TRABAJO ESPECIAL DE GRADO

DETECCION DE FALLAS DEL SISTEMA BIOMETRICO DE RECONOCIMIENTO DE HUELLAS DACTILAR DE LA EMPRESA CONVIASA

Presentado ante la Ilustre
Universidad Central de Venezuela
por la Br. Juana S. Lara L.
para optar al título de
Ingeniero Electricista

Caracas, 2017

TRABAJO ESPECIAL DE GRADO

DETECCION DE FALLAS DEL SISTEMA BIOMETRICO DE RECONOCIMIENTO DE HUELLAS DACTILAR DE LA EMPRESA CONVIASA

Tutor Académico: Ing. Pedro Pinto
Tutor Industrial: Ing. José G. Domínguez

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Juana S. Lara L.
para optar al Título de
Ingeniero Electricista

Caracas, 2017

CONSTANCIA DE APROBACIÓN

Caracas, 13 de junio de 2017

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Bachiller Juana S. Lara L., titulado:

"DETECCIÓN DE FALLAS DEL SISTEMA BIOMÉTRICO DE RECONOCIMIENTO DE HUELLAS DACTILAR DE LA EMPRESA CONVIASA"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la opción de Electrónica y Control, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Rafael Rivero
Jurado

Prof. Servando Álvarez
Jurado

Prof. Pedro Pinto
Prof. Guía

DEDICATORIA

"Determinación, Perseverancia
y Terquedad combustibles que
juntos permiten lograr sueños"
Juana Lara

Honor a Dios!

Honor a mis Padres!

Honor a mi Familia: Frencell, Ramsés y Luís Alejandro!

RECONOCIMIENTOS Y AGRADECIMIENTOS

Tengo el agrado de nuevamente mostrar la retribución, a ese ***ser***, luminoso, omnipresente y omnipotente que guía mis pasos y protege mi vida. Gracias

A mis amados padres Luís y Elba sin ellos no podría haber logrado una nueva meta. Gracias

A mis motores, mis chiquitines Ramsés y Luís Alejandro, que junto a Frencell rodean mi existencia. Gracias

A mis familiares Josefa, José, Elba, Santos, Carmen, Berta, Máximo, Katherin, gracias por impulsar cuando fue necesario.

A mis amigos que son muchísimos, sino los menciono aquí, igual saben que siempre lo seremos, Belkys, Carlos, Katerin, Angela, David, Kenny, Engels, Lucy, Jackson, Sergio, Alonso, Vicente, Milagros, Fariña, Dhayana, gracias por su constancia y dedicación en la carrera.

A los profesores de la Facultad de Ingeniería, Jesús Fernández, a los profesores de la Escuela de Ingeniería Eléctrica en especial al profesor Raúl Arreaza, Pedro Pinto, Rafael Rivero, Servando Álvarez, José Romero, Joao Nunes, Ebert Brea, Tamara Pérez, Mercedes Arocha. Gracias

A la Empresa Conviasa por permitirme adquirir conocimientos junto a su personal de la Oficina de Tecnología de Información: José Domínguez, Domingo Rodríguez, Alberto, María, Luís, Magali, Yoli, Wilfredo, Isidro, Yoberlyn, Jeily Maikol, Freddy, Anginet, entre otros.

Lara L. Juana S.

DETECCIÓN DE FALLAS DEL SISTEMA BIOMÉTRICO DE RECONOCIMIENTO DE HUELLAS DACTILAR DE LA EMPRESA CONVIASA

Prof. Guía: Ing. Pedro Pinto. Tutor Industrial: Ing. José Domínguez. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Electrónica, Instrumentación y Control. Institución: CONVIASA. 2017. 100 h. + anexos.

Palabras Claves: Sistema Biométrico, Biometría, Sensores de Huella Dactilar, Lector óptico, AMEF (Análisis de Modo Y Efecto de la Falla), Cableado Estructurado.

Resumen: Un Sistema Biométrico de Reconocimiento de Huella Dactilar debe garantizar un desempeño con un alto grado de exactitud, robustez y rapidez, al momento de verificar y comprobar la identificación de los usuarios que se encuentran registrados y almacenados en su Base de Datos, además de generar la confianza en este sistema cuando es utilizado. Se realiza una detección de fallas del Sistema Biométrico de la Empresa Conviasa, fundamentada en el estudio de sus características de funcionamiento, conexiones y enlaces de red principales, con el fin de generar ajustes en caso de que ocurran y compensar ciertas fallas especificas eliminando o disminuyendo su frecuencia con recomendaciones adaptadas al Sistema, al cual se aplico el formato AMEF, todas estas acciones se basan en la función primordial de operar el Sistema, bajo ciertas condiciones de fiabilidad durante el mayor tiempo posible.

INDICE GENERAL

CAPITULO III

EL SISTEMA BIOMETRICO DE LA EMPRESA

LISTA DE TABLAS, ESQUEMAS Y CUADROS

Paginas

LISTA DE FIGURAS

Paginas

SIGLAS Y ABREVIATURAS

AMEF	Análisis de Modo Y Efecto de la Falla
CANTV	Compañía Anónima Nacional Teléfonos de Venezuela
CEN	Código Eléctrico Nacional
FMEA	Failure Mode Effect Analysis
LAN	Local Area Network
OTI	Oficina de Tecnología e Información
VPN	Virtual Private Network
SUPREMA Inc	Suprema Internacional

ACRONIMOS

AFIS	Automated Fingerprint. Identification System
ANSI/INCITS 378	American National Standards Institute/ InterNational Committee for Information Technology
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
BC	Bonding Conductor
CCD	Charged Coupled Device
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DBMS	Data Base Management System
DRM	Digital Rights Management
FDDI	Fiber Distributed Data Interface
HDD	Hard Disk Drive
IEEE 802.3	Institute of Electrical and Electronics Engineers 802.3
IGMP	Internet Group Management Protocol
LAN	Local Area Network
RPN	Risk Priority Number
PC	Personal Computer
RAM	Random Access Memory
TBB	Telecomunications Boeing Backbone
TCP/IP	Transmission Control Protocol /Internet Protocol
TGB	Telecomunications Grounding Buscar
TMGB	Telecomunications Main Grounding Busbar
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair

INTRODUCCION

Conviasa es una aerolínea venezolana creada en 2004 para reemplazar a la extinta Viasa (Venezolana Internacional de Aviación, Sociedad Anónima) con el propósito de que Venezuela volviera a tener una línea aérea reconocida.

Conviasa (Consorcio Venezolano de Industrias Aeronáuticas y Servicios Aéreos S.A.) Tiene su sede en el Aeropuerto Internacional de Maiquetía Simón Bolívar. La empresa maneja alrededor de 1500 empleados en su sede principal, Maiquetía. Por tanto, fue imprescindible instalar un Sistema Biométrico de Reconocimiento de Huellas Dactilares para brindar seguridad a sus empleados. La red biométrica de la Empresa Conviasa utiliza sus dispositivos para controlar la asistencia de los trabajadores y sus accesos restringidos en algunos departamentos, como de libre acceso en otras áreas que son comunes a todo el personal, además de su función primordial la de garantizar la seguridad en dicha Empresa. Adicionalmente el Sistema Biométrico se encuentra instalado en las estaciones de Porlamar y Maracaibo por ser las estaciones con mayor cantidad de personal, luego de Maiquetía.

La detección de fallas en el Sistema Biométrico permitirá aumentar la confiabilidad al bajar la probabilidad de sus ocurrencias con menos frecuencia, o en su defecto anularlas, además se adquiere mejor operatividad del Sistema.

Para localizar dichas fallas, se recurre a efectuar una investigación acerca del funcionamiento del Sistema Biométrico en la Empresa, sus características de canalización, entre otras particularidades. Además, se genera una encuesta para indagar los inconvenientes mas frecuentes solucionados por el personal de Soporte Técnico. Luego, mediante una evaluación de cada falla se utiliza el método inductivo AMEF (Análisis de Modo Detección de Fallas). Además de recomendaciones para mejorar el Sistema Biométrico

CAPITULO I

DESCRIPCIÓN DEL PROYECTO

1. Planteamiento del Problema

Un Sensor de huellas digitales (también conocido como *sensor de huella dactilar, lector de huella dactilar o sensor biométrico*) es un dispositivo capaz de leer, guardar e identificar las huellas dactilares. Todos los sensores biométricos de huella dactilar, poseen una pieza que es sensible al tacto (que es el sensor en sí, aunque luego hacen falta ciertas partes electrónicas).

La biometría es una tecnología de seguridad, basada en el reconocimiento de una característica física e intransferible, como por ejemplo la huella digital. Las técnicas de la biometría se aprovechan del hecho que las características del cuerpo humano son únicas y fijas. Los rasgos faciales, el patrón del iris del ojo, los rasgos de la escritura, la huella dactilar, y otros muchos son los que se utilizan para estas funciones, incluyendo el ADN [1].

La identificación por medio de huellas digitales constituye una de las formas más representativa de la utilización de la biometría. Una huella digital está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados 'puntos de minucia' [2]. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general. La huella dactilar es utilizada por el equipo biométrico para realizar la plantilla digital que usa en la base de datos, para su posterior verificación y comprobación, lo cual permitirá el acceso o no del usuario en los lugares donde sea permitido.

El sistema biométrico de la empresa Conviasa en su sede de Maiquetía (Figura 1) requiere de mejoras en la configuración de control para accesos en sus instalaciones. Del mismo modo, corrección de fallas en la implementación del equipo, por tanto se formula de forma adecuada por medio de esta propuesta.

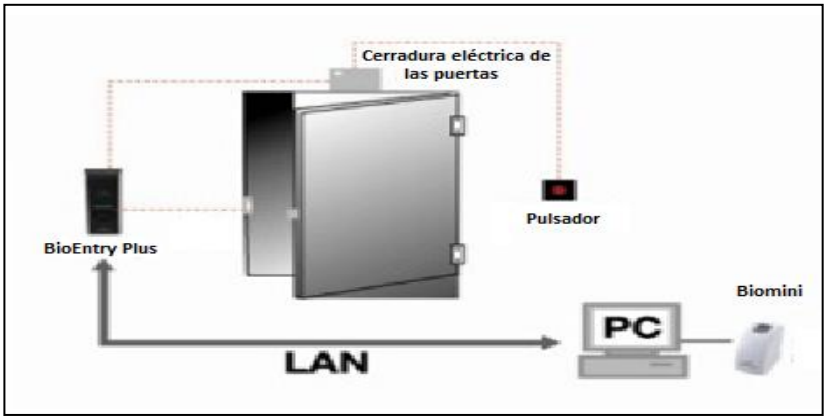


Figura 1. Interconexión de la Red Biométrica de Conviasa. **Fuente: Elaboración Propia basada en Guía de Administración BioStar [6].**

La carga de los datos del sistema biométrico se realiza por medio del escáner de inscripción, lo realizan tanto el personal del Departamento de Recursos Humanos como el personal de la Oficina de Tecnología de la Información, además de otros departamentos con acceso al Sistema Biométrico. Dicha huella es almacenada en el servidor principal, en forma de plantilla digital, contiene información de los accesos donde el trabajador puede o no transitar, estos lugares son restringidos por medio de equipos biométricos.

La oficina de Tecnología de la Información es la encargada de instalar, configurar y administrar la red biométrica utilizando el Software Biostar y el protocolo TCP/IP (Protocolo de Control de Transmisión/ Protocolo Internet). La Red biométrica presenta fallas de distintas formas, debido a la instalación de nuevos equipos dado que se requería una sustitución de los equipos viejos, además que el aumento de la base de datos exige un nuevo servidor. Por otro lado, existe el inconveniente de administrar los permisos de accesos del personal de la empresa en horarios no permitidos.

La detección de las fallas en el Sistema Biométrico de Conviasa, permitirá realizar propuestas para corregirlas buscando un sistema eficiente con miras a solucionarlas rápidamente en el momento que ocurra una nueva eventualidad y hacer el sistema más robusto.

1.1 Objetivos

General

Detectar las fallas del Sistema Biométrico de reconocimiento de huella dactilar de la Empresa Conviasa

Específicos

- Definir las características y el funcionamiento de los equipos biométricos utilizados en la empresa.
- Revisar las canalizaciones del Sistema Biométrico
- Revisar el circuito y el programa utilizado para el control de la base de datos del Sistema Biométrico
- Determinar posibles fallas del Sistema
- Elaborar un informe del estado del sistema y las recomendaciones para corregir las fallas detectadas en el Sistema

1.3 Acerca de la Empresa

Conviasa es una aerolínea venezolana creada en 2004 para reemplazar a la extinta Viasa (*Venezolana Internacional de Aviación, Sociedad Anónima*) con el propósito de que Venezuela volviera a tener una línea aérea reconocida. Conviasa *(Consorcio Venezolano de Industrias Aeronáuticas y Servicios Aéreos.)* Tiene su sede en el Aeropuerto Internacional de Maiquetía Simón Bolívar. Maiquetía es la sede principal entre otras sucursales a lo largo del país. El 10 de diciembre de 2004, Conviasa empezó formalmente sus operaciones tanto nacionales como internacionales contribuyendo de esta forma al desarrollo turístico sustentable, mediante la explotación del servicio público de transporte aéreo nacional e internacional de pasajeros, carga y correo.

1.3.1 Inicios

El 30 de marzo de 2004, el presidente Hugo Chávez firmó un decreto para establecer formalmente la aerolínea. Este decreto fue publicado al día siguiente en la Gaceta Oficial Nº 37.910 de Venezuela. El 28 de noviembre de 2004, se realizó el vuelo inaugural con un avión De Havilland Canada Dash 7, el cual voló desde el Aeropuerto Caracas "Oscar Machado Zuloaga" , en Charallave, Estado Miranda, hasta el Aeropuerto Internacional del Caribe Santiago Mariño, en la Isla de Margarita. El 10 de diciembre de 2004, Conviasa empezó formalmente sus operaciones tanto nacionales como internacionales.

1.3.2 Historia

La idea de formar Conviasa como la Línea Aérea Bandera de Venezuela, comienza a gestarse en mayo de 2001, con la finalidad de canalizar en forma dinámica la incorporación de la población al desarrollo de la economía social nacional y global en cada localidad o municipio de la República Bolivariana de Venezuela, contribuyendo de esta forma al desarrollo turístico sustentable,

mediante la explotación del servicio público de transporte aéreo nacional e internacional de pasajeros, carga y correo.

En diciembre de 2002 se frena este proyecto. Es retomado el 01 de octubre de 2003, bajo la tutela del Ministerio de la Producción y el Comercio. En fecha del 30 de marzo de 2004, el Presidente de la República Bolivariana de Venezuela, Hugo Chávez Frías, firma el Decreto de la creación de la línea aérea. El 31 de marzo, el mismo es publicado en la Gaceta Oficial. N° 37.910.

El Consorcio Venezolano de Industrias Aeronáuticas y Servicios Aéreos (Conviasa), realizó el primer vuelo con la aeronave modelo DASH-7, de siglas venezolanas YV-1169, el 28 de noviembre de 2004, desde el Aeropuerto de Charallave rumbo al Aeropuerto Santiago Mariño, en la Isla de Margarita, que la certificó como línea aérea comercial, despegando luego hacia la Isla de Granada.

El 10 de diciembre de 2004, la Aerolínea Bandera de Venezuela, inicia formalmente sus operaciones de vuelos nacionales e internacionales. El 20 de noviembre de 2015 por Gaceta Oficial Nº 40.793, a través del Decreto N° 2.106 asume la Presidencia de Conviasa el Mayor General Franklin Rafael Gil Espinoza, quien actualmente asume el cargo. La ubicación actual de Conviasa, es en la Av. Intercomunal Aeropuerto Internacional de Maiquetía, Edif. Sector 6-3. Zona Estratégica, lado Este del Aeropuerto Internacional de Maiquetía, Adyacente a Tránsito Terrestre, hangares PB, Maiquetía - Edo. Vargas, Venezuela. Apartado postal 1161.

Misión

Prestar servicios aeronáuticos para el desarrollo social y sustentable de la Nación, con personal altamente capacitado, logrando la satisfacción de nuestros clientes.

Visión

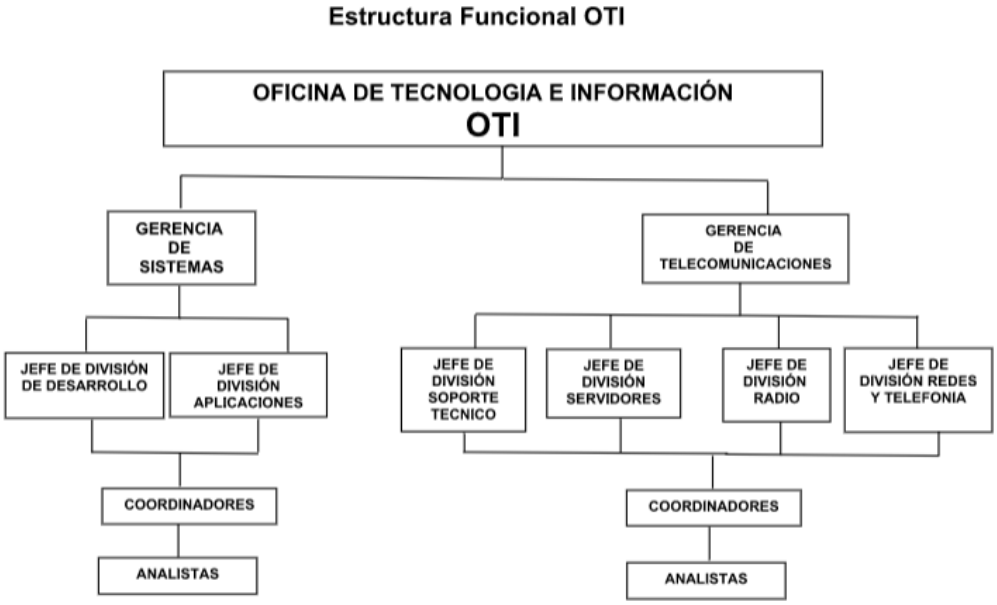
Consolidarse como la empresa líder en América Latina y el Caribe en la prestación de servicios aeronáuticos, cumpliendo con los más altos estándares nacionales e internacionales de gestión ambiental, seguridad y calidad, enmarcados en el Plan Estratégico de la Nación.

