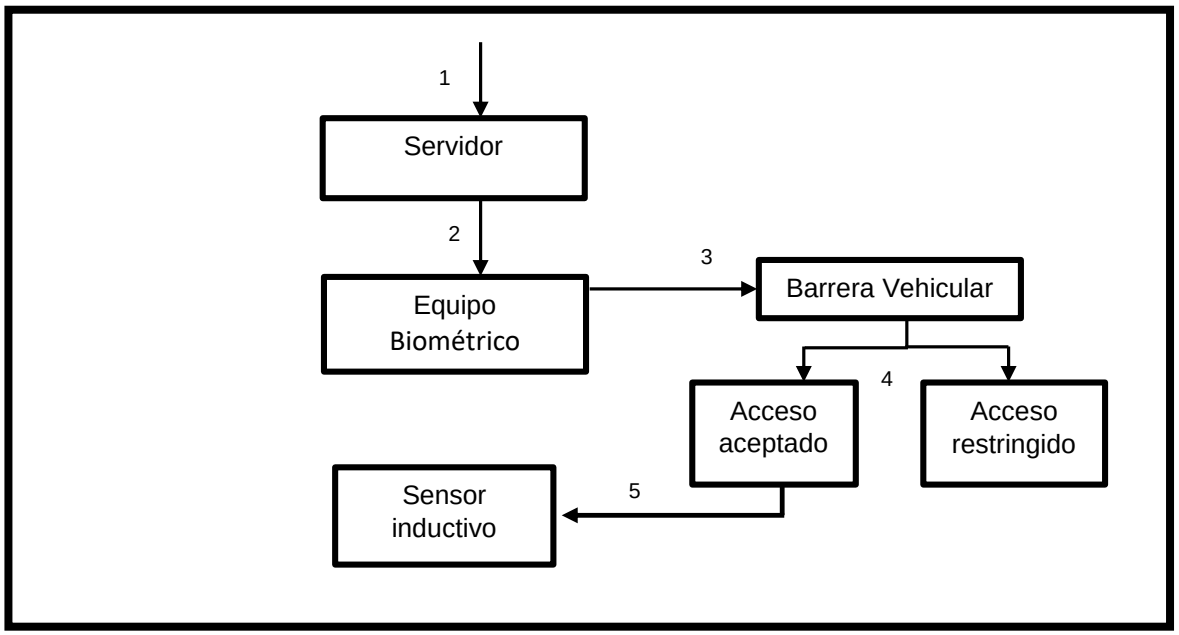


Figura 27. Funcionamiento de un control de acceso implementado con barrera vehicular.

En general el funcionamiento de este tipo de control de acceso inicia cuando se realiza la carga la base de datos de los trabajadores al servidor (figura 27, paso1), a través del software se envía la base de datos al equipo biométrico (figura 27, paso 2), teniendo un almacenamiento interno de los datos de los trabajadores en el equipo biométrico, los usuarios ya pueden acceder a través de la barrera vehicular, se tiene que presentar la tarjeta de proximidad frente al biométrico a una distancia aproximada de 30 cm, el equipo biométrico realiza la lectura de la tarjeta del usuario, en un lapso de 2 a 3 segundos realiza la comparación de la información enviando una señal digital a la tarjeta controladora de la barrera (figura 27, paso 3), si el usuario se encuentra fuera de horario laboral o no está registrado se restringe el paso, de lo contrario si la información es correcta la barrera da acceso elevando el mástil a 45 grados (figura 27, paso 4), el mástil funciona con un motorreductor que a su vez es manipulado por la tarjeta controladora.

Cuando la barrera da acceso, se genera un campo magnético que se produce entre el sensor inductivo con la placa metálica del vehículo, una vez que el vehículo pasa por el sensor inductivo, este envía una señal analógica a la tarjeta controladora, la tarjeta controladora convierte esta señal en una señal digital enviándola al

motorreductor, quien al detectarla hace descender el mástil de la barrera a su posición original (figura 27, paso 5), este proceso dura entre 2 a 4 segundos dependiendo de la velocidad del vehículo.

En general los controles de acceso son una excelente opción para mantener un control riguroso sobre el acceso de los usuarios, teniendo la posibilidad de restringir el acceso a aquellos que no estén autorizados, de esta manera se garantiza al cliente un estricto control sobre el personal y las actividades que desempeñan. Por su parte, el control de acceso vehicular te permite tener un registro de los automóviles tanto de los residentes como de los visitantes, además si se implementa con un sistema de control de asistencia o con un lector de huella digital, la empresa puede llevar el control exacto de todas las horas trabajadas y así medir la productividad de sus empleados.