Valores

- Calidad, el cliente es primero.
- Seguridad, es tarea de todas y todos.
- Trabajo en Equipo, para alcanzar los objetivos.
- Compromiso, creemos en lo que hacemos y hacemos lo que nos gusta.
- Honestidad, lideramos con el ejemplo.
- Somos venezolanos, servimos con calidez.

1.4 Estructura Organizativa de la Empresa

Dentro de la organización de la Empresa, se encuentra la Oficina de Tecnología e Información (OTI), dentro de sus actividades se encarga de gestionar la automatización de procesos y servicios en Conviasa, con el objeto de facilitar el control eficiente, eficaz y oportuno de la gestión comercial, a través del diseño, desarrollo, implementación, evaluación, respaldo y mantenimiento de sistemas basados en nuevas tecnologías, con el fin de establecer una posición vanguardista que permita sustentar el modelo de negocios de la empresa. La Oficina de Tecnología de la Información (OTI) se presenta bajo el siguiente esquema 1:



Esquema 1. Organigrama del Departamento de la Oficina de la Información.

Fuente: Conviasa 2016

El desarrollo de la pasantía se llevara a cabo en la División de Redes y Telefonía, la cual es la encargada de gestionar la instalación y configuración de los dispositivos biométricos, así como también, la administración de la base de datos del Sistema Biométrico.

CAPITULO II

MARCO TEORICO

2. Biometría

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física o de comportamiento intransferible de las personas [2, 20], tal como se muestra en la figura 2.1.

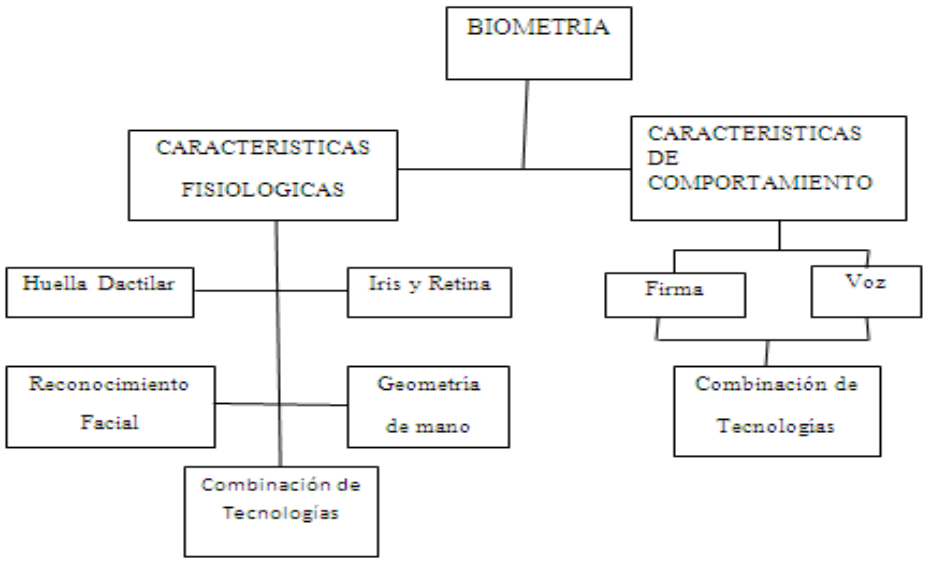


Figura 2.1: Características Biométricas.

2.1 Características de la Biometría

Los rasgos biométricos se pueden usar en cualquier rasgo anatómico o de comportamiento humano como identificador biométrico para identificar o verificar a las personas si satisface los requerimientos siguientes:

- **Universalidad**: Cada persona debe poseer ese rasgo biométrico.
- **Particularidad**: Todas las personas tienen que ser suficientemente diferentes en términos del rasgo biométrico.

- **Permanencia**: El rasgo biométrico debe ser invariante en el tiempo y a cualquier otro factor desde el punto de vista de la comparación entre rasgos biométricos.
- **Medible**: El rasgo biométrico se tiene que poder medir cuantitativamente.
- **Rendimiento**: El rasgo biométrico debe garantizar precisión y robustez en diferentes factores ambientales.
- **Aceptabilidad**: Los usuarios del sistema deben aceptar el uso de ese rasgo biométrico para su identificación.
- **No falsificable**: El rasgo biométrico tiene que garantizar que su falsificación sea dificultosa. Un sistema biométrico debe tener una precisión y velocidad aceptable con un número de recursos razonable. Además, no puede ser nocivo para los usuarios, debe ser aceptado por los usuarios potenciales y ser lo suficientemente robusto ante los métodos fraudulentos.

2.2. Huella dactilar

Las huellas dactilares o digitales son un identificador único para cada ser humano, nunca coinciden dos huellas, ni en los gemelos idénticos. Ya que estas se desarrollan en la etapa embrionaria. Tiene muchos fines como proteger derechos de autor o en sistemas de seguridad de alta tecnología. También se llama DRM (Digital Rights Management traducido como Gestión de Derechos Digitales), sirven para proteger contenido digital por el "problema" de la copia pirata.

2.2.1 Lectores de Huella Dactilar

Un lector de huella digital lleva a cabo dos tareas: Obtener una imagen de la huella digital y comparar el patrón de valles y crestas de dicha imagen con los patrones de las huellas que tiene almacenadas. Los dos métodos principales de obtener una imagen de una huella digital son por lectura óptica o lectura de capacitancia.

2.2.1.1 Lectores ópticos

Un lector o sensor óptico funciona con un dispositivo CCD (Dispositivo de Carga Acoplada, del inglés, Charged Coupled Device) tiene un arreglo de fotodiodos sensible a la luz, que generan una señal eléctrica en respuesta a fotones de luz. Dicho lector detecta los relieves de la huella mediante las sombras y la iluminación. Tras esto crea un mapa digital con la información recogida y se asegura de que la iluminación sea la correcta. Si esto se ha cumplido entonces envía la información para ser almacenada, si no fuese así se volvería a tomar la imagen digital.

Cada fotodiodo graba un píxel, un pequeño punto que representa la luz que le es reflejada. Colectivamente, la luz y perfiles oscuros forman una imagen de la huella leída. El proceso de lectura comienza cuando se coloca el dedo sobre la ventana del lector, el cual tiene su propia fuente de iluminación, típicamente un arreglo de leds, para iluminar las crestas de la huella digital. El CCD genera, de hecho, una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y áreas más claras que representan menos luz reflejada (los valles entre las crestas).

Antes de comparar la información obtenida con la almacenada, el procesador del lector se asegura de que el CCD ha capturado una imagen clara. Chequea la oscuridad promedio de los píxeles, o los valores generales en una pequeña muestra, y rechaza la lectura si la imagen general es demasiado oscura o demasiado clara. Si la imagen es rechazada, el lector ajusta el tiempo de exposición para dejar entrar más o menos luz, e intenta leer la huella de nuevo. Si el nivel de luz es adecuado, el lector revisa la definición de la imagen (que tan precisa es la imagen obtenida). El procesador busca varias líneas rectas que se mueven horizontal y verticalmente sobre la imagen, y si esta tiene buena definición, una línea que corre perpendicular a las crestas será hecha de secciones alternantes de píxeles muy claros y muy oscuros.

Dicho detector detecta los relieves de la huella mediante las sombras y la iluminación como muestra la figura 2.2. Tras esto crea un mapa digital con la información recogida y se asegura de que la iluminación sea la correcta. Si esto se ha cumplido entonces envía la información para ser almacenada, si no fuese así se volvería a tomar la imagen digital.

Figura 2.2: Principio básico del lector óptico de huella digital.

Fuente: http://st2biometricstechniques.blogspot.com/2012

2.2.1.2 Lectores capacitivos

Los lectores capacitivos de huella digital generan una imagen de las crestas y valles que conforman una huella digital, pero en vez de hacerlo con luz, los capacitores utilizan corriente eléctrica. La figura 2.3 muestra un ejemplo de sensor capacitivo. El sensor está hecho de uno o más circuitos integrados que contienen un arreglo de pequeñas celdas. Cada celda incluye dos placas conductoras, cubiertas con una capa aislante.

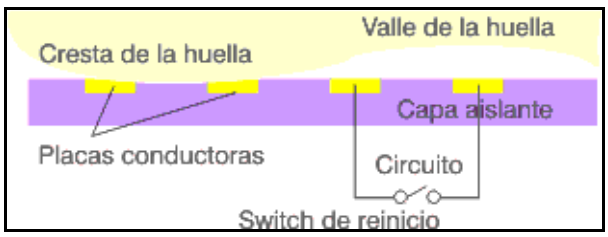


Figura 2.3: Principio básico del lector capacitivo de huella digital. **Fuente: https://tec-mex.com.mx/promos/bit/bit0903-bio.htm**

Las celdas son más pequeñas que el ancho de una cresta del dedo. El sensor está conectado a un integrador, un circuito eléctrico construido sobre la

base de un amplificador operacional inversor que altera un flujo de corriente. La alteración se basa en el voltaje relativo de dos fuentes, llamado la terminal inversora y la terminal no-inversora. En este caso, la terminal no-inversora es conectada a tierra, y la terminal inversora es conectada a una fuente de voltaje de referencia y un bucle de retroalimentación que incluye las dos placas conductoras, que funcionan como un condensador, esto es, un componente que puede almacenar una carga. La superficie del dedo actúa como una tercera placa condensadora, separada por las capas aislantes en la estructura de la celda y, en el caso de los valles de la huella, una bolsa de aire.

Al variar la distancia entre las placas condensadoras (moviendo el dedo más cerca o más lejos de las placas conductoras), se cambia la capacitancia (o habilidad para almacenar una carga) total del condensador. Esta cualidad, permite que el condensador en una celda bajo una cresta, tenga una capacitancia más grande, que el condensadora en una celda bajo un valle. Ya que, la distancia al dedo altera la capacitancia, la cresta de un dedo resultará en una salida de voltaje diferente a la del valle de un dedo. El procesador del lector lee esta salida de voltaje y determina si es característico de una cresta o un valle. Al leer cada celda en el arreglo de sensores, el procesador puede construir una imagen de la huella, similar a la imagen capturada por un lector óptico.

La principal ventaja de un lector capacitivo es que requiere una verdadera forma de huella digital y no sólo un patrón de luz y oscuridad que haga la impresión visual de una huella digital. Esto hace que el sistema sea más difícil de engañar. Adicionalmente, al usar un circuito integrado semiconductor en vez de una unidad CCD, los lectores capacitivos tienden a ser más compactos que los ópticos.

2.3 Sistema Biométrico

Es un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada [1, 100]. En base a la obtención de un sistema biométrico con utilidad práctica podremos hablar de ciertas características que se considerarán a la hora de su diseño.

El desempeño: Se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

La aceptabilidad: Indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica.

La fiabilidad: Refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, etc.

Los sistemas biométricos poseen tres componentes básicos. El primero se encarga de la adquisición analógica o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema.

La arquitectura típica de un sistema biométrico se presenta en la siguiente figura 2.4:

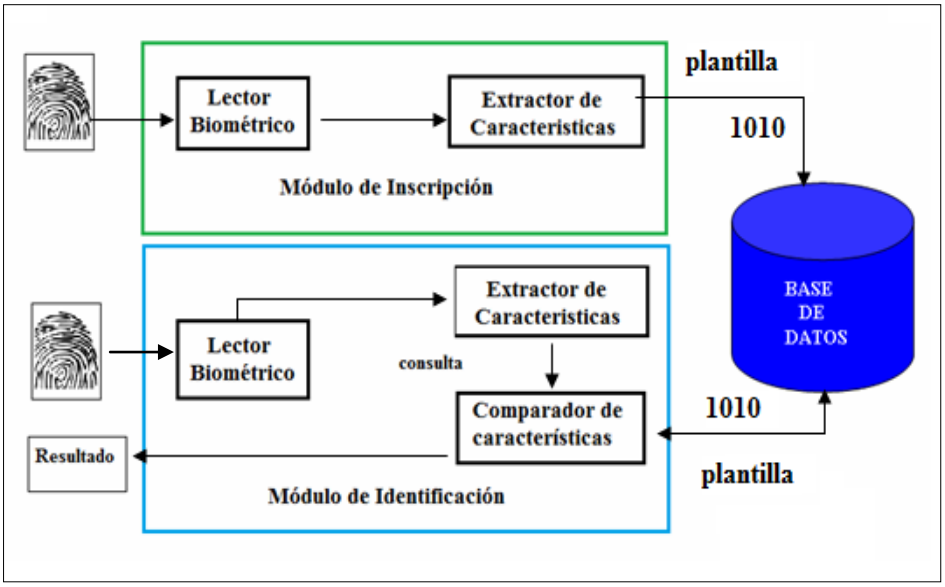


Figura 2.4: Arquitectura de un Sistema Biométrico para identificación personal. **Fuente: Elaboración Propia basada en "Sistemas de Seguridad basados en Biometría" [1]**

En la figura se distinguen dos módulos diferentes:

El módulo de inscripción: Se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El módulo de identificación: Extrae características representativas del indicador biométrico para luego compararlas con la información almacenada en una base de datos que previamente ha sido completada por el módulo de inscripción.

Un sistema biométrico puede operar en dos modos:

Modo de verificación: Comprueba la identidad de algún individuo comparando la característica sólo con registros guardados de ese individuo. El modo de verificación responderá a la pregunta: ¿eres tú quien dices ser?

Modo de identificación: Descubre a un individuo mediante una comparación exhaustiva con todos los registros guardados de distintos individuos. El modo de identificación responderá a la pregunta: ¿quién eres tú?

2.4 Fundamentos de la Canalización de los Dispositivos Biométricos

El medio de comunicación en una red LAN (Redes de Área Local, de sus siglas en ingles, Local Area Network) es el canal o enlace físico entre los nodos de una red a través del cual es transmitida la información. Los principales medios de comunicación son: a) Un medio de comunicación alambrico se define como un cable y quizá otros dispositivos electrónicos que conectan físicamente adaptadores de comunicación entre sí. b) La fibra óptica transmite haces de luz a altas velocidades y tráficos muy altos. Sí el medio de comunicación consta solamente de cable, el medio de comunicación es llamado pasivo [4].

La conexión de los dispositivos biométricos esta fundamentada en cableado estructurado, ya que de allí depende su transmisión de datos por toda la red biométrica de la empresa, desde y hacia el servidor principal. También requiere de un cableado eléctrico para los pulsadores, la alimentación eléctrica y la cerradura de la puerta.

2.4.1 Cableado Estructurado

Se trata de una red física que combina cable UTP (Unshielded Twisted Pair, par trenzado sin blindaje), bloques de conexión y adaptadores entre otros elementos. Soporta diversos dispositivos de telecomunicaciones, el cableado estructurado permite ser instalado o modificado sin necesidad de tener conocimiento previo sobre los productos que se utilizan sobre él. Permite transportar dentro de una edificación las señales, que provienen de un emisor hasta su correspondiente receptor.

Entre los elementos principales del sistema de cableado estructurado se encuentra el cableado horizontal (recorre el suelo, techo y paredes de la estructura física), el cableado vertical (interconecta diversos cuartos) y el cuarto de telecomunicaciones (con los equipos de telecomunicaciones). Otro de los conceptos relacionados con el cableado estructurado es el sistema de puesta a tierra y puenteo. El Apéndice A contiene el tema referente a cableado estructurado [5].

12.5 Puesta a Tierra

El sistema de puesta a tierra es un componente fundamental en un gabinete moderno. El objetivo de este recurso es desviar a tierra toda provisión indebida de corriente eléctrica a los dispositivos que se encuentran al alcance de los usuarios, lo cual sucede a raíz de un error en el aislamiento de los conductores activos.

El sistema de puesta a tierra para un cableado estructurado está diseñado para asegurar una misma referencia eléctrica para todos los sistemas electrónicos contenidos en los diferentes espacios de un edificio o un Centro de Datos. Este sistema está normado por el estándar ANSI/J/STD-607-A [6].

Según el Código Eléctrico Nacional (CEN) y la norma ANSI/J/STD 607-A permite que el sistema de puesta a tierra para telecomunicaciones se debe unir al sistema de puesta a tierra del edificio mediante un puente de conexión equipotencial la siguiente figura 2.5.1 muestra las conexiones, los cables de puesta a tierra deben de instalarse con un número mínimo de dobleces.

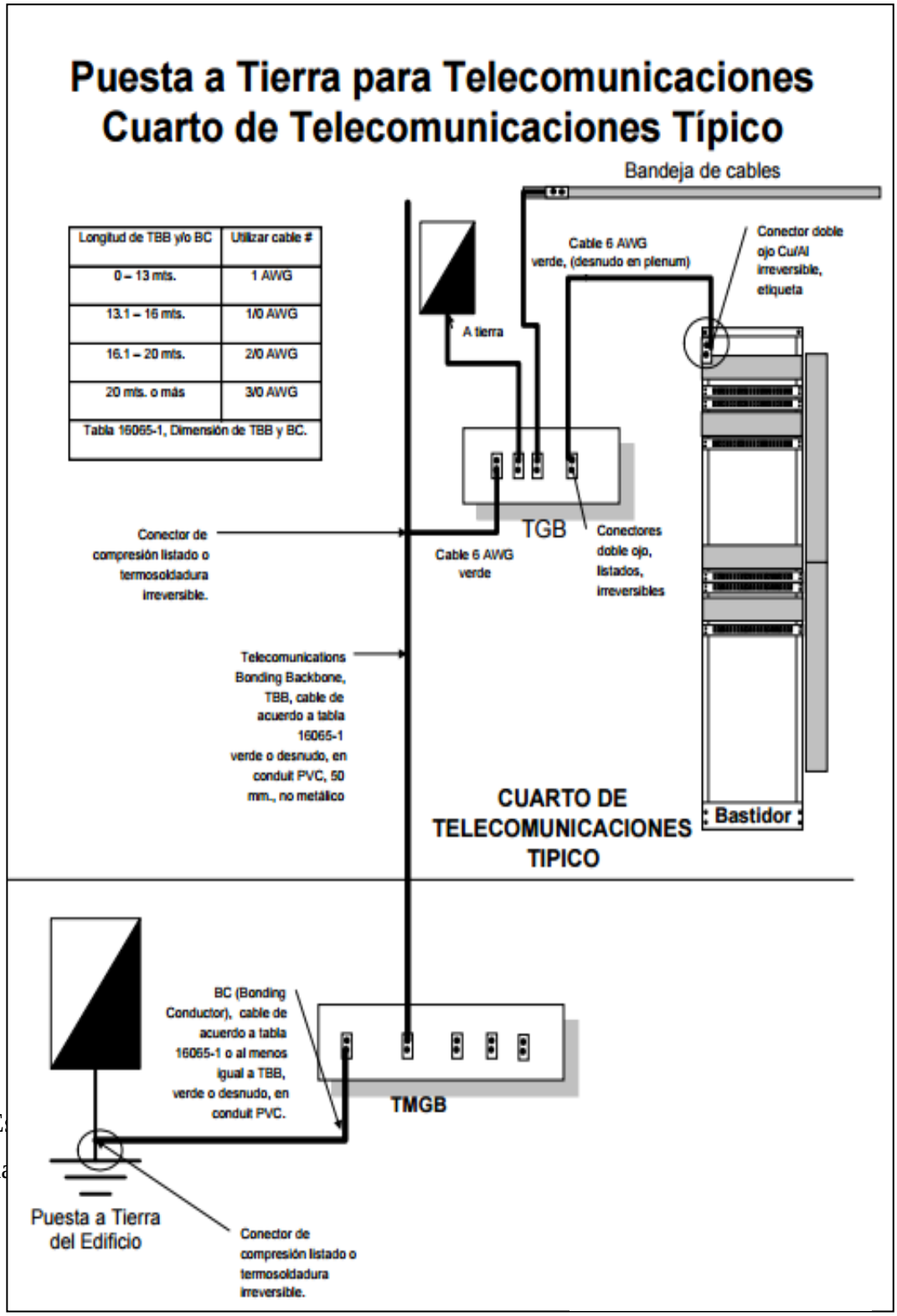


Figura 2.5: Puesta a Tierra para el cuarto de Telecomunicaciones.

2.6 BASE DE DATOS

Una base de datos es una colección de información útil, organizada de una manera específica, se coleccionan archivos relacionados que permiten el manejo de la información de alguna Empresa. Cada uno de dichos archivos puede ser visto como una colección de registros y cada registro está compuesto de una colección de campos. Cada uno de los campos de cada registro permite llevar información de algún atributo de una entidad del mundo real. Un archivo de una base de datos, también puede ser pensado como una tabla en la que tenemos renglones y columnas, cada renglón correspondiendo a un registro del archivo y cada columna correspondiendo a un campo

Los componentes de un Sistema de Base de Datos involucran los siguientes componentes:

- Hardware
- Software
- Datos

Hardware: Consiste básicamente de unidades de almacenamiento secundario, principalmente discos duros, discos compactos, entre otros.

Software: Entre la base de datos física y los usuarios existe una capa de Software denominada Sistema Manejador de Base de Datos (SMBD ó DBMS). Todos los requerimientos de acceso a la base de datos son manejados por el SMBD.

Una red es una configuración de computadoras que intercambian información. Pueden proceder de una variedad de fabricantes y es probable que tenga diferencias tanto en hardware como en software, para posibilitar la comunicación entre estas es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos. Un protocolo es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos [4, 113].

2.6.1 Protocolo TCP/IP

El más ampliamente utilizado es el TCP/IP. Es un protocolo que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto. El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa [4, 114]. Los módulos del software de protocolos se modelan pensando en una pila vertical constituida por capas como se observa en la figura 2.6.1. Cada capa tiene la responsabilidad de manejar una parte del problema.

Figura 2.6: Capas de red de la norma TCP/IP.

La capa de RED: Permite enrutamiento de datos por la conexión, coordinación de la transmisión de datos (sincronización), formato de datos, conversión de señal (análoga/digital) detección de errores a su llegada. Protocolos: Ethernet, Frame Relay, entre otros.

La capa INTERNET: define los datagramas y administra las nociones de direcciones IP. Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben. Protocolos: IP (Protocolo Internet), ARP (Protocolo de Resolución de Direcciones, del inglés, Address Resolution Protocol), RARP (Protocolo de Resolución de Direcciones Inverso, en inglés, Reverse Address Resolution Protocol) y IGMP (Internet Group Management Protocol)

La capa TRANSPORTE: permite que las aplicaciones que se ejecuten en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones. Además, el nombre de la aplicación puede variar de sistema en sistema. Se implementa el sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se llaman puertos. Protocolos: TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagrama de usuario, del ingles, User Datagram Protocol)

La capa APLICACIÓN: La mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interna con el sistema operativo. Servicio de administración de archivo e impresión (transferencia), servicio de conexión a red, servicio de conexión remota y diversas utilidades de Internet.

Direcciones IP

Es el identificador de cada host dentro de su red de redes, cada host conectado a una red tiene una dirección IP asignada, la cual, debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host.

Clasificación

Publicas: direcciones IP públicas son visibles en todo la red de Internet.

Privadas: direcciones IP privadas (reservadas) son visibles únicamente por otros host de su propia red o otras redes privadas interconectadas por routers.

Estáticas: direcciones IP (fijas). Un host que se conecta a la red con dirección IP estática siempre lo hará con una misma IP.

Dinámicas: direcciones IP (dinámica) Un host que conecta a la red mediante dirección IP dinámico, cada vez lo hará con una dirección IP distinta.

Direccionamiento

Las direcciones IP están formadas por 4 bytes (32 bits), que define 3 campos

1. La clase
2. El identificador de red
3. El identificador de la estación

Clases de direcciones

Hay 5 patrones diferentes en uso, cada uno define la clase de dirección IP.

A solo utilizan un byte para identificar la clase y la red y deja 3 bytes disponibles para números de estaciones. Esta división significa que las redes de clase **A** pueden tener más estaciones que las redes **B** y **C** que ofrecen campos de 2 o 3 bits.

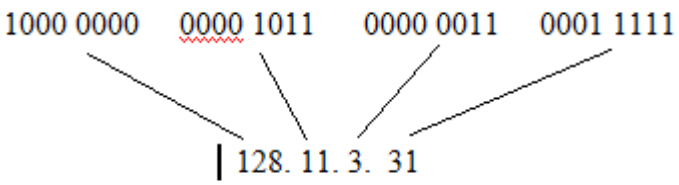
La clase **D** se reserva para direcciones de multienvio.
Las direcciones de clase **E** se han reservado para usos futuros.
La Tabla 2.1 identifica la clasificación y la estructura de las clases de direcciones IP existentes.

Tabla 2.1: Clasificación y Estructura de las Direcciones IP.

	Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Clase A	0 **Identificador de red**	**Identificador de estación**		
Clase B	10 **Identificador de red**		**Identificador de estación**	
Clase C	110 **Identificador de red**			**Identificador de estación**
Clase D	1110 **Direcciones de multienvio**			
Clase E	11110 **Reservada para uso futuro**			

Notación con punto decimal

Para que el formato de 32 bits sea más corto y fácil de leer, las direcciones de Internet se escriben en formato decimal con puntos que separan los bytes.



Al observar el primer byte de una dirección en formato decimal se puede determinar a que clase pertenece la dirección

Tabla 2.2: Clases de direcciones IP. Fuente: Elaboración propia

Clase A	**0.0.0.0**	**127.255.255.255**
Clase B	**128.0.0.0**	**191.255.255.255**
Clase C	**192.0.0.0**	**223.255.255.255**
Clase D	**224.0.0.0**	**239.255.255.255**
Clase E	**240.0.0.0**	**255.255.255.255**

Mascara de red: es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos que parte de la dirección IP es el número de la red, incluyendo la subred y que parte es el host.

Básicamente mediante la mascara de red una computadora podrá saber si debe enviar los datos dentro o fuera de la red.

Router IP: 192.168.1.1

Mascara 255.255.255.0

Rango IP desde 10.0.0.0 hasta

Mascara 10.255.255.255.

.

Se entiende que todo lo que se envia a una IP que empiece por 192.168.1 para la red local y todo l Si todas ellas formaran parte de la misma red su mascara de red seria 255.0.0.0

También se puede escribir 10.0.0.0/8

Mascaras 0,128,192,224,240,248,252,254, y 255

Mascara de subred

Tabla 2.3: Mascaras de subred de cada clase de Direcciones IP. **Elaboración Propia**

Clase	Mascaras de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Ethernet: Las redes LAN usan el estándar Ethernet que emplea el método CSMA/CD (Acceso Múltiple por Detección de Portadora con Detector de Colisiones) que mejora el rendimiento de dicha conectividad. Se trata de un estándar que define no solo las características de los cables que deben utilizarse para establecer una conexión de Red, sino también lo relativo a los niveles físicos de dicha conectividad, además de brindar los formatos necesarios para las tramas de datos de cada nivel. El estándar que rige algunas conexiones Ethernet es el IEEE 802.3.

2.7 ANÁLISIS DEL MODO Y EFECTO DE FALLAS

El Análisis del Modo y Efecto de Fallas, también conocido como AMEF (FMEA por sus siglas en inglés Failure Mode Effect Analysis), es un procedimiento de gran utilidad para aumentar la confiabilidad y buscar soluciones a los problemas que puedan presentar los productos y procesos antes de que estos ocurran.

Permite identificar fallas en productos, procesos y sistemas, así como evaluar y clasificar de manera objetiva sus efectos, causas y elementos de identificación, para de esta forma, evitar su ocurrencia y tener un método documentado de prevención. Por lo tanto, el AMEF puede ser considerado como un método analítico estandarizado para detectar y eliminar problemas de forma sistemática y total, cuyos objetivos principales son:

- Reconocer y evaluar los modos de fallas potenciales y las causas asociadas con el diseño y manufactura de un producto.
- Determinar los efectos de las fallas potenciales en el desempeño del sistema.
- Identificar las acciones que podrán eliminar o reducir la oportunidad de que ocurra la falla potencial.
- Analizar la confiabilidad del sistema.
- Documentar el proceso

Es aplicable para la detección y bloqueo de las causas de fallas potenciales en productos y procesos de cualquier clase de empresa, así como también es aplicable para sistemas administrativos y de servicios.

Requerimientos del AMEF

Para hacer un AMEF se requiere lo siguiente:

- Un equipo de personas con el compromiso de mejorar la capacidad de diseño para satisfacer las necesidades del cliente.
- Diagramas esquemáticos y de bloque de cada nivel del sistema.
- Especificaciones de los componentes.
- Especificaciones funcionales de módulos.
- Requerimientos de manufactura y detalles de los procesos que se van a utilizar.

Los Beneficios de implantación de AMEF en un sistema son:

- Identifica fallas o defectos antes de que estos ocurran.
- Incrementar la confiabilidad del servicio
- Procesos de desarrollo mas cortos
- Documenta los conocimientos sobre los procesos
- Incrementa la satisfacción del cliente
- Mantiene el Know-How en la compañía.

Antes de iniciar una detección de fallas, se enfoca el procedimiento en estudiar la evidencia, realizar preguntas específicas acerca del sistema, de los equipos, de las características de posibles fallas, de acontecimientos relacionados de la falla, se toman notas de las respuestas. No se destruyen evidencias y luego de unir al personal involucrado se discute el problema, frecuencia de las fallas, secuencia de eventos que preexistieron a la falla, entre otras [7].

Cuando hay una Falla?

Existen causas comunes en las que se puede enfocar la búsqueda, entre ellas están:

1. Mal diseño del sistema, selección del material sin tomar en cuenta condiciones de operación del equipo.
2. Imperfecciones del material, del proceso y/o de su fabricación.
3. Errores en el servicio de mantenimiento, instalación y/u operación del sistema al momento de realizar el montaje.

Curva de la bañera: Es un gráfica que representa los fallos durante el período de vida útil de un sistema o máquina. Se llama así porque tiene la forma de una bañera cortada a lo largo. Está basada en las siguientes etapas mostrada en la figura 2.7 :

Fallos iníciales: Esta etapa se caracteriza por tener una elevada tasa de fallos que desciende rápidamente con el tiempo.

Fallos normales: Etapa con una tasa de errores menor y constante. Los fallos no se producen debido a causas inherentes al equipo, sino por causas aleatorias externas.

Fallos de desgaste: Etapa caracterizada por una tasa de errores rápidamente creciente

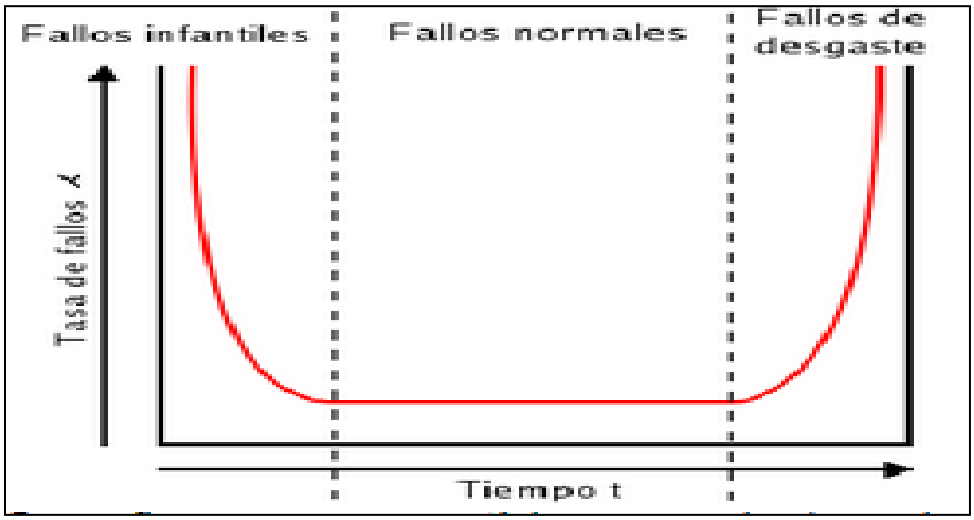


Figura 2.7: Curva de la Bañera**. Fuente: Elaboración Propia basada en [7]**

Asignación del grado de Severidad

Cuando se determinan las fallas se procede a calificar la severidad, es decir, la gravedad de los efectos potenciales. Para estimar el grado de severidad, se debe de tomar en cuenta el efecto de la falla en el sistema. Se utiliza una escala del 1 al 10: el '**1**' indica una consecuencia sin efecto y el "**10**" indica una consecuencia grave, tal como lo indica la tabla 2.4.

Tabla 2.4. Criterio de severidad.

CALIFICACION		CRITERIO DE SEVERIDAD
EFECTO	**RANGO**	
NO	**1**	Sin efecto perceptible
MUY POCO	**2**	Poco efecto en el desempeño del Sistema o dispositivo. Defecto notado por el 1 por ciento de los clientes.
POCO	**3**	Poco efecto en el desempeño del Sistema o dispositivo. Defecto notado por el 5 por ciento de los clientes.
MENOR	**4**	Efecto menor en el desempeño del Sistema o dispositivo. Defecto notable
MODERADO	**5**	Efecto moderado en el desempeño del Sistema o dispositivo
SIGNIFICATIVO	**6**	El desempeño del Sistema o dispositivo, se ve afectado pero es operable y esta a salvo. Falla parcial pero operable.
MAYOR	**7**	El desempeño del Sistema o dispositivo se ve seriamente afectado, pero es funcional y esta a salvo. Sistema afectado
EXTREMO	**8**	Equipo inoperable pero a salvo. Sistema inoperable
SERIO	**9**	Se cumple con normas de riesgo. Sistema o dispositivo inoperable.
PELIGRO	**10**	Falla repentina. Se incumple con normas de riesgo. Efecto peligroso.

Asignación de una Ocurrencia

Las causas son evaluadas en términos de ocurrencia, ésta se define como la probabilidad de que una causa en particular acontezca y resulte en un modo de falla durante el lapso esperado del sistema instalado, es decir, representa la remota probabilidad de que el sistema perciba el efecto del modo de falla, tal como lo indica la tabla 2.5.

Tabla 2.5: Criterio de Ocurrencia.

Calificación		**CRITERIO DE OCURRENCIA**
Ocurrencia	**Rango**	
Remota	**1**	Falla improbable. No existen fallas relacionadas con este proceso
Muy Poca	**2**	Solo fallas aisladas asociadas
Poca	**3**	Fallas aisladas asociadas
Moderada	**4**	Fallas ocasionales
Alta	**5**	Han fallado a menudo
Muy Alta	**6**	Siempre falla

Asignación de un Valor de Detección

La detección es una evaluación de las posibilidades de que los controles del proceso propuestos detecten el modo de falla. Al detectar y evaluar se describe el tipo de control que se tiene para detectar cada falla. Además se evalúa la clasificación en una escala del 1 al 10, la capacidad de detección de la misma. Entre mayor sea la posibilidad de detectar la falla, menor será la calificación, así como se indica la tabla 2.6.

Tabla 2.6 Criterio de Detección.

Probabilidad	Rango	CRITERIO DE DETECCIÓN
Alta	**1**	El defecto es una característica funcionalmente obvia
Medianamente Alta	**2-5**	Es muy probable detectar la falla
Baja	**6-8**	El defecto es una característica fácilmente identificable
Muy Baja	**9**	No es fácil detectar la falla por métodos usuales o pruebas manuales
Improbable	**10**	No se puede determinar la falla fácilmente.

Calculo del RPN

El Número de Prioridad de Riesgo (RPN, del ingles Risk Priority Number) para cada falla y tomar decisiones. Este valor que establece una jerarquización de los problemas a través de la multiplicación del grado de ocurrencia, severidad y detección. El RPN provee la prioridad con la que debe de atacarse cada modo de falla, identificando ítems críticos.

El RPN es un número entre 1 y 600 que nos indica la prioridad que se le debe dar a cada falla para eliminarla. Cuando el RPN es superior a 60 es un claro indicador de que deben implementarse acciones de prevención o corrección para evitar la ocurrencia de fallas, de forma prioritaria.

RPN= Ocurrencia * Severidad * Detección

Prioridad de NPR:

541 - 600 Riesgo de falla MUY ALTO
481- 540 Riesgo de falla ALTO
301 - 480 Riesgo de falla MEDIO
61 - 300 Riesgo de falla BAJO
1 - 60 Riesgo de falla MUY BAJO

CAPITULO III

3. El Sistema Biométrico

El Sistema Biométrico de la Empresa Conviasa esta basado en una red WAN (red de área amplia, en inglés, Wide Area Network), es una red de computadoras que une varias redes locales, aunque sus miembros no están todos en una misma ubicación física, establecida principalmente en la sede de Maiquetía desde donde se administra el sistema. El Servidor del Sistema Biométrico, esta configurado como una maquina virtual en el equipo, el cual tiene aplicaciones propias de la Empresa y se conecta con los equipos biométricos por medio del protocolo TCP/IP. Desde otra maquina configurada como cliente, se permite realizar pruebas de conexión de todos los dispositivos biométricos pertenecientes al Sistema y la configuración de nuevos equipos para su instalación, además de realizar pruebas de funcionamiento de equipos con fallas.