CAPÍTULO 3. CONOCIMIENTOS PUESTOS EN MARCHA EN LA EMPRESA IBIX S.A DE C.V.

3.1. Necesidades actuales y fallas típicas de los sistemas biométricos

Se tiene registro teórico que la implementación de los equipos biométricos es una práctica que ha estado en uso desde el año de 1858, siendo utilizado como un estampando de huella de la palma de la mano al reverso de los contratos, como una forma de diferenciar a los trabajadores de las empresas de otras personas que podrían exigir el pago de sus actividades [Díaz, 2013], durante ese mismo periodo (XIX) la biometría fue utilizada para fines legales básicamente en investigaciones criminales, lo que se pretendía era identificar las características físicas de los criminales, de esta manera se dio paso a una gran variedad datos obtenidos de los registros que se realizaban, simultaneo a este proceso se desarrolló la identificación de huellas digitales que pronto se convirtió en una metodología internacional utilizada principalmente por las fuerzas policiales.

Con el paso de los años hubo un gran interés por la posibilidad de usar la electrónica y los microprocesadores para poder automatizar la verificación de identidad, ya no solo en el ámbito policial sino también en el ámbito comercial, durante esta época se iniciaron varios proyectos con la finalidad de mejorar dichos sistemas dando como resultado el lector de geometría de mano que se introdujo al mercado convirtiéndose en una de los pilares de la biometría [Díaz, 2013].

En años recientes la biometría ha tenido mejorías constantes hasta convertirse en equipos confiables que facilitan su utilidad, recientemente se han implementado nuevas técnicas biométricas como el escaneo de iris y reconocimiento facial por lo que ha sido de fácil acceso para las diferentes industrias a nivel mundial [Sánchez, 2013].

En la actualidad contamos con una variedad de equipos capaces de identificar a las personas a partir de los registros de una parte de su cuerpo como las manos, la retina, el iris, los dedos, huellas dactilares, la voz o la firma, incluso se plantea la

posibilidad de crear un sistema basado en el AND, de esta manera los sistemas biométricos se han convertido en una necesidad evidente para determinados ámbitos de la sociedad tanto en el área comercial, como en el área de salud y judicial, ya sea al nivel público o privado, siendo sistemas cada vez más completos para la identificación de personas, de esta manera se pasó del registro de las características biométricas como nombre, fecha de nacimiento, sexo, descripción física, entre otros, a la inclusión de características como el rostro, las huellas dactilares, la vos , el iris y la palma de la mano [Etchart, s.f.].

Una de las limitaciones para el uso de los sistemas biométricos a través de los años han sido los costos elevados que representa la puesta en marcha de dichos sistemas, por lo que se han ajustado los costos a las necesidades de los diferentes sectores, dando como resultado una gran variedad de equipos capaces de identificar determinadas características de las personas, contribuyendo a la prevención de situaciones que podrían causar efectos negativos a las empresas logrando un control de acceso y el desplazamiento de los individuos en el interior de las empresas, controlar tiempos desperdiciados y acceso restringidos, de esta manera se considera que los sistemas biométricos son un medio rápido y seguro para validar diversas operaciones y control de acceso [Etchart, s.f.].

Hoy en día la utilización de los sistemas biométricos forma parte importante en todos los sectores, considerado uno de los mejores y más completos sistemas de seguridad para el acceso a instalaciones, además de que representa bajos costos de mantenimiento, así también es un sistema difícil de suplantar o falsificar, no requiriendo dispositivos extras para su funcionamiento, sin embargo, se han presentado algunas fallas típicas a las cuales los usuarios se han enfrentado, algunas tienen que ver directamente **con el equipo biométrico** tales como; que el equipo biométrico no detecten la huella dactilar, el rostro o la geometría de mano registrada anteriormente lo que imposibilita el acceso adecuando de las personas.

Algunas otras fallas tienen que ver directamente con **la variación de voltaje**, usualmente se reportan casos de equipos que han quedado bloqueados o desbloqueados totalmente, es decir, no permite el acceso de las personas, aunque

detecte correctamente la huella digital o por lo contrario se queda liberado el equipo permitiendo el libre acceso, otra falla relacionada con la electrónica es que le equipo biométrico se apague completamente o se reinicie constantemente.

Otras fallas típicas presentadas tienen que ver con la **conexión de internet**, checador – servidor, algunos usuarios han reportado la perdida de información de los registros realizados, además de reportar que el equipo biométrico constantemente es muy lento, otro error que comúnmente se presenta y que tiene que ver con la conexión de red es que no se pueden realizar de nuevos registros de nuevos usuarios del servidor – checador. Otra falla que se ha detectado tiene que ver la **manipulación de los datos** registrados por parte del administrador, traduciéndose en constantes errores en la base de datos.

La implementación de los sistemas biométricos en la actualidad ha sido de gran utilidad ajustándose a la nuevas necesidades de los usuarios y respondiendo a mejorar la productividad en los determinados sectores, sin embargo hay probabilidades de presentar algunas fallas específicas, es importante mencionar que dichas fallas varían dependiendo de las características de los usuarios y las actividades que desempeñan, **IBIX S.A. de C.V.** cuenta con un equipo capacitado para resolver las diferentes fallas que se presenta así como orientar al cliente para prevenir futuras incidencias, en el siguiente apartado se explicarán las posibles soluciones para resolver las fallas típicas mencionadas.

3.2. Relación de conocimientos útiles en la detección y reparación de fallas

Con la implementación de los sistemas biométricos en **IBIX S.A. DE C.V.**, he puesto en marcha conocimientos adquiridos durante mi formación académica en la Universidad Autónoma de la Ciudad de México, sin embargo, dichos conocimientos también me han sido de gran utilidad para la detección y reparación de fallas, en general desde mi experiencia laboral me he enfrentado a una diversidad de fallas y dudas con respecto al funcionamiento y mantenimiento de los biométricos, en esta ocasión hago referencia a las más comunes, las cuales dividí en cuatro grupos, tal y como podemos ver en la tabla 8, en primer lugar menciono las fallas que tienen

que ver directamente con el equipo biométrico, en segundo lugar las que tiene que ver con la variación de voltaje, en tercer lugar las fallas que tiene que ver con la conexión a internet y por último las que tienen que ver con la manipulación de la base de datos.

FALLAS TÍPICAS DE LOS SISTEMAS BIOMÉTRICOS *Control de acceso implementado con puertas, torniquetes y barreras vehiculares*	
FALLA TÍPICA	**POSIBLES CAUSAS**
1. EQUIPO BIOMÉTRICO El equipo biométrico no detecta, la huella digital, palma de la mano, rostro, tarjeta de proximidad o código de barras.	- Que la huella o la palma de la mano del trabajador este deteriorada. - Que en el rostro tenga algún objeto que obstruya su detección (barba, lentes, cabello.) - Que la tarjeta de proximidad no esté dada de alta en el biométrico o esté dañada. - Que el código de barras esté deteriorado.
2. VARIACIÓN DE VOLTAJE El equipo se quedó bloqueado o liberado completamente. El equipo se apagó por completo.	-Posible sobrecalentamiento en la tarjeta de control. - Que la tarjeta de control esté quemada.
3. CONEXIÓN A INTERNET El equipo es muy lento. No se pueden realizar nuevos registros de nuevos usuarios. Perdida de información de los registros.	**-**No hay una conexión de red entre biométrico/servidor. -Falla directamente en el nodo de red. -Fallas directas con el servicio de internet**.**
4. MANIPULACIÓN DE LA BASE DE DATOS Errores en la base de datos; no se puede abrir el software. Posible introducción de datos inadecuados. IP duplicado.	-Que el administrador agregue datos extras. -Que el administrador agregue datos incorrectos. -Mal uso de la base de datos.

Tabla 8. Fallas típicas de los sistemas biométricos

Las fallas que tienen que ver **directamente con el equipo biométrico,** en general es cuando el usuario reporta que el equipo no detecta la huella digital, la palma de la mano, el rosto o la tarjeta de proximidad en el caso de las barreras vehiculares o en algunos casos el código de barras, para dar solución a estos problemas lo que se hace en un primer momento es verificar que el equipo se encuentre en buen estado físico, así como comprobar que la palma de la mano o huella del usuario no

esté deteriorada, si es el caso, se indica que se tiene que dar de alta nuevamente al usuario con otra huella o en el caso de la palma de la mano se tiene que dar de alta nuevamente, si esto no diera solución a su problema podría ser opción asignarle una tarjeta de proximidad, siempre y cuando el equipo tenga la función de realizar lectura de tarjetas de proximidad.