Para realizar la conexión en el Sistema Biométrico desde la maquina cliente con otras estaciones del interior del país utilizan VPN **(**Red Privada Virtual, de sus siglas en inglés, Virtual Private Network*)* este enlace es proporcionado por la empresa privada CANTV (acrónimo de Compañía Anónima Nacional Teléfonos de Venezuela), así como se observa en la figura 3.1. La red VPN permite crear una conexión segura a otra red a través del Internet. Cuando se conecta cualquier dispositivo a una red VPN, este actúa como si estuviese en la misma red que la que tiene la VPN y todo el tráfico de datos se envía de forma segura a través de la red VPN.

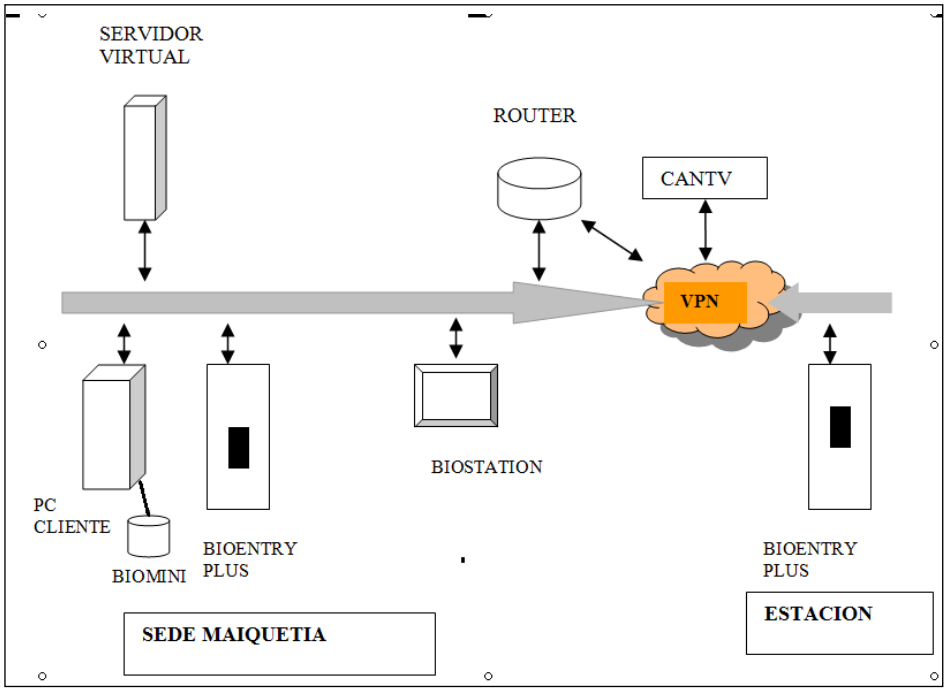


Figura 3.1. Enlace VPN entre sede Maiquetía y estación remota. **Fuente: Elaboración Propia**

Si se toma como base la Guía del Administrador BioStar 1.8 [8], se pueden extraer una serie de pasos para realizar la instalación del programa BioStar, es un proceso bastante sencillo, aunque es necesario cumplir con algunos requisitos antes de iniciar la instalación:

- En primer lugar, es necesario elegir una PC que pueda permanecer conectada de forma constante y que pueda funcionar como el servidor BioStar. El servidor recibirá y almacenará los datos de registro de los dispositivos conectados en tiempo real.
- En segundo lugar, es necesario elegir el tipo de base de datos que se va a utilizar. El servidor BioStar es compatible tanto con MySQL o MS SQL Server (incluyendo las versiones inferiores, como la base de datos gratuita MS SQL Server Express). En la red Biométrica se utiliza el tipo de base de datos MySQL.
- En tercer lugar, las computadoras que se utilizan para el programa Servidor o Cliente cumplen con los requerimientos mínimos para su instalación.

3.1 Requisitos del Sistema para instalación del Servidor BioStar

La *Guía de Instalación del Software BioStar* [10] permitió la instalación del software BioStar el cual, necesito de ciertos requisitos:

BioStar es compatible con los siguientes sistemas operativos

Windows 8 (sistemas de 32-bits y 64-bits)

Windows 7 (plataformas de 32-bit or 64-bits)

Windows Server 2008 R2

Windows Vista

Windows XP, Service Pack 1 o posteriores (sólo versiones de 32 bits)

Windows Server 2003

Windows 2000, Service Pack 4 o posteriores

Los requisitos mínimos del sistema para instalar y utilizar el software BioStar son los siguientes:

CPU: Intel Pentium o procesador similar capaz de procesar velocidades superiores

RAM: 512 MB

HDD: 5 GB

Sin embargo, Suprema Inc. recomienda la siguiente configuración de hardware para un rendimiento óptimo:

CPU: Intel Pentium Dual Core o procesador similar capaz de procesar velocidades de 2GHz o superiores.

RAM: 1 GB para Windows XP; 2 GB para otros sistemas operativos

HDD: 10 GB

3.2 El Servidor Virtual

En la actualidad el Sistema Biométrico se administra, por medio del Software BioStar instalado en un Servidor el cual contiene distintas aplicaciones y maquinas virtuales con distintos sistemas operativos. La maquina virtual con sistema operativo Windows Server 2008, esta configurada con el BioStar versión 1.8, el cual es un programa cliente-servidor que permite máximo 2 clientes con la versión gratuita y hasta 32 clientes con licencia. Una configuración típica esta formada por muchos dispositivos de control de acceso conectado a un servidor central mediante una conexión Ethernet.

El Software BioStar 1.8 es compatible tanto con MS SQL Server o con MySQL. La base de datos utilizada es MySQL y se cuenta con suficiente derechos y privilegios de acceso para conectarse a la base de datos y crear nuevas tablas.

El instalador Express instalará los siguientes componentes en el Servidor BioStar:

MS SQL Server Express: Admite la base de datos
Programa cliente-servidor BioStar

3.3 Funciones de Control de Acceso

Para la autenticación de usuario los dispositivos de control de acceso BioEntry Plus y Biostation incorpora un avanzado algoritmo de reconocimiento de huellas dactilares para ofrecer un control de acceso seguro. El Sistema Biométrico combina la identificación mediante huella dactilar y la identificación de usuario (solamente en los dispositivos Biostation). Por otra parte, los dispositivos BioEntry Plus disponen de la lectura de una huella dactilar de forma exclusiva.

El Software BioStar permite manejar toda la estructura a nivel de conexión de dispositivos biométricos instalados en las puertas de las oficinas administrativas o áreas comunes de libre acceso. Además de administrar a los usuarios de la base de datos para crear los distintos accesos a los grupos formados dentro de la empresa. Las siguientes gestiones enmarcan las principales funciones que se realizan con la base de datos que usa el Software BioStar.

- Gestión de usuarios
- Gestión del grupo de acceso
- Gestión de dispositivos
- Gestión de puertas

En el Apéndice B se indica las gestiones utilizadas para el control de acceso.

3.4 Administración del Sistema Biométrico

Para administrar la red biométrica se utiliza el Software BioStar versión 1.8 y el BioStar Server Config. El Software BioStar 1.8 (Figura 3.2), admite ingresar a la base de datos y realizar funciones de control de acceso, por medio de las gestiones de usuarios, puertas, dispositivos y creación de grupos de acceso. Maneja un nombre de usuario y una contraseña para el acceso al Sistema Biométrico (figura 3.3), aunque la versión gratuita tiene sus limitantes debido a que solo permite dos usuarios conectados. Mientras que el Software BioStar Server Config, permite realizar un monitoreo en tiempo real actualizado de cada dispositivo conectado, el cual debe estar configurado con una IP asignada por el Departamento de Redes.

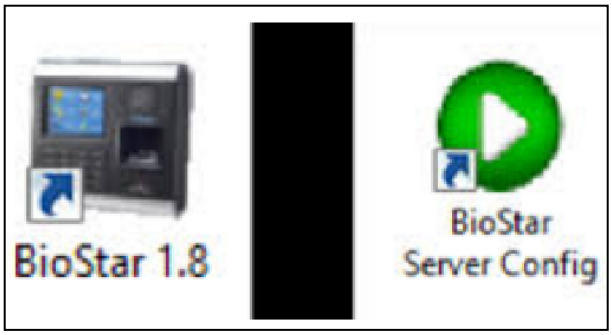


Figura 3.2. Logos del software BioStar versión 1.8 y el Software BioStar Server Config. **Fuente: Elaboración Propia basada en Guía de Administración BioStar [9].**

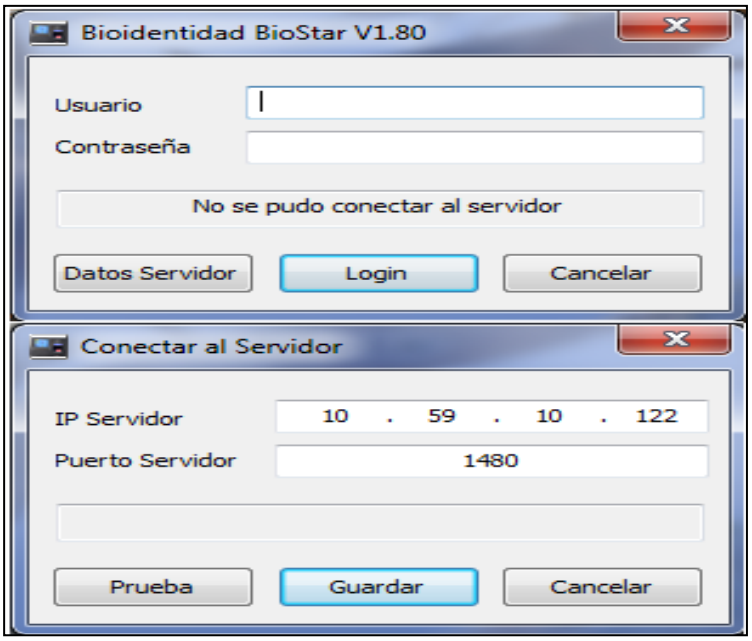


Figura 3.3. El nombre Usuario y la contraseña para el acceso al Sistema Biométrico, además de colocar la dirección IP del Servidor BioStar y su puerto. **Fuente: Elaboración Propia basada en Guía de Administración BioStar [8].**

El Software BioStar Server Config, permite realizar un monitoreo en tiempo real actualizado de cada dispositivo conectado, el cual debe estar configurado con una IP asignada. Muestra el estado de la conexión, el puerto y clientes activos. Además de la base de datos, tipo de base de datos y autenticación de Windows. En el apéndice E esta el contenido para detallar el estado del servidor y la forma de configurar el adaptador de red con la IP asignada.

En la siguiente figura 3.4 se observan todas las conexiones con los dispositivos que se manejan en el Sistema Biométrico. El servidor principal, el computador configurado como cliente para administrar el sistema, el Biomini para la recolección de huellas dactilares, el BioStation y el BioEntry Plus, conectados con cable UTP, topología ethernet, bajo la distribución del cableado estructurado para transmisión de datos en la red WAN y LAN (menos el Biomini que usa cable USB)

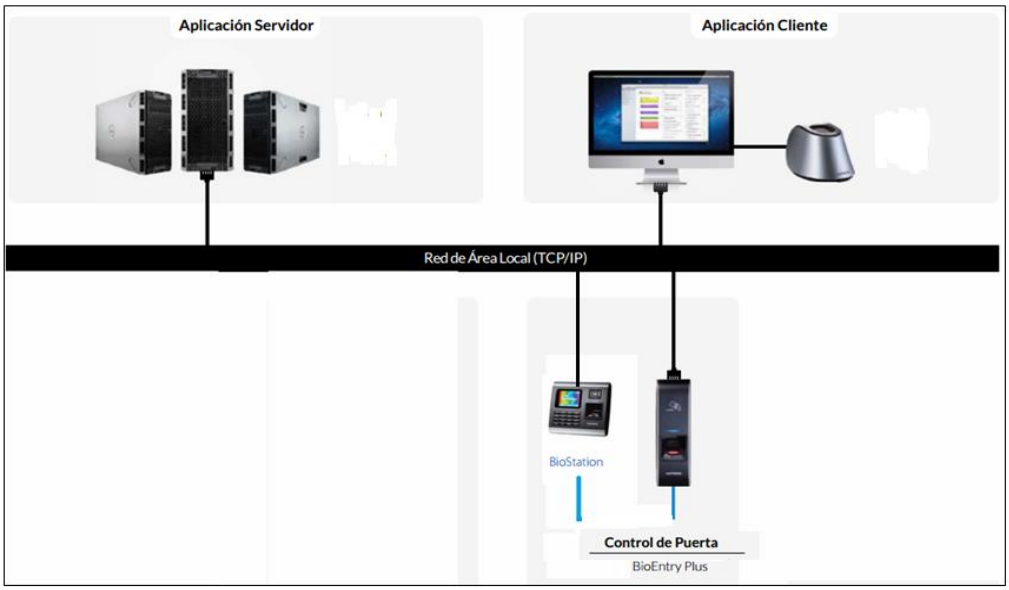


Figura 3.4 Conexiones de los dispositivos del Sistema Biométrico.

3.5 El Software BioStar

Es el sistema de control de acceso de última generación de Suprema Inc., basado en conectividad IP y en seguridad biométrica. La mayoría de los dispositivos que desarrolla están basados en escáneres de huellas y lectores de tarjetas para múltiples niveles de autentificación de usuario. Sin embargo, los dispositivos biométricos de Suprema Inc., funcionan no sólo como escáneres de huellas dactilares, sino también como controladores de acceso inteligente. La edición estándar con licencia de BioStar se desbloquea con una llave USB. Sin la llave, BioStar funciona como una versión gratuita con capacidad limitada. Con la llave, BioStar ofrece mayor versatilidad y funciones adicionales, tal y como se muestra en la siguiente tabla 3.1:

Tabla 3.1. Funciones de BioStar. Fuente: Elaboración Propia basada en Guía de Administración BioStar [8].

	Edición estándar	Versión gratuita
# máximo de puertas	512	20
# máximo de clientes	32	2
Soporte de zona	Sí	No
Notificaciones por e-mail	Sí	No
Identificación de servidor	Sí	No
Tipos de turnos	Diarios y semanales	Sólo semanales
Placa de entradas/salidas (I/O)	Sí	No
Mapa visual	Sí	No

3.5.1 Especificaciones del Software BioStar

El Software BioStar es un sistema de inteligencia distribuida. En lugar de los complejos controles cableados y centralizados que los sistemas de control de acceso convencionales necesitan, los dispositivos de control de acceso de Suprema Inc. se pueden conectar mediante TCP/IP o sin cables a una red de área local o también se pueden conectar mediante conexiones en serie. La información de usuario, las normas de acceso y cualquier otra información se pueden distribuir a cada uno de los dispositivos para acelerar el tiempo de autorización y ofrecer un funcionamiento continuo aún incluso cuando se haya perdido la conexión a la red.

El Software BioStar es un programa Servidor-Cliente, en general, permite un máximo de 512 puertas y 512 dispositivos (20 puertas y dispositivos en la versión gratuita).

El apéndice C detalla el software BioStar usado como servidor y cliente.

3.5.2 Autentificación de usuario

Los dispositivos biométricos son privilegiados por algoritmos de reconocimiento de huellas dactilares para ofrecer un control de acceso seguro. El único método utilizado en la empresa Conviasa para acceder en las puertas es la autentificación mediante *la lectura de la huella dactilar*. El Software BioStar almacena dos plantillas para cada huella dactilar y hasta dos huellas dactilares por usuario (cuatro plantillas en total).

En la actualidad la Empresa Conviasa usa la licencia gratuita, aunque es requerida la licencia original con llave USB del Software BioStar, la cual permitiría obtener otras ventajas que obviamente no ofrece una versión gratuita, la siguiente tabla 3.2 muestra estos beneficios, los cuales son una comparación entre las dos licencias.

Tabla 3.2. Comparación entre las Licencias del Software BioStar. **Fuente: Elaboración Propia basada en Guía de Especificaciones del Software BioStar [10]**

		BioStar BE	**BioStar SE**
Sistema	**Licencia**	Gratis	
	Arquitectura del Sistema	Software del Sistema	Software del Sistema
	Sistema Operativo	Windows	Windows
	Base de datos	MSSQL, MySQL, Oracle	MSSQL, MySQL, Oracle
	Comparación en Servidor	N/A	Sí
	Máximo Dispositivos	20	512
Control de Acceso	**Clientes concurrentes en PC**	2	32
	Calendario de tiempo	128	
	Grupo de Acceso /Nivel	128	
	Máximo Grupo de Acceso por Usuario	4	
	Puerta	20	512
	Plantilla en tarjeta	Sí	
	Zona	N/A	Antipassback, Limite de Entrada, Alarma, Acceso, Alarma de Incendio, Muster
	Notificación por E-mail	N/A	Sí
	Pase de Lista	N/A	Sí
	Mapa Visual	N/A	Sí
	Monitoreo de Evento	Sí	
	Camara IP	N/A	Sí
	Integración NVR	N/A	Sí
Control de Asistencia	**Administración de Elevadores**	N/A	Sí (Hasta 120 pisos)
	Cálculo de Tiempo Trabajado	Sí	
	Administración de Turnos	Semanal	Diario/Semanal
	Administración de Días Festivo/Ausencias	Sí	
	Reportes	Sí	
	Tablero Entrada / Salida	Sí	Sí

3.6 Configuraciones de los dispositivos del Sistema Biométrico

Los dispositivos BioEntry Plus conectados en la figura 3.5, requieren para su instalación configurarse por separado y luego unirlos dentro del Sistema Biométrico, a través de la distribución de cableado estructurado por toda la red LAN de la Empresa.