En el caso de que el equipo no lea la tarjeta de proximidad o el código de barras, se verifica si estos se encuentran en buen estado físico, además de asegurarse que estén dados de alta en la base de datos correctamente, de lo contrario se tiene que repetir el procedimiento de registro de usuario, en general con respecto a fallas que tienen que ver con el biométrico directamente, estas son las posibles soluciones que se les pueden dar, sin embargo se han presentado casos en los que a pesar de realizar las posibles soluciones mencionados anteriormente el equipo continua presentando estas fallas, para esto se puede tomar la opción de resetear el equipo a modo fabrica con la finalidad de restablecer los parámetros y de esta manera volver realizar el registro de usuarios, si aun así las incidencias persisten, se procede a retirar el equipo para enviar a garantía.

En ocasiones los usuarios han reportado fallas como que el equipo se apagó por completo o que se quedó bloqueado no dando acceso a las personas, a pesar de que lea adecuadamente la huella, la palma de la mano, la tarjeta de proximidad, el código de barras o el rostro, o por el contrario se quedó liberado dejando acceder libremente a los usuarios, estas fallas típicas que tienen que ver con la **variación de voltaje**, pueden ser a causa de un posible calentamiento en la tarjeta de control o incluso que se haya quemado por una inadecuada alimentación eléctrica.

Para dar solución a estas fallas, se procede a identificar el voltaje en distintos puntos de la tarjeta de control, en el caso del control de acceso implementado con torniquetes se tiene que identificar que el voltaje de corriente alterna suministre los 120 VCA a la tarjeta, esto se realiza con un multímetro colocándolo en la entrada de la alimentación (figura 28,1), de esta manera si la alimentación es incorrecta en la tarjeta de control, posiblemente es una falla que procede directamente de la instalación eléctrica, por lo que se tiene que remplazar el contacto eléctrico o la

pastilla termomagnética del circuito derivado, en el caso de que el voltaje sea correcto en la entrada de la tarjeta, se tiene que revisar la medición de voltaje en los sensores optoacopladores que normalmente deben entregar 12 VCD (figura 28, 2), si alimentación es adecuada en esta parte, se realiza una revisión de voltaje en las salidas de los solenoides que normalmente dan un voltaje de 12VCD (figura 28, 3).

Las salidas de los solenoides son la última parte en la que se verifica el voltaje, para poder identificar si la tarjeta está funcionando adecuadamente, en este caso si el voltaje es incorrecto significa que la tarjeta está totalmente dañada y se tiene que remplazar por una nueva, si en esta parte el voltaje es correcto (12 VCD), se concluye que la falla ya no tiene que ver con la variación del voltaje sino con el mecanismo del funcionamiento del torniquete.

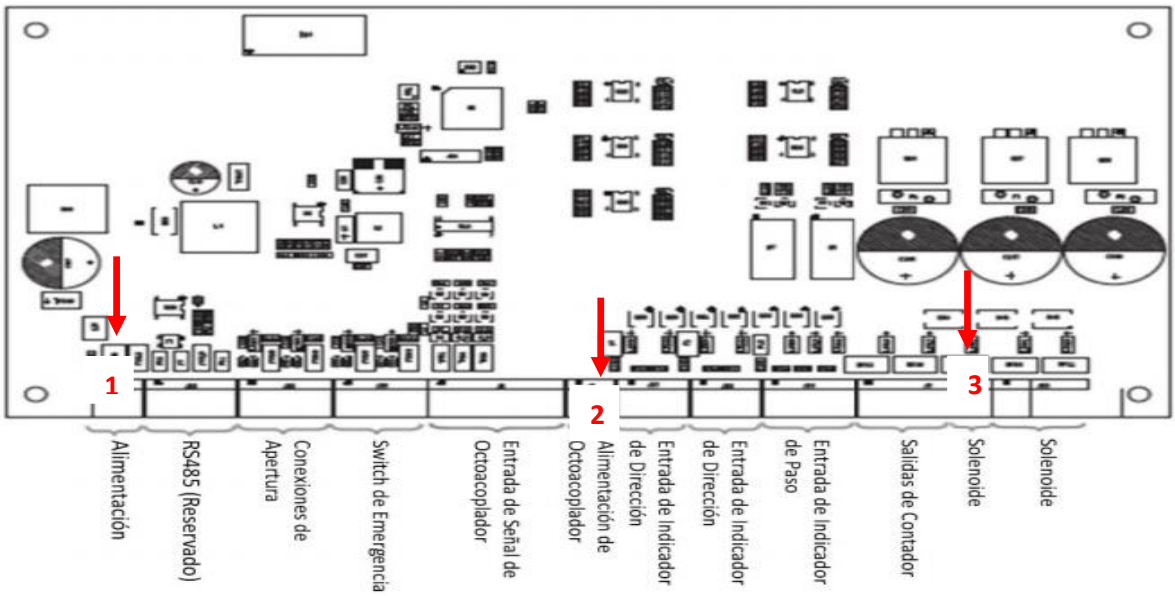


Figura 28. Tarjeta de control de torniquete

Para la identificación y la solución de estas fallas típicas, se pusieron en práctica los conocimientos adquiridos en algunas de las materias cursadas en el siclo superior, por ejemplo, instalaciones eléctricas, electrotecnia y electrónica aplicada, en las cuales se revisaron temas como: identificación componentes eléctricos y electrónicos, identificación de polaridad positiva y negativa, conexiones eléctricas, lectura de diagramas.