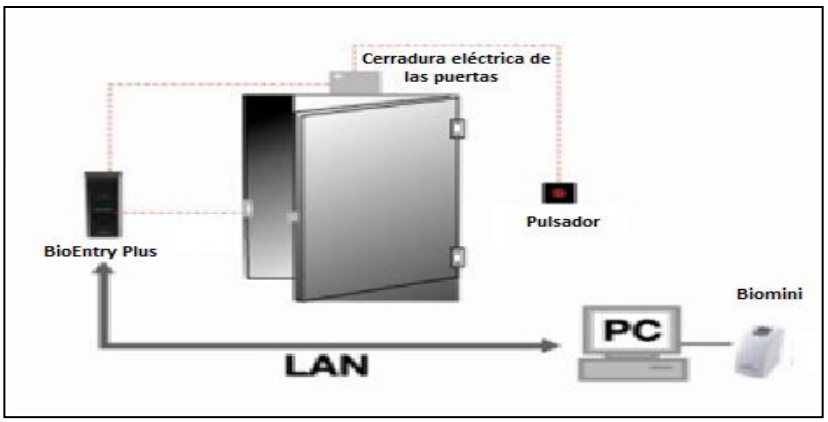


Figura 3.5: Dispositivos del Sistema Biométrico**. Fuente: Elaboración Propia basada en Guía de Administración BioStar [8].**

Los dispositivos biométricos que captan la huella dactilar como el BioEntry Plus y el Biostation son para control de acceso y se configuran con el Software BioStar 1.8. Se añaden al servidor y se almacenan los datos requeridos del personal, para acceder a las instalaciones por las puertas aseguradas con el equipo biométrico.

El accesorio Biomini, solo requiere de un driver de instalación en la PC configurada en la red biométrica como cliente y que a su vez, la utilice el personal autorizado para realizar el almacenamiento de las huellas dactilares del personal de la empresa. Este software permite el reconocimiento del accesorio Biomini al momento de realizar la captación de las huellas dactilares del personal y que realice su operación de cambio de huella dactilar a plantilla digital de datos. Es utilizado por el personal del Departamento de Recursos Humanos para ingresar al nuevo personal y por el departamento de OTI para asignar los accesos permitidos.

3.7 Modelo BioEntry Plus

El modelo BioEntry Plus es un dispositivo de control de acceso basado en IP (Protocolo Internet, de sus siglas en ingles, Internet Protocol) que incluye tanto reconocimiento de huellas dactilares como entrada mediante una tarjeta de acceso. El dispositivo de la figura 3.6 se puede controlar de mediante la interfaz de El Software BioStar. El BioEntry Plus se puede conectar a cerraduras eléctricas para puertas mediante un relay interno.

Figura 3.6. Dispositivo Modelo BioEntry Plus. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

La tabla 3.3 muestra los modelos de BioEntry Plus, el apéndice D muestra los tipos de sensores que escanean la huella dactilar y las especificaciones del dispositivo

Tabla 3.3 Tipos de BioEntry Plus. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

Modelo	**BioEntry**	**V(v)**	**I(A)**
BEPH-OC	HID	12	1.5
BEP- (B)		12	1.0
BEPL- (OC)	EM	12	1.0

3.7.1 Conexión del Modelo Bioentry Plus

El manual de referencia para la instalación del biométrico indica las instrucciones y el contenido básico para la conexión del Dispositivo BioEntry Plus en la pared, el soporte, los tornillos, la llave allen de ajuste y los 4 cables adaptadores con sus pines característicos, tal como se muestra en la figura 3.7.

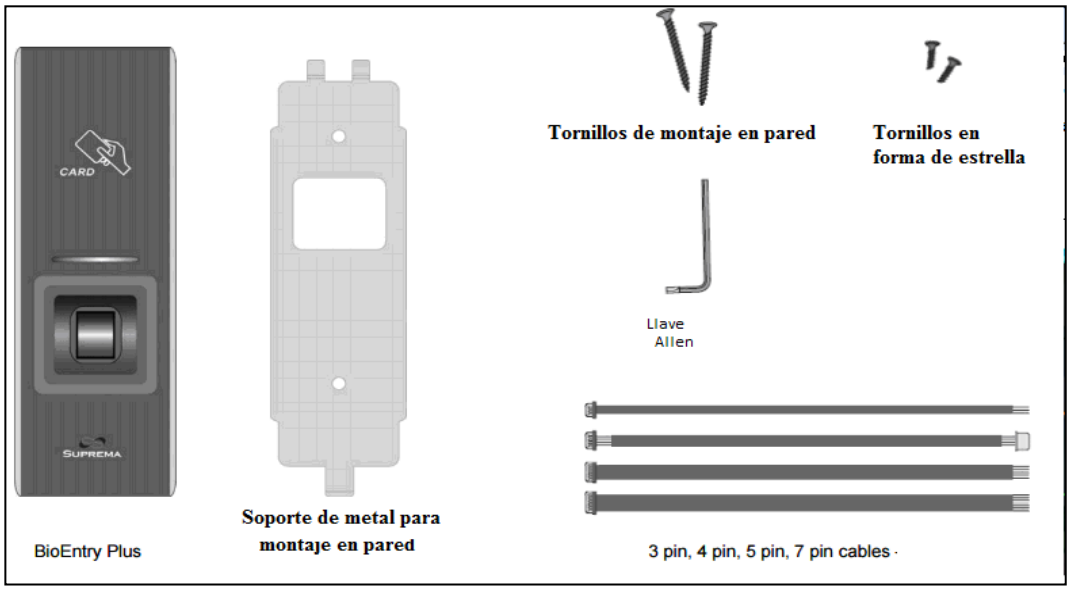


Figura 3.7: Contenido básico para la instalación en la pared. Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].

3.7.2 Cables y adaptadores del Modelo BioEntry Plus

El modelo BioEntry Plus utiliza 4 tipos de adaptadores distintos. Requiere de la alimentación eléctrica, adaptador para la conexión de red, adaptador de la salida del relé para la puerta, la figura 3.8 muestra los conectores usados.

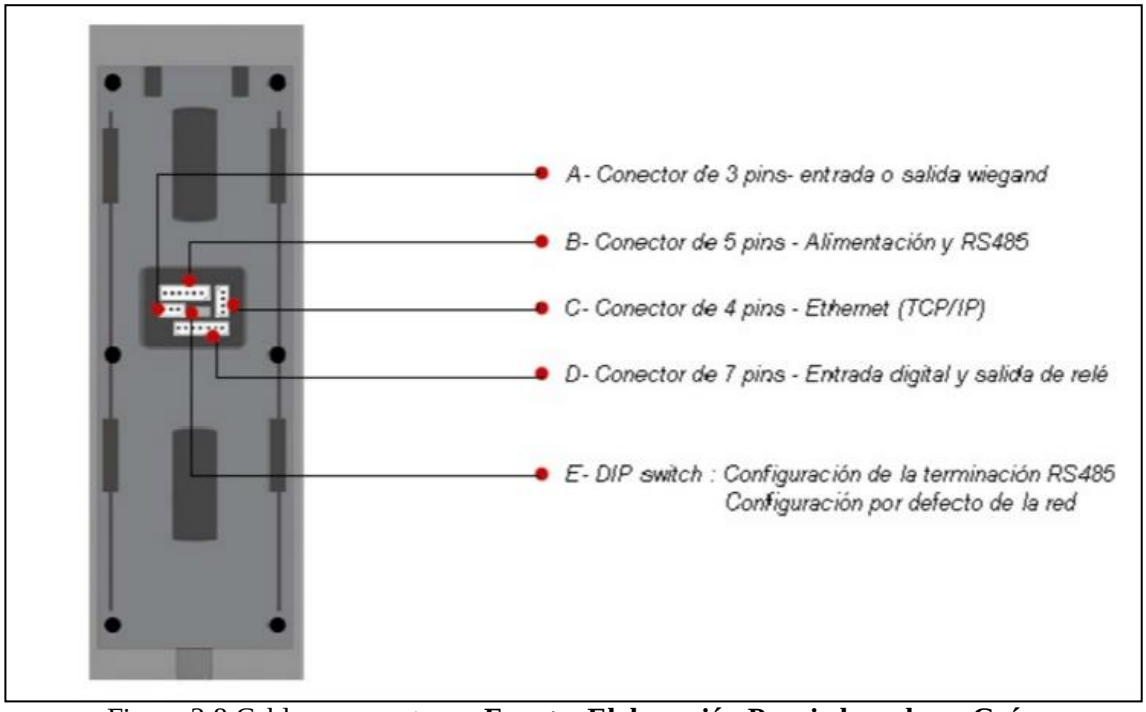
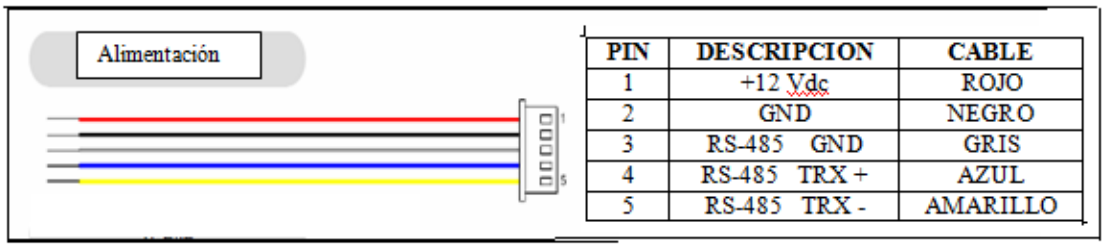


Figura 3.8 Cables y conectores. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

La figura 3.9 muestra los colores de los cables, la simbología eléctrica para la respectiva conexión del adaptador que suministra el fabricante, esta alimentación eléctrica es de 12 V DC. Este adaptador también posee la conexión RS-485

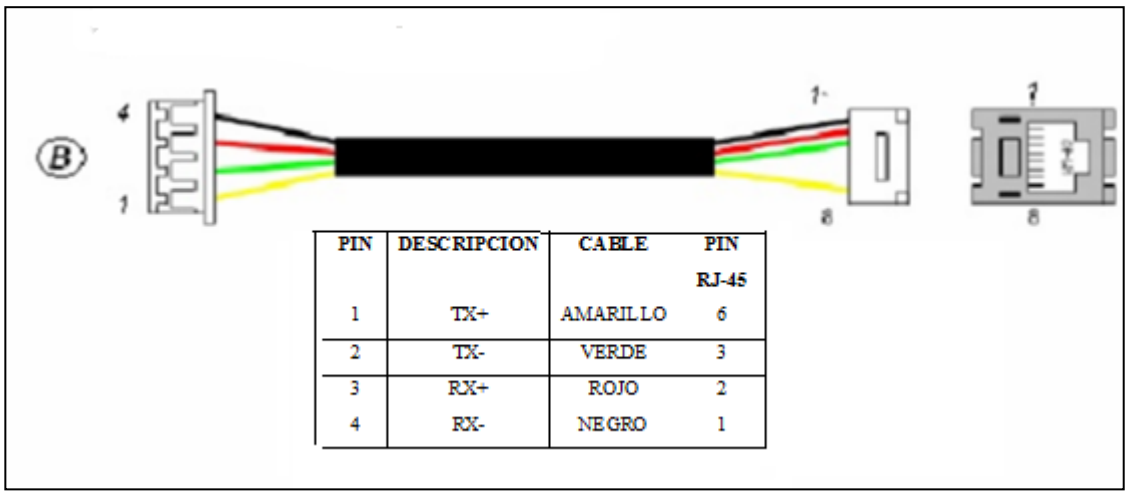


PIN	DESCRIPCION	CABLE
1	+12 Vdc	ROJO
2	GND	NEGRO
3	RS-485 GND	GRIS
4	RS-485 TRX +	AZUL
5	RS-485 TRX -	AMARILLO

Figura 3.9. Alimentación y conexión RS-485. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

3.7.3 Conexión del BioEntry Plus para la Comunicación TCP/IP

En el dispositivo BioEntry Plus se realiza la conexión TCP/IP por medio del cable con adaptador RJ-45 hacia la red LAN transmite bajo el estándar Ethernet, también conocido como estándar IEEE 802.3, permite transmitir datos para redes de área local como se muestran en las figuras 3.10 y 3.11. Emplea el método CSMA/CD (Acceso Múltiple por Detección de Portadora con Detector de Colisiones) que mejora notoriamente el rendimiento de dicha conectividad.



PIN	DESCRIPCION	CABLE	PIN RJ-45
1	TX+	AMARILLO	6
2	TX-	VERDE	3
3	RX+	ROJO	2
4	RX-	NEGRO	1

Figura 3.10. Cable desde el dispositivo biométrico hacia el adaptador RJ-4. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

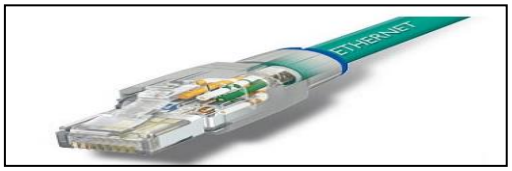


Figura 3.11. Cable y adaptador RJ-45 hacia red LAN.

Al realizar la conexión del cable UTP desde el equipo de biométrico hacia el servidor, se consigue la plataforma del cableado estructurado durante el trayecto, los cuales se muestra en la figura 3.12 equipos de comunicación, como son switches, routers y topología de red.

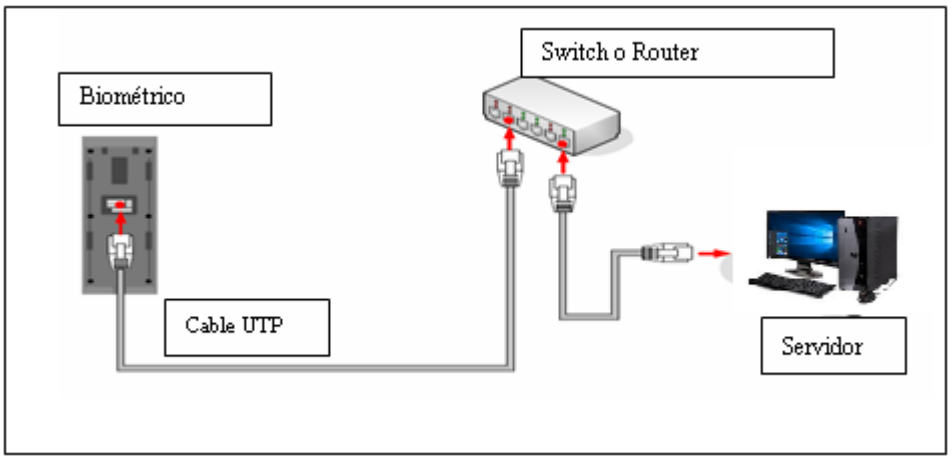


Figura 3.12: Cableado desde el dispositivo biométrico hasta el servidor.

Cuando se utiliza el software Biostar para configurar los dispositivos biométricos, se realiza directamente conectando la PC y el dispositivo solo por cable UTP, como se indica en la figura 3.13 también se realiza el almacenamiento de huella dactilar y clasificación del tipo de acceso que se requiere en los biométricos.

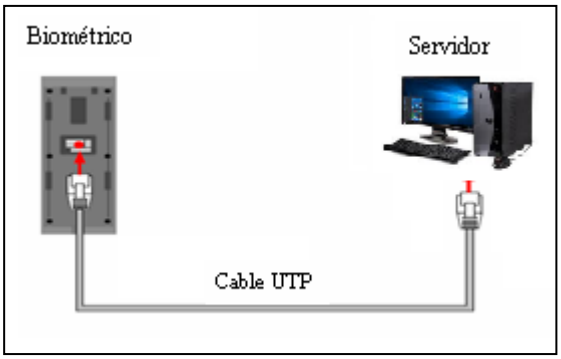


Figura 3.13: Cableado UTP desde el dispositivo biométrico hasta el servidor.

3.7.4 Conexión de Entrada digital y salida del relé

Este cable se utiliza para realizar la conexión del dispositivo biométrico con las puertas, tanto la cerradura de hembrilla como la cerradura magnética, además del cableado que requiere el pulsador para habilitar dichas puertas cuando el personal no tiene el acceso permitido en esas zonas, tal como se indica en la figura 3.14.

Figura 3.14: Adaptador desde el dispositivo biométrico hasta el adaptador de red. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

La siguiente tabla 3.4 especifica los pines del cable del relé con su respectiva descripción y el color usado para cada conexión. Los pines 1 y 2 se usan para la conexión del pulsador no requiere energizarse. Los pines usados para la conexión de las cerraduras serán: pines 5 y 6 cerradura magnética y pines 7 y 6 cerradura de hembrilla, requieren de alimentación eléctrica cada una. Por otra parte, presentan distintas características de funcionamiento eléctrico y por tanto difieren en sus conexiones.

Tabla 3.4: Descripción del cable de conexión de entrada digital y salida de relé. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

PIN	DESCRIPCION	COLOR
1	ENTRADA SW1	AMARILLO
2	GND SW1	NEGRO
3	ENTRADA SW2	VERDE
4	GND SW2	NEGRO
5	RELE NORMALMENTE CERRADO	NARANJA
6	RELE COMUN	AZUL
7	RELE NORMALMENTE ABIERTO	BLANCO

3.7.5 DIP Switch para la configuración del Dispositivo Bioentry Plus

Para efectuar la instalación del equipo BioEntry Plus (TCP / IP) se requiere configurarlo previamente, se utiliza el software BioStar y el cambio de los pines del DIP Switch. El operador puede borrar toda la información contenida en el equipo mediante los pines del Dip Switch del panel posterior del equipo, la figura 3.15, ejemplifica el modo para cambiar dichos pines y llevarlo a modo fabrica.

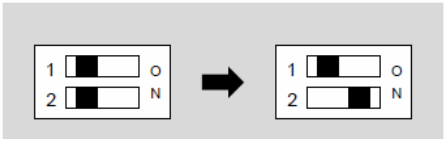


Figura 3.15: Posición del Dip Switch : Modo Fabrica. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

En este cambio se debe realizar los siguientes pasos:

1. Se apaga la alimentación de BioEntry Plus.
2. Se coloca el interruptor DIP SW # 2 en "ON" (ver la figura 3.15)
3. Se enciende el BioEntry Plus y es posible modificar la dirección de red TCP / IP o RS-485 por medio del software Biostar.

Se efectúa la configuración del equipo con lo requerido, dirección IP, la gestión de acceso a las puertas, la gestión para agregar usuarios, entre otros.

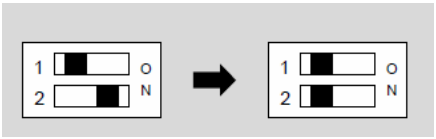


Figura 3.16. Posición del Dip Switch: Modo Configurado. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

4. Se modifica la dirección TCP / IP o RS-485 y se guarda.
5. Se coloca el DIP SW # 2 en la posición "OFF" (Ver la Figura 3.16)
6. Se comprueba la dirección TCP / IP o RS-485 modificada.