Además de las fallas típicas identificadas en la implementación de control de acceso con torniquetes, también para el caso de las barreras vehiculares se han reportado fallas que tienen que ver con la variación de voltaje, para ello en un primer momento se tiene que identificar que el voltaje de corriente alterna que suministra la tarjeta principal sea de 120 VCA, esto se realiza con un multímetro colocándolo en la entrada de la alimentación (figura 29,1), de esta manera si la alimentación es incorrecta es una falla que procede directamente de la instalación eléctrica, por lo que se tiene que remplazar el contacto eléctrico o la pastilla termomagnética del circuito derivado, en el caso de que el voltaje sea correcto se tiene que revisar la medición de voltaje en el fusible de línea (figura 29, 2), si se detecta que no está realizando el paso de la corriente es necesario remplazarlo por una pieza igual con el mismo voltaje.

Si las fallas persisten a pesar de haber realizado las adecuaciones en la entrada de la alimentación y el fusible de línea, se procede a realizar una revisión en el fusible del motorreductor (figura 29, 3) que debe estar alimentado con 24 VCD si el voltaje no es el adecuado se verifica que el fusible central esté funcionando adecuadamente (figura 29,4), este procedimiento se realiza revisando la continuidad con ayuda del multímetro, si se encuentran dañados será necesario cambiarlos con los mismos parámetros para que funcione correctamente.

También se debe realizar una revisión a los capacitores, resistencias, diodos y contactores, tienen que estar en buen estado y funcionando correctamente, de lo contrario estos componentes tienen que cambiarse (figura 29, 5), si aun así la tarjeta sigue sin funcionar será necesario remplazarla por una nueva con las mismas características.

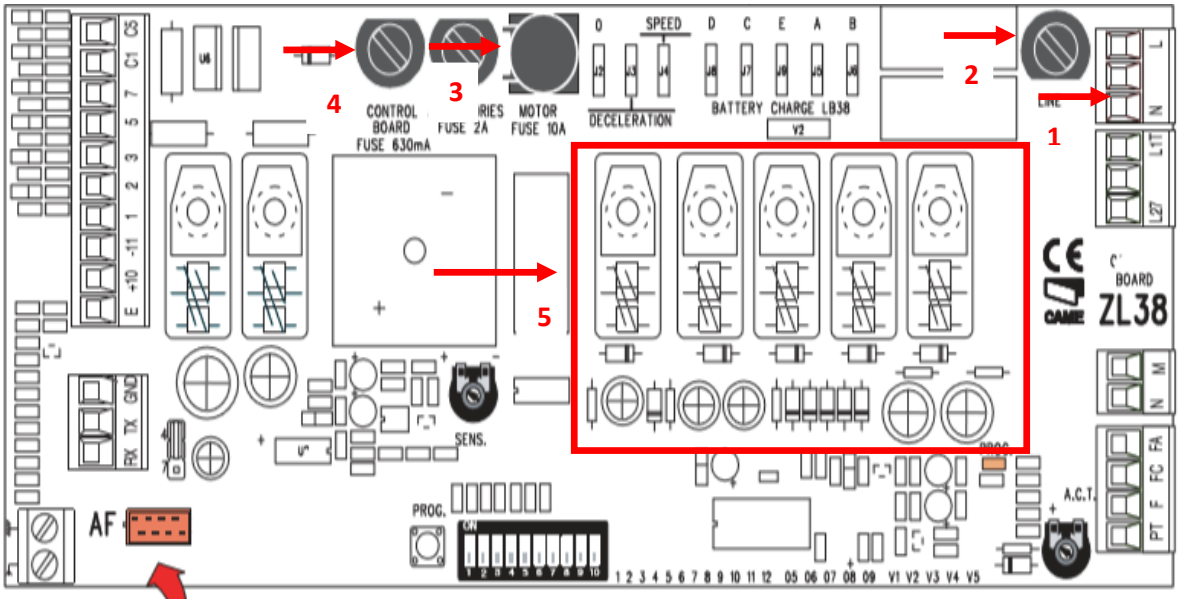


Figura 29. Tarjeta de control de la barrera vehicular

Los conocimientos adquiridos a lo largo de mi formación académica, me han sido de gran utilidad para la identificación de las fallas típicas en los controles de acceso, de esta manera he puesto en marcha algunos de ellos obtenidos en la materia electrónica de potencia, circuitos integrados analógicos, microprocesadores y microcontroladores, dispositivos electrónicos y electrónica digital en los cuales se revisaron temas como; identificación circuitos electrónicos, lectura de diagrama electrónico, lectura de los parámetros de los componentes electrónicos, utilización de las herramientas (Multímetro, soldar componentes electrónicos), tal es el caso de las fallas que presentan las tarjetas de control.

Así también se han presentado fallas relacionadas con **la conexión a internet,** en ocasiones nuestros clientes han reportado perdida de información de los registros, que el equipo es muy lento o que no pueden dar de alta nuevos usuarios ya que el biométrico no lo permite, las causas de estos problemas pueden ser principalmente que no haya una conexión de internet entre el equipo biométrico y el servidor o que las fallas sean directas del servicio de internet del usuario.

Para recuperar la información de los registros de los usuarios que se perdió por falta de red, se le indica al cliente que tiene que realizar la descarga de la información de forma manual directamente en el equipo biométrico con una memoria USB, una vez realizado el proceso se transfiere la información directamente a la base de datos del software del control de asistencia para unificar la información de los días anteriores que no pudieron descargarse, una vez realizado el respaldo de la información se indica que se tiene que borrar todos los registros en el equipo biométrico para que funcione correctamente, debido a que por la falta de conexión de red los datos se quedan almacenados localmente en el equipo.

En caso de que el usuario siga reportando la perdida de información, se procede realizar una revisión directa a la instalación de red, por lo que se le indica que se tiene que cambiar de nodo de red o el cableado, así como verificar que el modem no esté dañado o si es así será necesario realizar el cambio del dispositivo.

Es muy común encontrase con fallas que ya no dependen en su totalidad de la instalación, ni directamente con el funcionamiento del equipo biométrico, más bien tiene que ver con la **manipulación de datos** por parte del administrador, puede ser que haya agregado datos extra que causen que el funcionamiento se vea alterado, para solucionar esta falla que es muy común se realiza una revisión de su base de datos en donde se verifica que los datos sean correctos.

Cuando el administrador inserta mal la información o caracteres que no reconozca la base de datos, en el momento que se desea ingresar al sistema arroja un error, cuando sucede esta incidencia se le pide una copia de su base de datos al cliente para analizarla, una vez encontrando el error ya sea en el número de trabajador, en el área, departamento o una mala captura de la huella, se corrige la incidencia y se devuelve la copia de la base de datos para que sea instalada nuevamente, de manera que funcione correctamente.

En general las fallas de los sistemas biométricos varían dependiendo de su utilización y las condiciones físicas en las que se encuentren instalados (tabla 8), sin embargo, su funcionamiento óptimo también depende de los servicios que brinda **IBIX, S.A de C,V** para prevenir las fallas típicas mencionadas anteriormente, de esta

manera en el momento en el que el cliente adquiere un equipo biométrico también tiene la opción de adquirir una póliza de servicio con la que podrá recibir soporte técnico ya sea de forma remota o presencial; de forma remota se brinda servicio para la prevención de fallas que tiene que ver directamente con la manipulación de datos o la conexión a internet, de manera presencial se brinda un mantenimiento preventivo interno de los equipos biométricos cada 6 meses, que va desde la revisión de las condiciones del cableado de red y energía eléctrica y la limpieza de los equipos, asegurando el funcionamiento óptimo del dispositivo, además de un mayor tiempo de vida útil.

En general para prevenir fallas por variación de voltaje, es necesario que el cliente cuente con una instalación eléctrica con un circuito derivado independiente solo para los equipos de controles de acceso, así también las salidas de voltaje deben estar debidamente protegidas y aterrizadas en un sistema de alimentación ininterrumpido (SAI).

Para prevenir las fallas que tienen que ver con la conexión de internet, se indica al usuario que los nodos de red RJ45 macho, los 8 pines que posee deben de estar bien conectados, en ambos extremos del cable deben tener la misma distribución, debido a que ahí se conecta el equipo biométrico hacia al conmutador y no deben de sobre pasar de los 100 metros de trayectoria.