La dirección IP: 192.168.0.1 es la predeterminada del equipo biométrico BioEntry Plus.

3.8 Modelo Biostation

Es una terminal multifuncional con un teclado numérico y una pantalla LCD en color de 2.5 pulgadas que permite registrar usuarios y gestionar funciones directamente desde el dispositivo (figura 3.17). Biostation se conecta a la red LAN e incluye una entrada USB e interfaz de dispositivos para facilitar la transferencia de datos.

Figura 3.17: Modelo Biostation. Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico Biostation Plus [12].

El apéndice E muestra los tipos de sensores que escanean la huella dactilar y las especificaciones del dispositivo.

3.9 BioMini

Es un escáner dactilar de altas prestaciones con comunicación USB, para aplicaciones de validación dactilar y seguridad en entornos basados en computadoras PC, servidores y redes. Compara 100.000 huellas en 1 segundo (velocidad basada en procesador Core 2). Tiene un diseño elegante y estable, combinado por un sensor óptico durable y de alta calidad, tal como se muestra en la figura 3.18. La instalación del dispositivo es simple: se conecta a un puerto USB de cualquier computadora que se encuentre conectada al servidor BioStar y se instala el controlador.

a) **b)**

Figura 3.18:a) BioMini y b) el Lector Óptico. **Fuente: Elaboración Propia basada en Guía de Configuración del dispositivo biométrico Biostation Plus [13].**

En el Apéndice F se detallan los beneficios, las especificaciones, las aplicaciones, y el algoritmo utilizado para identificación de huellas dactilares es estos escáneres.

3.10. Características de las Instalaciones de los dispositivos Biométricos.

Los modelos BioEntry Plus y el Bioestation requieren de una instalación basada en el siguiente diagrama esquemático de la figura 3.19, donde se señalan las distintas conexiones de alimentación, de red y la de la puerta de acceso (que contiene la cerradura eléctrica con el circuito del pulsador).

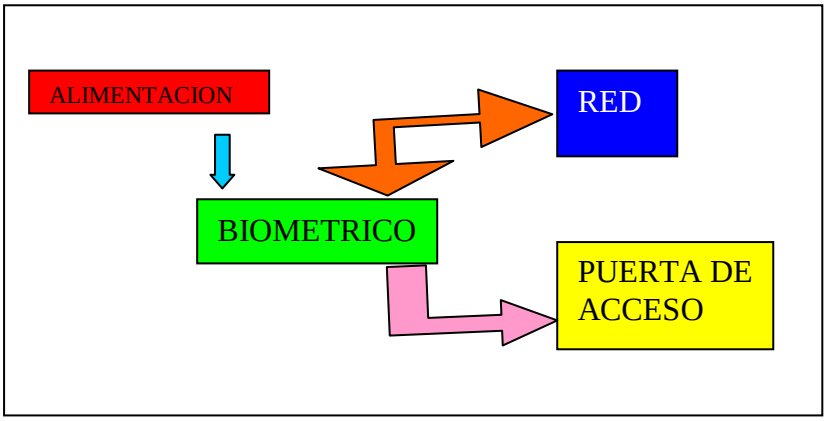


Figura 3.19: Diagrama Esquemático para la Instalación de los dispositivos Biométricos.

Los equipos biométricos usados (BioEntry Plus y Biostation) por el Sistema difieren en las conexiones de la instalación del cable de red, así como en la conexión de los cables del relé de salida. Por otra parte la conexión de red LAN con cable UTP, bajo la norma Ethernet y cableado estructurado permiten la instalación de estos dispositivos.

3.10.1 Instalación para la alimentación eléctrica

Requiere de una canalización eléctrica para lograr instalar una toma de corriente que permite alimentar el adaptador AC-DC de los dispositivos BioEntrry Plus y Biostation, lo muestra la figura 3.20.

Figura 3.20. Adaptador de alimentación. Fuente: Guía de Configuración del dispositivo biométrico BioEntry Plus [9].

La alimentación es realizada con las especificaciones del adaptador de la siguiente figura 3.21

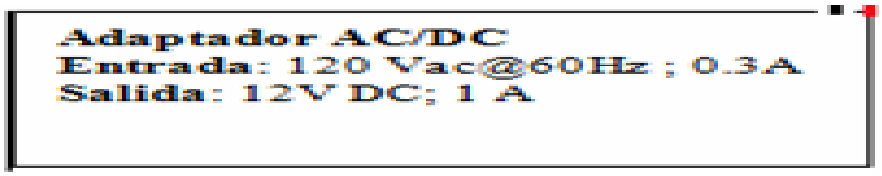


Figura 3.21: Especificaciones del adaptador.

Todos los modelos biométricos del Sistema utilizan este adaptador, para el encendido del equipo y utilizan su conector especial del fabricante. Tal como se

indica en la figura 3.21, una vez encendido realiza una rutina de escaneo de funcionamiento, que se observa al cambiar su iluminación frontal. El conector contiene 5 cables aunque los utilizados para la alimentación son el rojo y negro. Los otros 3 cables se usan para conexiones no utilizadas dentro del Sistema Biométrico.

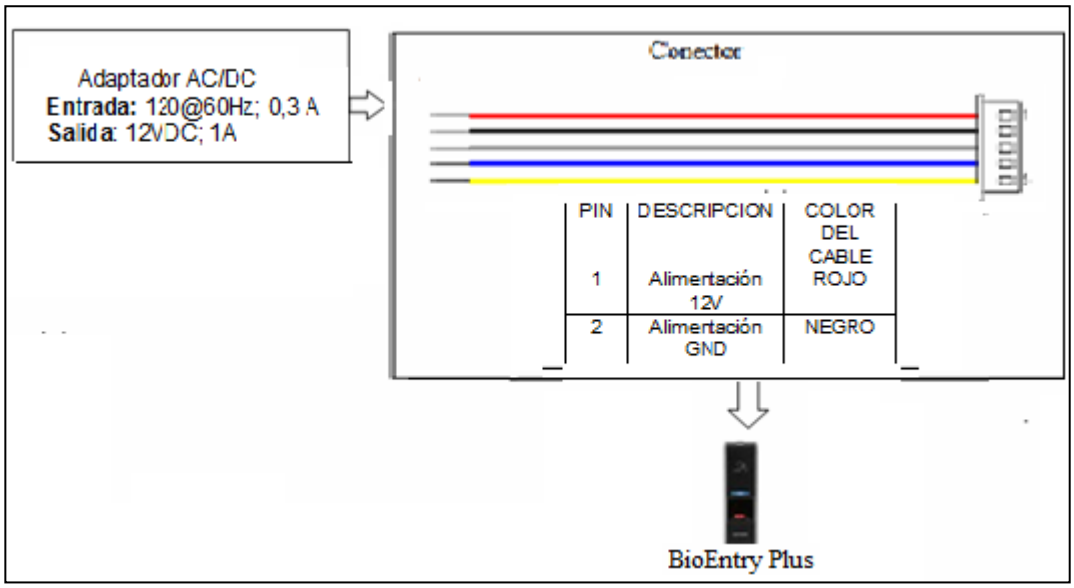


Figura 3.21: Conexión del BioEntry Plus con la red local usando cableado estructurado. **Fuente: Guía de Configuración del dispositivo biométrico BioEntry Plus [11].**

3.10.2 Instalación para la Red LAN

Para conectar el dispositivo biométrico en la red LAN se utiliza el conector dado por el fabricante, el cual contiene adaptador desde el dispositivo hasta la red. Todos los modelos de BioEntry Plus utilizan el mismo adaptador, en el caso del Biostation se realiza directamente del equipo a la red. La figura 3.22 muestra los pines, la descripción y el color de cada cable del adaptador. Esta unión permite la configuración del equipo biométrico desde una PC, además de la conexión hacia la red local, así como el monitoreo en tiempo real de todos los dispositivos conectados al Sistema Biométrico.

Además esta conexión es indispensable para realizar los registros personalizados de control de asistencia del personal.

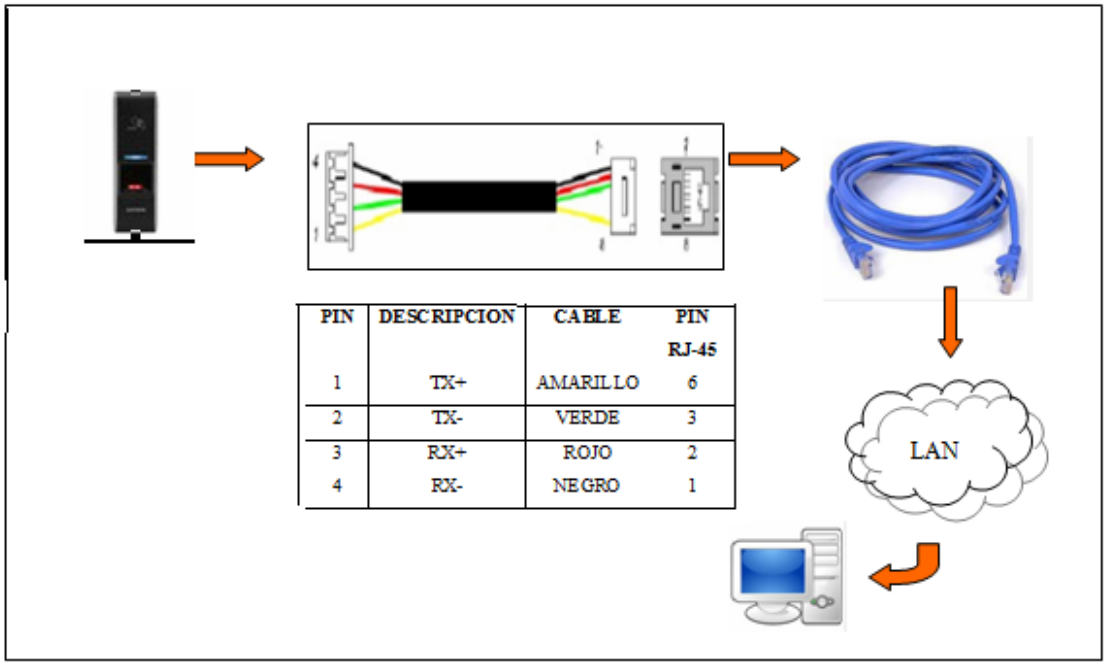


Figura 3.22: Descripción del conector y la conexión con la Red.

La siguiente figura 3.23 muestra toda la conexión que requiere para enlazar el dispositivo BioEntry Plus a la red y a la base de datos del servidor en el Sistema Biométrico y desde una PC configurada como cliente realizar un monitoreo en tiempo real de todos los equipos biométricos conectados.

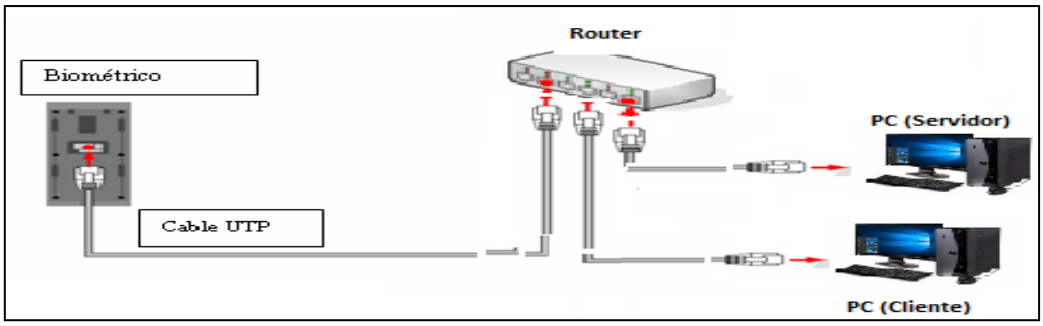


Figura 3.23: Conexión general del equipo con la red LAN.

3.10.3 Instalación para el Pulsador

La siguiente figura 3.24 señala el circuito que se conecta a la salida del relé, que corresponden al switch 1, cables de color amarillo y negro según la tabla 3.4, de la sección correspondiente a la conexión de Entrada Digital y salida del relé**.** El pulsador 1 requiere de un cableado eléctrico hasta los terminales del relé del dispositivo BioEntry Plus, si existen otras puertas anexas al circuito se agregan P2, P3 y así sucesivamente.

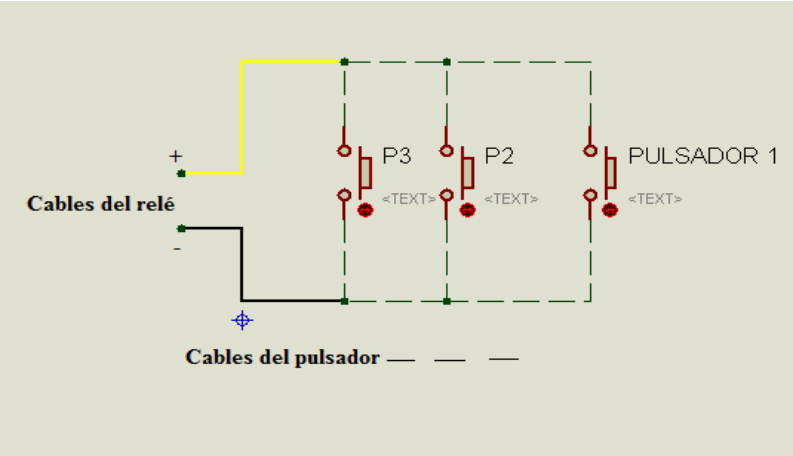


Figura 3.24: Circuito del pulsador. Fuente: Elaboración Propia

El cableado según el Código Eléctrico Nacional (CEN) debe estar dentro de tuberías, además se requieren canaletas para cubrir los cables en las paredes.

3.10.4 Instalación del biométrico en las puertas con cerradura electromagnética

Las cerraduras en las puertas son elementos indispensables en la seguridad hoy día. En la actualidad presentan un gran número de variantes, cada una asociada a distintas tecnologías, las cerraduras son un complemento esencial para un sistema de control de accesos.

La cerradura electromagnética se utiliza como medio de apertura en lugares donde la entrada debe ser limitada (control de acceso). Además, cuentan

con dos piezas principales, por un lado el electroimán, y por el otro lado una lámina metálica llamada pieza móvil o pieza polar. El electroimán se coloca en el marco de la puerta, trabaja como imán en la medida que circule corriente por su bobina y cierra la puerta; al dejar de recibir corriente eléctrica permite la apertura de la puerta. Todas estas cerraduras electromagnéticas son de tipo **"Fail Safe**", lo que significa que se mantienen cerradas solo, mientras exista corriente eléctrica, tal como se muestra en la figura 3.25, a diferencia de los otros tipos de cerraduras eléctricas, que funcionan del modo **"Fail Secure"** las cuales funcionan de modo contrario cuando no hay electricidad se mantienen cerradas.

Figura 3.25: Cerradura electromagnética.

Existen varios modelos de cerraduras electromagnéticas estas se basan mayormente en la resistencia, la fuerza de empuje que pueden ofrecer generalmente se pueden encontrar desde 300 lbs a 1200 lbs de presión, mientras mayor sea las libras de presión mayor seguridad brindara la cerradura.

Formas de Instalación:

La instalación de las cerraduras electromagnéticas opera como regla básica que el electroimán se encuentre perfectamente alineado con la placa metálica (pieza móvil o pieza polar), para lograr esta alineación existen varios tipos de bases para estas cerraduras, ya que se conocen diferentes tipos de puertas y situaciones de apertura. Entre el tipo de bases se pueden encontrar las siguientes: Base plana incluida con la cerradura, y otros tipos de bases, las cuales

se deben adquirir por separado: base tipo U, base Tipo L, base tipo Z, el apéndice G recopila información de los tipos de bases.

3.10.5 Instalación del BioEntry Plus con la canalización eléctrica.

Esta instalación se realiza para situar completamente el dispositivo de Reconocimiento Dactilar en las puertas, se caracteriza por contener los circuitos de la cerradura electromagnética, el circuito del pulsador y el circuito de alimentación eléctrica, bajo el diagrama esquemático 3.26.

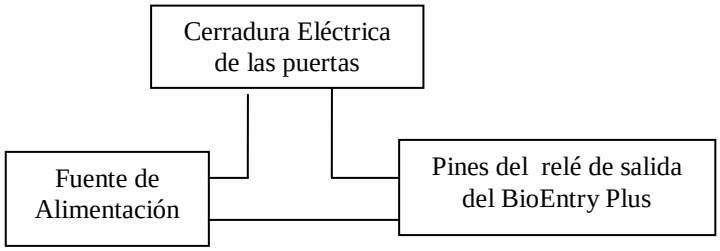


Figura 3.26: Diagrama Esquemático de la instalación de la cerradura, la fuente de Alimentación eléctrica y los pines del relé de salida del BioEntry Plus

La siguiente figura 3.27 muestra todas la conexiones del dispositivo biométrico, el cableado de la cerradura magnética con su respectiva alimentación eléctrica, el cableado del pulsador con su conexión hacia el relé de salida del dispositivo (pin 1 y 2) y el cableado que cierra el circuito entre la cerradura y la fuente de alimentación de 12 VDC son los pines de relé de salida del modelo BioEntry Plus (5 y 6)

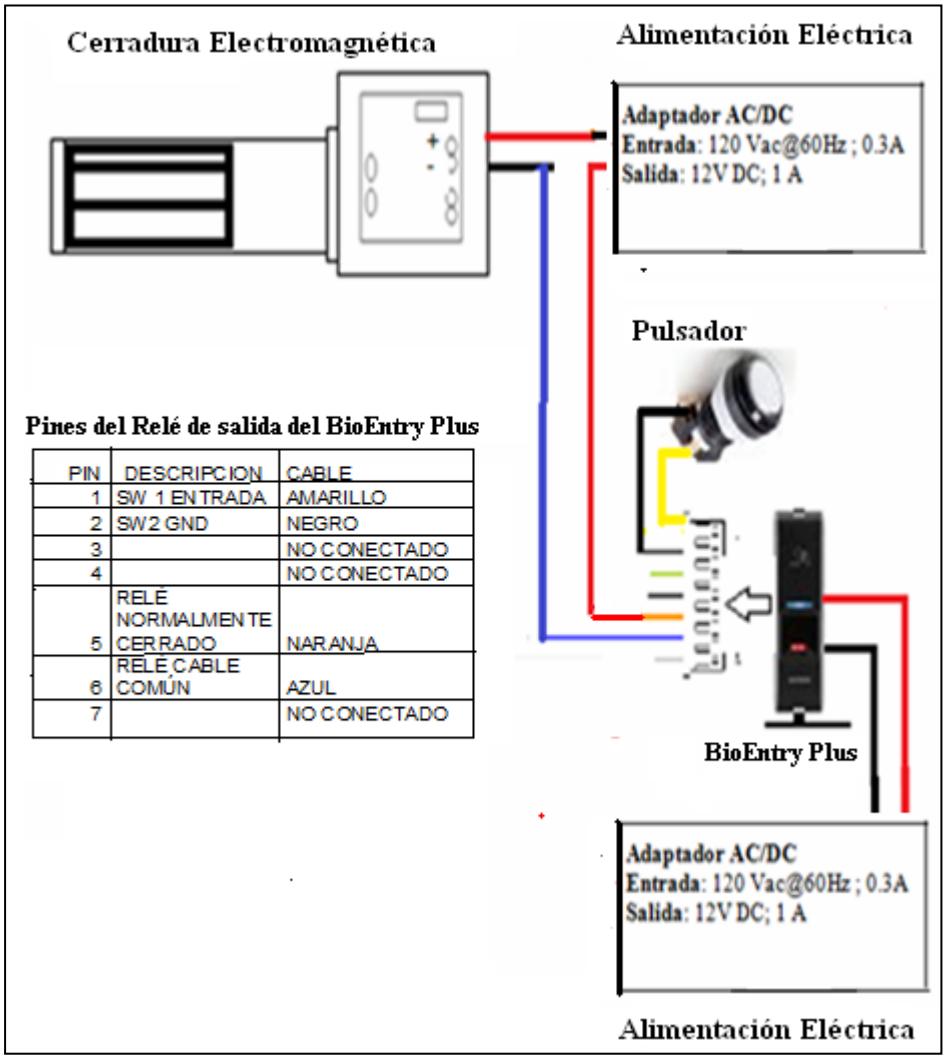


Figura 3.27: Instalación del cableado eléctrico entre el dispositivo biométrico la cerradura eléctrica, el circuito del pulsador y la fuente de alimentación de la cerradura magnética.