En el caso de las la fallas que tienen que ver con la manipulación de datos, es necesario que le administrador tenga conocimientos de la estructura de la base de datos de dicho sistema y antes de realizar algún cambio será necesario realizar un respaldo de toda la base de datos por cualquier incidencia que surja por mal manejo, de esta manera si hay alguna falla sólo se estaría restableciendo la copia de la base en el equipo.

Para que el funcionamiento de los sistemas biométricos sea correcto, es importante brindar un servicio integral que incluya soporte de manera remota pero también en campo, ya que de esta manera se asegura un mayor tiempo de vida útil de los equipos.

3.3 Relación de conocimientos útiles en el diseño de sistemas

Con mi experiencia laboral en **IBIX S.A. DE C.V.,** se me ha dado la oportunidad de poner en práctica los conocimientos obtenidos durante mi carrera, sin embargo, considero que dichos conocimientos se pueden utilizar en la implementación de nuevos sistemas y proyectos, por ejemplo, los PLC tienen una infinidad de funciones para el control de procesos pudiendo trabajar en conjunto con los sistemas biométricos, de esta manera habría la posibilidad de implementarse en conjunto conformando un sistema que se pueda utilizar para mover un brazo robótico, poniéndolo en marcha en alguna manufactura para mover piezas de un lado a otro y no tan sólo para el control de asistencia. Además de controlar el desplazamiento de las piezas de un lado a otro, el biométrico permitiría registrar quien opera en determinados rangos de tiempo, asegurando una mayor productividad en las manufacturas.

Otro ejemplo que me permitiría poner en práctica mis conocimientos, sería en la implementación del control de velocidad del montacargas, la idea es que se haga una conexión del biométrico con la tarjeta electrónica del montacargas de manera que se pueda encender el vehículo con una tarjeta de proximidad, así si el trabajador está fuera de turno se le impedirá su uso.

Otro sistema en el cual podría poner en práctica mis conocimientos es en el control de acceso a través de elevadores, es decir, implementar un sistema que permita restringir la entrada a ciertos pisos de un edificio, buscando la manera de que al ingresar al elevador te permita ingresar únicamente al piso solicitado, evitando el libre acceso a los demás pisos.

En general los conocimientos adquiridos durante mi carrera, así como los que he adquirido en **IBIX S.A DE C.V.,** me han permitido abrir un panorama sobre las diferentes áreas en las cuales me puedo desempeñar, pudiendo aportar a nuevos proyectos de investigación y de puesta en marcha de diferentes dispositivos.

CONCLUSIONES

La elaboración de este reporte contribuyó a visualizar la importancia que tiene poner en marcha los conocimientos adquiridos durante mi formación profesional, además de que me permitió identificar las diferentes áreas en las cuales puedo desempeñarme, de esta manera considero que **IBIX S.A de C.V** , es una empresa sólida que aporta soluciones para el control adecuado de acceso y de asistencia, y con el paso del tiempo ha ido acoplándose a las nuevas necesidades del mercado iniciando como una empresa que manejaba únicamente tecnologías de la información hasta llegar al desarrollo de su propio hardware y software con la fabricación de sus propios relojes checadores digitales.

Desde mi experiencia profesional considero que **IBIX S.A de C.V**, es una excelente oportunidad para poder adquirir nuevos conocimientos, pero para también para poner en marcha las habilidades adquiridas en el ámbito académico, debido a que cuenta con una gran cantidad de equipos biométricos de gama baja, media y alta, los cuales se pueden implementar de acuerdo a las necesidades del cliente brindándoles la mejor opción para sus requerimientos, esto me ha permitido experimentar y poner en marcha mis conocimientos para la detección y solución de fallas, así como para identificar las posibles problemáticas que los sistemas biométricos pudieran presentar.

Así también mi permanencia en **IBIX S.A de C.V**, me ha permitido adquirir nuevos conocimientos en el área electrónica, tales como el funcionamiento y la estructura de los microprocesadores Microchip Technology/Amtel AT91SAM9260, así como del microcontrolador Atmega48A, así también la interfaz y carga de firmware (programa lógico de funcionamiento).

Por otro lado, también he adquirido conocimientos respecto al correcto ensamblamiento de los lectores de huellas, lectores de proximidad, lectores de códigos de barra, así como la colocación de semáforo, cámara fotográfica y display, de igual forma con respecto a la tarjeta de control de los equipos biométricos he aprendido a realizar la electrónica controladora de los torniquetes y barreras

vehiculares, además de reparar las fuentes de voltaje y las tarjetas controladoras para los equipos de acceso (torniquetes y barreras vehiculares).

Algo que también he tenido la oportunidad de aprender es la instalación de los equipos biométricos que tienen una interfaz con los equipos PLC´S para el sistema de bloqueo de accesos para puertas.

En general mi paso por **IBIX, S.A de C.V** ha sido una excelente oportunidad para poner en marcha los conocimientos adquiridos durante mi formación en la Universidad de la Ciudad de México (Ingeniera en Sistemas Electrónicos Industriales) y en la Escuela Mexicana de Electricidad (Diplomado en PLC, Diplomado en Control Industrial de Motores), sin embargo, también para adquirir nuevas experiencias y conocimientos útiles para poder poner en marcha los sistemas biométricos, siendo un gran reto profesional lograr conjugar mis experiencias profesionales y los nuevos retos que se me han presentado en **IBIX, S.A de C.V.**

La elaboración de este reporte me deja conocimientos muy amplios sobre la implementación de los sistemas biométricos, así como nuevas ideas sobre dónde poder implementar los conocimientos adquiriros, abriendo un nuevo panorama que me ha permitido visualizar nuevas áreas de desempeño profesional.

BIBLIOGRAFÍA

1. IBIX, S.A de C.V, (2013). Sitio Web: http://www.ibix.com/

2. Oktaba, H. (2003). *Modelo de Procesos para la Industria de Software*. Ciudad de México: Moprosoft.

3. Valdés, R (2012), *Automatización de un sistema de climatización con PLC* (tesis de pregrado), Instituto Politécnico Nacional, Ciudad de México, disponible en: https://tesis.ipn.mx/jspui/bitstream/123456789/10566/1/98.pdf

4. Gutiérrez I, Serrano V (2016), *Sistemas para cerradura electromagnética utilizando modulo bluetooth*, (tesis de pregrado) Instituto Politécnico Nacional, Ciudad de México, disponible en: file:///C:/Users/DELL/Downloads/%E2%80%9CSISTEMA%20PARA%20CERRADURA%20ELECTROMAGN%C3%89TICA%20(1).pdf

5. Olvera Y, Rizo J (2013), *Implementación de un dominio en el centro de apoyo a la docencia del CELE para la optimización de sus recursos y servicios* (tesis de pregrado), Universidad Nacional Autónoma de México, disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/4306

6. Fabla, Vélez, Moran (2011), I*mplementación de elementos para prácticas de cableado estructurado para el laboratorio de comunicaciones*, (tesis de pregrado), Universidad Católica de Santiago de Guayaquil, Ecuador, disponible en; http://repositorio.ucsg.edu.ec/bitstream/3317/8557/1/T-UCSG-PRE-TEC-ITEL-224.pdf

7. Castellon, A. (2014), *Cableado estructurado norma EIA TIA 568*, 01 junio 2020, de Fundación Tecnológica Arévalo de Sitio web: https://mtlsasturiasnoe.files.wordpress.com/2015/10/cableadoestructurado_norma-eia-tia-568.pdf

8. López X (2008), *Rediseño de la Red con Calidad de Servicios para datos y Tecnología de voz sobre IP en el Ilustre municipio de Ambato* (tesis de pregrado), Pontificia Universidad Católica del Ecuador, Ecuador, disponible en: https://repositorio.pucesa.edu.ec/bitstream/123456789/645/1/85008.PDF

9. Montaño, MA (2006), *Diseño de un servidor web embebido* (tesis de postgrado), Universidad Nacional Autónoma de México, Ciudad de México, disponible en: http://132.248.9.195/pd2006/0608232/Index.html

10. Mora, A (2016), *Control de acceso en gestión de prevención,* Universidad Politécnica de Cartagena, España, disponible en: https://repositorio.upct.es/bitstream/handle/10317/5636/tfmmorges.pdf?sequence=3&isAllowed=y

11. Estrada, A (2004), Protocolos TCP/IP de internet, Revista Digital Universitaria, Vol. 5, 1–7, disponible en: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

12. Díaz, Vanessa (2013) *Sistemas biométricos en materia criminal: un estudio comparado.* Revista IUS*, Vol.7, 1–20,* disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003

13. Sánchez LA (2019*), Manual para el uso de los datos biométricos en los servicios financieros* (tesis de pregrado), INFOTEC Centro de investigación e innovación en tecnologías de la información y la comunicación, CDMX, disponible en: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/329/1/INFOTEC_MDTIC_LASC_10102019.pdf

14. Etchart, Graciela, y Col (s.f), *Sistemas de reconocimiento biométricos, Importancia del uso de estándares en entes estatales,* Facultad de ciencias de administración, Universidad nacional de entre ríos, Argentina, disponible en: https://core.ac.uk/reader/15776878