3.10.6 Instalación del biométrico en las puertas con cerradura de hembrilla

La cerradura de hembrilla es un mecanismo que permite el bloqueo de una puerta eléctricamente, dichas cerraduras impiden el acceso en ciertas zonas, son cómodas y seguras. Su funcionamiento difiere de la cerradura electromagnética, ya que esta compuesta por una bobina y un microswitch que

permite una señalización óptica, sonora u otras, las cuales se usan para indicar alarma o apertura de puertas las figuras 3.28 la muestran.

Estas cerraduras de hembrilla pueden contener una o doble bobina, las mejores cerraduras contienen doble bobina, ya que se distribuye uniformemente la carga, lo cual garantiza gran fiabilidad en el tiempo. Dichas cerraduras están enmarcadas en las puertas, pueden ocurrir desalineaciones en el marco de la puerta donde se coloca la cerradura y el recibidor metálico, por modificaciones debido a dilataciones o retracciones derivadas del cambio de temperatura, movimientos mínimos de la estructura donde se fijo la puerta, entre otras, los cuales dificultan el cierre correcto de la puerta, en algunas ocasiones impiden abrirla o cerrarla.

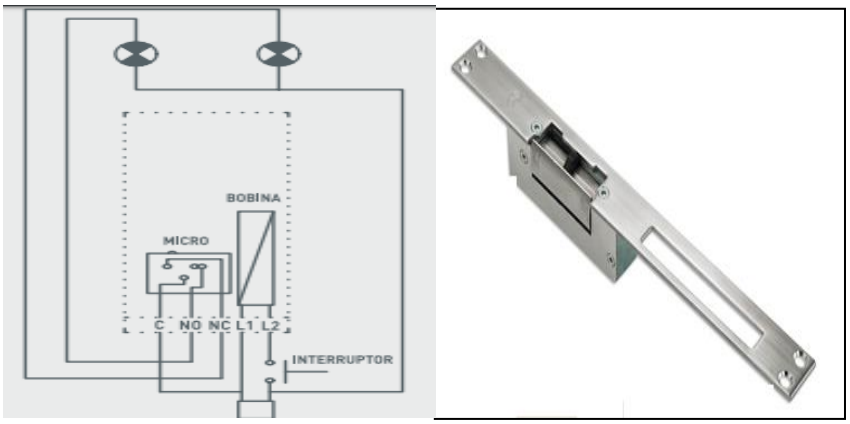


Figura 3.28 Circuito interno de una Cerradura de Hembrilla y Cerradura de Hembrilla

Las cerraduras de hembrilla utilizan un pulsador para accionarlas por un interruptor sin corriente eléctrica. Algunos fabricantes recomiendan que el pulsador sea de latón, porque no se decolora, no se agrieta ni se rompe y tendría una mayor duración. Estas cerraduras contienen además un expulsor con resortes, ligeros o duros dependiendo del esfuerzo que se requiera para cerrar. Algunos fabricantes recomiendan expulsores con resortes modificables a través de simples ajustes internos, es decir, expulsores con fuerza de cierre regulable. El apéndice H muestra las especificaciones de esta cerradura.

3.10.7 Instalación del BioEntry Plus con la canalización eléctrica de la cerradura de hembrilla en las puertas

La alimentación eléctrica de la hembrilla pude ser AC o DC. En el Sistema Biométrico se utiliza de 120 VAC, y se coloca en serie con los pines del relé de salida, normalmente abierto y el común respectivamente y la fuente de alimentación de 120 VAC, el pulsador se conecta en los pines 1 y 2 del relé de salida del dispositivo biométrico como se muestra en la figura 3.29

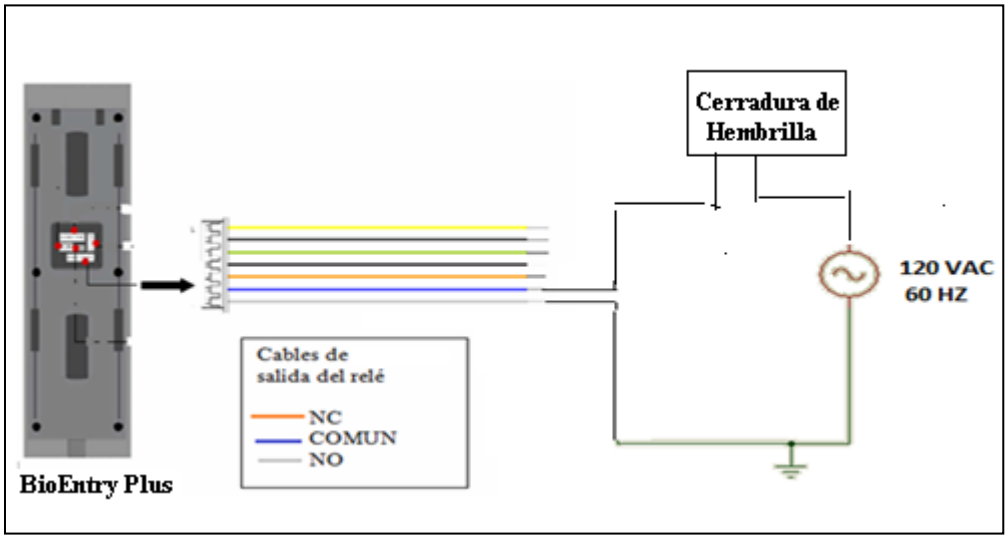


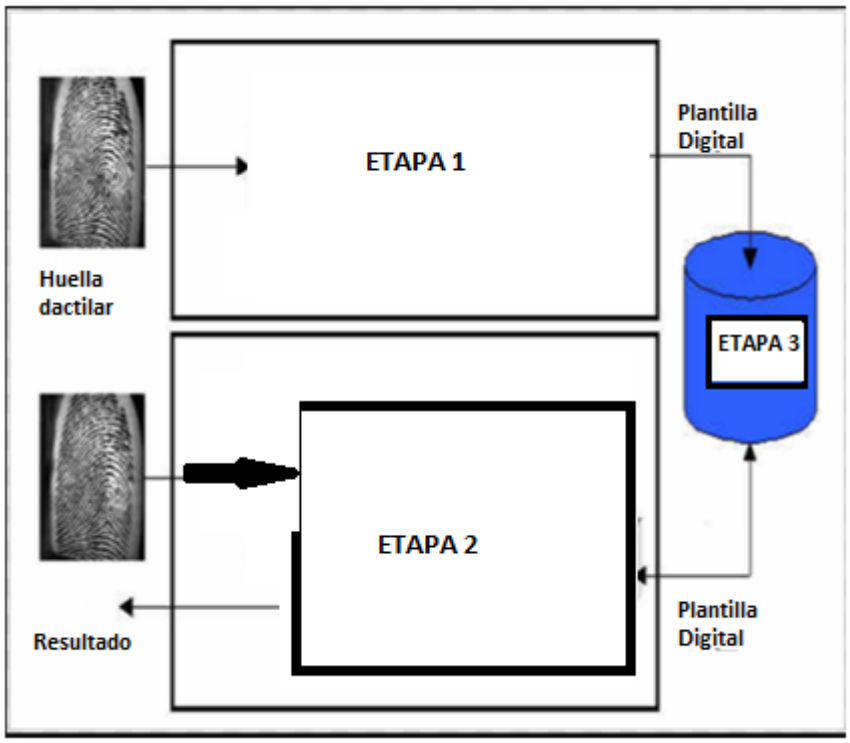
Figura 3.29: Instalación de la cerradura de hembrilla.

CAPITULO IV

FALLAS DETECTADAS EN EL SISTEMA BIOMETRICO

4. Evaluación del Sistema Biométrico

Para registrar las fallas en el Sistema Biométrico, se ejecuto una inspección con un conjunto de acciones dirigidas a realizar una evaluación del Sistema Biométrico de la empresa, fundamentada principalmente en la separación de sus niveles de funcionamiento, con el fin de identificar las fallas en cada etapa como se muestra en el siguiente diagrama 4.1.



Cuadro 4.1. Diagrama de Etapas del Sistema Biométrico

La Etapa 1 esta basada principalmente en la recolección de datos, se ejecuta por medio de la utilización del software BioStar y por el uso del accesorio Biomini para captar las huellas dactilares del personal. Esta Etapa 1, es gestionada principalmente por el personal tanto de Recursos Humanos como de Soporte

Técnico de Redes en OTI, entre otros departamentos que solo lo usan para registros personalizados.

Desde el momento que se registran los trabajadores en el Sistema Biométrico (cuando se ingresan sus datos y se almacenan en la base de datos, en forma de plantilla digital) ya pueden acceder al Sistema Biométrico, es decir, el personal se encuentra habilitado para recorrer las instalaciones permitidas por los accesos y realizar formalmente su asistencia en la empresa. Entre los datos personales recogidos, se encuentran la huella dactilar, la identificación de usuario, el departamento al que pertenece y los accesos donde pueden transitar sin inconvenientes, ni restricciones.

ETAPA 1

Recolección de Datos

Personal operativo ejecuta:
- Software BioStar
- Biomini

Obtiene:
- Datos personales
- Huella dactilar
- Departamento que labora
- Accesos permitidos

La Etapa 2 está constituida por el dispositivo biométrico, que puede ser el BioEntry Plus o el Biostation y toda la conexión en la red que implica la comprobación y verificación de los datos almacenados en el Servidor BioStar. Esta Etapa contiene toda la instalación física del dispositivo, la alimentación eléctrica, la conexión de las cerraduras de las puertas, tanto de hembrilla como la electromagnética, la conexión del pulsador, el cableado estructurado de la red WAN y LAN.

ETAPA 2

Dispositivo Biométrico

Dispositivo Instalado

- Alimentación Eléctrica
- Red
- Conexión de cerraduras en las puertas
- Conexión del pulsador

Comprobación y Verificación de Huella Dactilar

- Servidor BioStar

La Etapa 3 involucra al Servidor BioStar, ya que contiene la Base de Datos del Sistema Biométrico, almacena las plantillas digitales que permiten confirmar la huella dactilar, que fue colocada en el lector óptico del dispositivo y se proporciona los datos para su comprobación y verificación en la Etapa 2. Luego el acceso será o no otorgado por la puerta donde se encuentre instalado el dispositivo. Además, existen dispositivos biométricos (Biostation) de control de asistencia, que indica la hora de llegada y de salida en su pantalla, en cambio el BioEntry Plus suministra estos datos solamente por medio de reportes realizados por el personal que tenga permitido acceder a la Base de Datos.

ETAPA 3

Servidor BioStar

Almacena

- Base de Datos
- Plantilla Digital

Para la detección de fallas en el Sistema Biométrico, se recopiló la información de eventos no deseados, por medio de una Encuesta dirigida al personal de soporte técnico, encargados de administrar dicho Sistema, tanto en la etapa de registro e inscripción en el Sistema, como la instalación de los dispositivos y la realización de reportes personalizados. Esta encuesta, fue un conjunto de preguntas dirigidas para recopilar tan solo una muestra representativa de las fallas más comunes en el mismo, con el fin de conocer el estado de las etapas ante hechos específicos y exclusivos. Se evalúa además la confiabilidad del sistema.

4.1.2 Encuesta realizada

La base muestreada para detección de fallas permitió recolectar algunos datos, sobre las fallas comunes, que la división de soporte técnico recibe a diario, con un número de 6 individuos que componen esta división, los cuales tratan cada Etapa del Sistema en forma particular, existen encargados de la recopilación de datos, otros se encargan de la instalación de los dispositivos en las puertas y otros administran el software para configurar y operar la base de datos para carga de reportes y controles de accesos hacia los distintos lugares de la empresa.

La encuesta mostrada en el formato 4.2 tiene consultas sobre el tipo de equipo usado en la red biométrica, posibles fallas en los componentes del Sistema como son: el lector de huella dactilar, la cerradura de las puertas y el pulsador. En cuanto a la canalización del equipo biométrico, se indaga acerca de las condiciones físicas del cableado, posibles irregularidades en las conexiones de las cerraduras, del pulsador y en el equipo biométrico. También se examinó a lo concerniente a la base de datos, específicamente al manejo en la recolección de datos de los usuarios y la realización de los registros de asistencia.

Cabe destacar que esta información respalda algunas de las fallas detectadas en el análisis del sistema, debido a que el personal tiene mas tiempo manejando la red, aun desconociendo todo el funcionamiento en conjunto.

Figura 4.2: Formato de la encuesta realizada

Fecha: _____

División de Redes y Telefonía

Encuesta dirigida al personal de Soporte Técnico, para recopilar información de las fallas detectadas dentro del Sistema Biométrico de la empresa Conviasa*.*

Por favor, dedique unos momentos a completar esta encuesta.

La información que nos proporcione se utilizará para realizar un análisis del estado de los componentes del Sistema Biometrico, el cual permitirá una evaluación del mismo, y así mejorar las técnicas y procedimientos para la instalación, configuración y utilización de los equipos.

1. ***¿Cuánto tiempo lleva operando el Sistema Biométrico (Dispositivos, instalación y administración de la base de datos)***

- *Menos de un año*
- *Entre 1 y 3 años*
- *Mas de 3 años*
- *Nunca lo he utilizado*

Dispositivos Biométricos

2. ***Mencione los modelos que ha utilizado para la instalación***

- *BioEntry Plus*
- *Biostation*
- *Coloque otro modelo usado _____*

3. ¿El lector óptico ha presentado fallas visibles?

- *No*
- *Si, en este caso, responder los siguientes ítems.*
  - *No escanea la huella dactilar*
  - *No enciende el lector óptico*
  - *Mencione otra falla _____*

4. ¿Los dispositivos han mostrado indicaciones de retardo para abrir la puerta?

- *Si*
- *No*
- *Mencione otra característica_____*

5. ¿Los dispositivos han tenido fallas para abrir las puertas?

- *Si*
- *No*
- *Mencione otra característica_____*

6. ¿El pulsador para abrir la puerta se daña con que frecuencia?

- *Poca*
- *Mucha*
- *Ninguna*

Canalización del Equipo Biométrico

7. ¿Ha observado deterioro en los cables de instalación de los equipos operativos?

- *Si*
- *No*
- *Otro _____*

8. ¿Cuál cableado tiende a dañarse de forma más recurrente?

- *Red*
- *Pulsador*
- *Fuente de Alimentación (Adaptador)*
- *Todas sin distinción*
- *Ninguna*
- *Otra_____*

9. ¿Cuáles tipos de cerradura para las puertas ha maniobrado?

- *Cerradura para la puerta magnética*
- *Cerradura para la puerta de hembrilla*
- *Otro _____*

10. ¿Ha notado cual de las cerraduras de las puertas ha presentado mas fallas con el uso del equipo biométrico?

- *Puerta magnética*
- *Puerta de hembrilla*
- *Otra _____*

Administración del Software del equipo

11. ¿Existen inconvenientes para registrar la huella dactilar de los usuarios?

- *No*
- *Si, en este caso, responder los siguientes ítems.*
  - *No aparecen sus datos personales registrados en la base de datos*
  - *Están registrados, pero el biomini no verifica la huella*
  - *Los dispositivos no admiten su huella dactilar*
  - *Mencione otras falla _____*

12. ¿Los reportes personalizados tienen inconvenientes para su elaboración?

- *No*
- *Si, en este caso, responder los siguientes ítems.*
  - *No aparece su información personal en la base de datos*
  - *El personal que utiliza el programa no tiene la destreza para usarlo*
  - *Los dispositivos no guardaron la información solicitada*
  - *Mencione otras fallas _____*

4.2 Resultados de la Encuesta

La experiencia del Personal de Soporte con el Sistema Biométrico, es mixto, tal como se refleja en la figura 4.3, ya que existe un personal que tiene más de 3 años operando el sistema, ya sea el software, la configuración, la instalación o la base de datos y otras personas que están recientes en el uso del mismo.

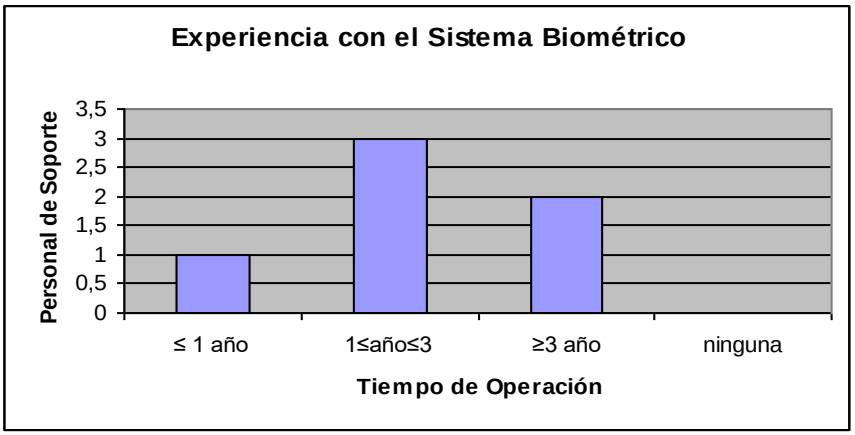


Figura 4.3: Experiencia con el Sistema Biométrico.

Dispositivos Biométricos

Solo se utilizan dos modelos de dispositivos biométricos (Figura 4.4) el BioEntry Plus y el Biostation en el Sistema.

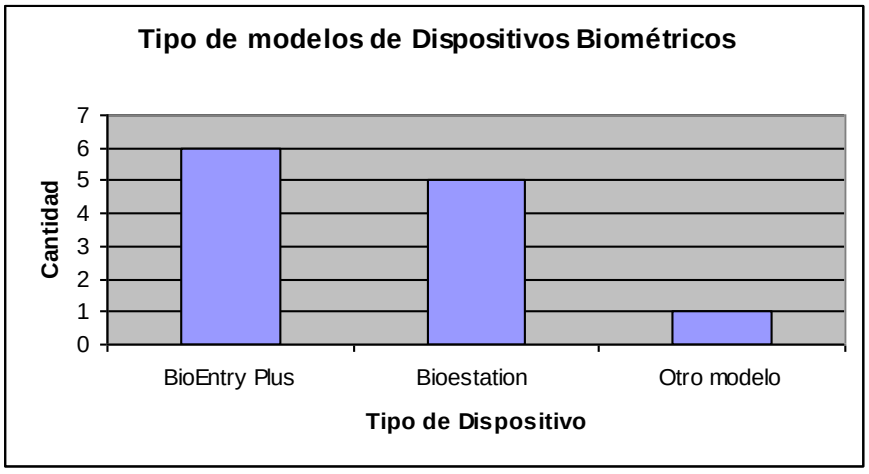


Figura 4.4: Modelos usados en el Sistema Biométrico.

El lector óptico ha presentado fallas visibles (Figura 4.5) dentro del sistema.

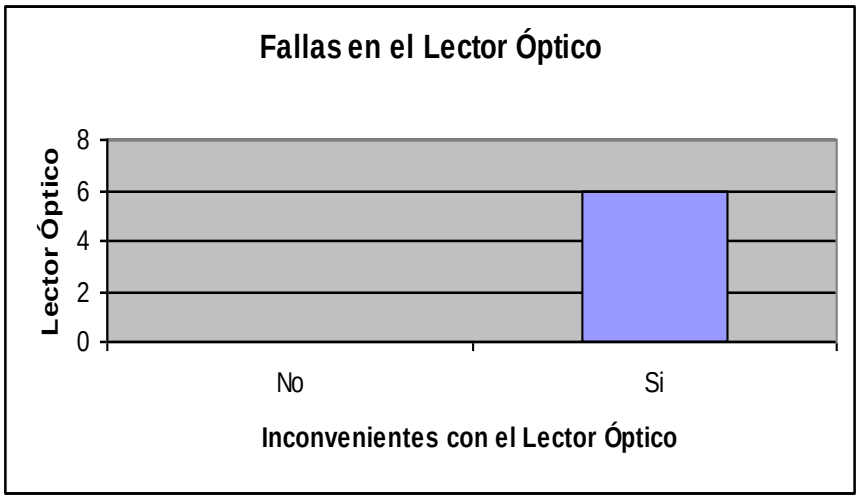


Figura 4.5 Visualización de problemas en el Lector Óptico.

Dentro de las fallas frecuentes en el Lector se consiguen: inconvenientes para escanear la huella dactilar, para reconocerla y algunas restricciones en el sistema Figura 4.6.

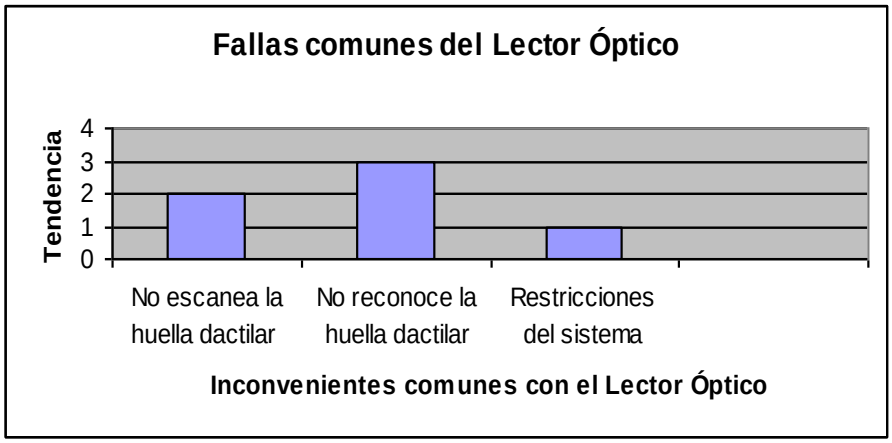


Figura 4.6: Fallas frecuentes del Lector Óptico.

Otra falla evidente es el retardo en la apertura de puertas Figura 4.7 dentro de las zonas de control de acceso

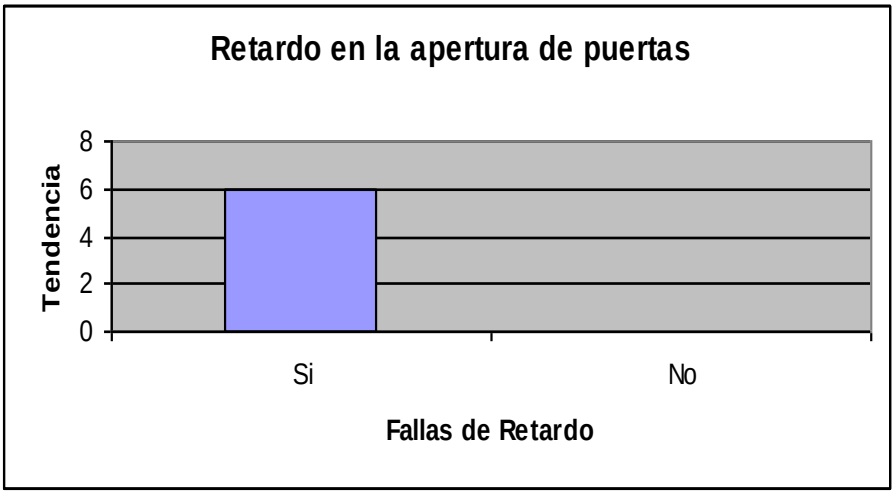


Figura 4.7 Tendencia del Retardo.

Es frecuente abrir las puertas y observar inconvenientes, ya sea con cerraduras de hembrilla o con la cerradura electromagnética (Figura 4.8).

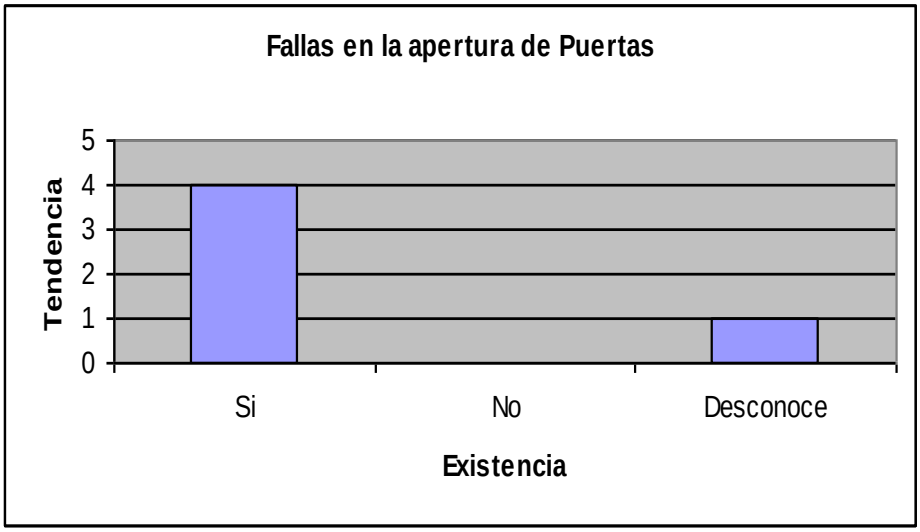


Figura 4.8: Tendencia alta de fallas cuando se abren las puertas. Fuente: Elaboración Propia

Es poco frecuente que se dañe el pulsador que activa la cerradura en las puertas (Figura 4.9), pero si han surgido algunos inconvenientes.

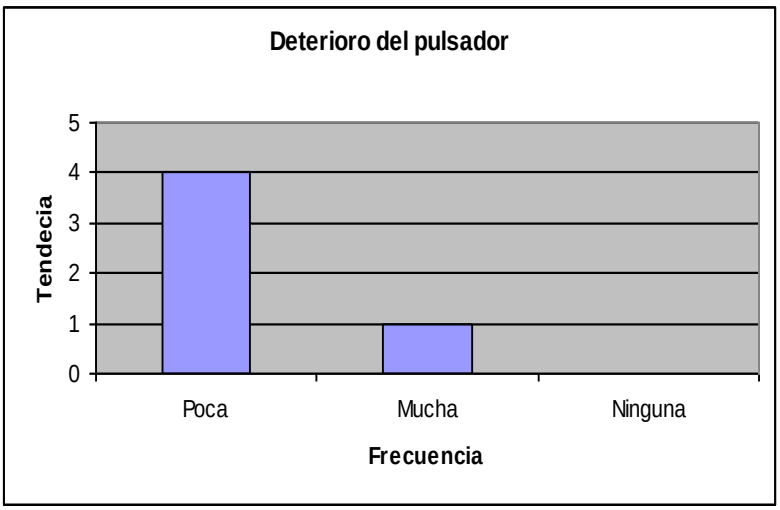


Figura 4.9: Tendencia baja de daños en el pulsador.

Canalización de los dispositivos biométricos

En cuanto al cableado eléctrico de manera general, se puede decir que presenta poco deterioro en sus conexiones (Figura 4.10) de red, de alimentación eléctrica, del pulsador o de la conexión de las cerraduras de las puertas. Aunque la falla usual es en la fuente de alimentación y el pulsador (Figura 4.11).

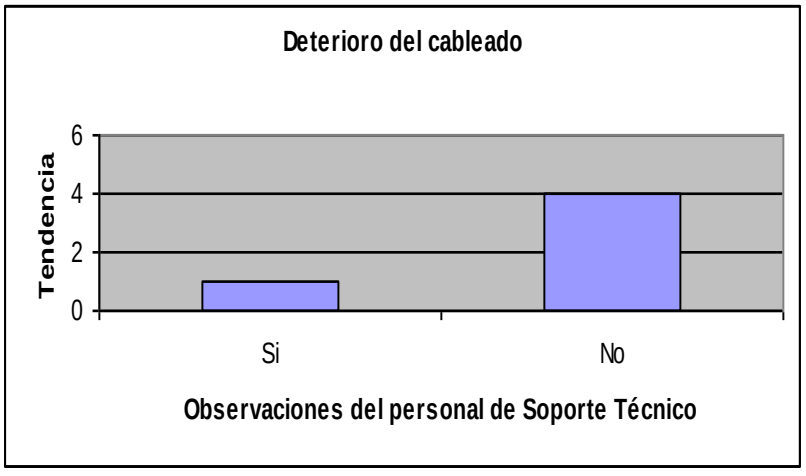


Figura 4.10: Baja frecuencia de inconvenientes con el cableado.

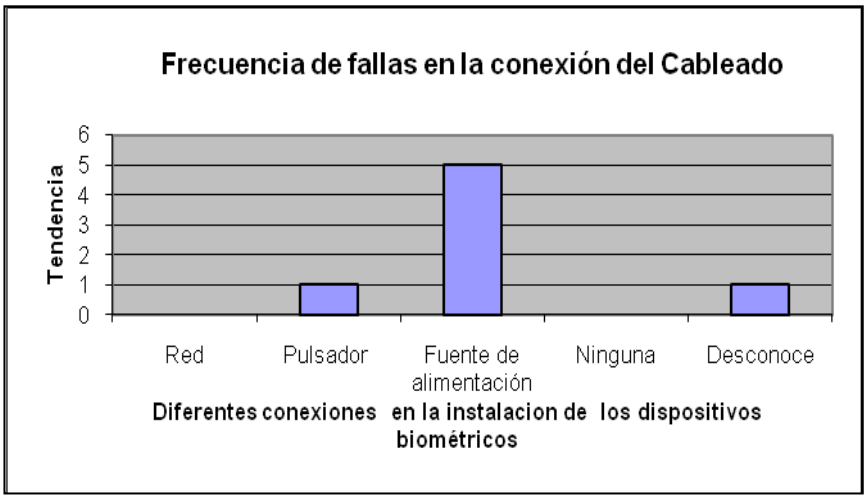


Figura 4.11: Adaptadores de alimentación eléctrica dañadas con frecuencia alta.

Existen dos tipos de cerraduras que se usan en las puertas del sistema biométrico, cerraduras electromagnéticas y las de cerradura eléctrica de hembrilla (Figura 4.12)

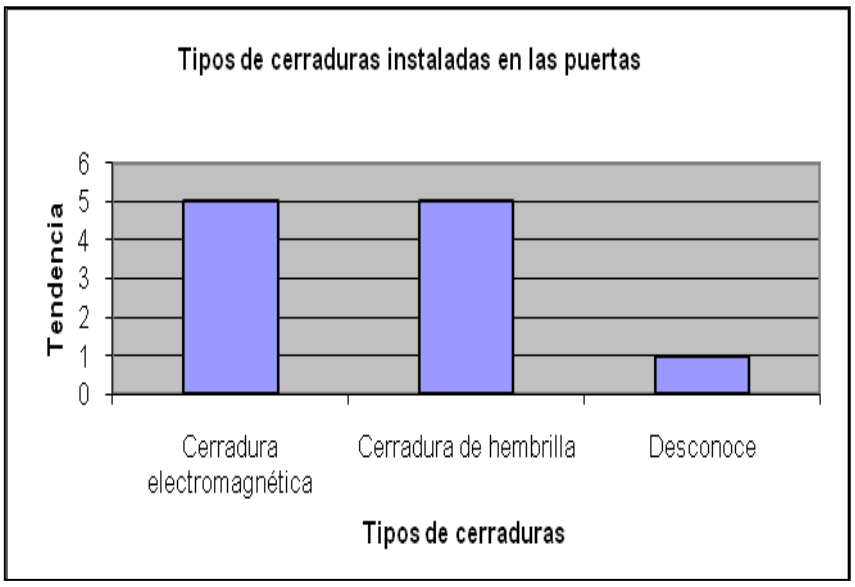


Figura 4.12 Existen dos tipos de Cerradura instalada.

La cerradura que presenta mas fallas en las puertas, es la de eléctrica de hembrilla (Figura 4.13)

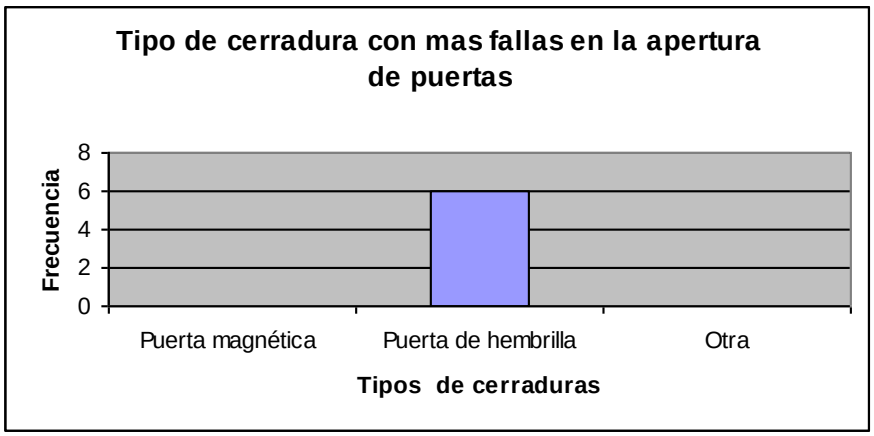


Figura 4.13: Alta frecuencia de daños en la puerta de hembrilla.

Administración de la base de datos

En cuanto a la administración de la Base de Datos se han registrado inconvenientes para registrar la huella dactilar (Figura 4.14)

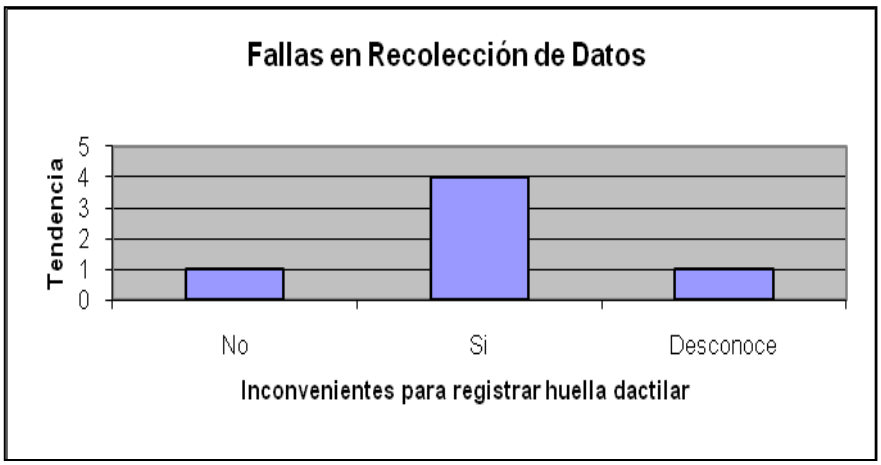


Figura 4.14: Inconvenientes para recopilar los Datos

La ocurrencia de las fallas es alta al momento de comprobar y verificar la huella dactilar, en menor proporción se presentan inconvenientes para

reconocer la huella dactilar y de igual tendencia se observa la falta de destreza del personal para operar la recopilación de datos (Figura 4.15), ya sea reconocimientos de huellas o manejos de la Base de Datos.

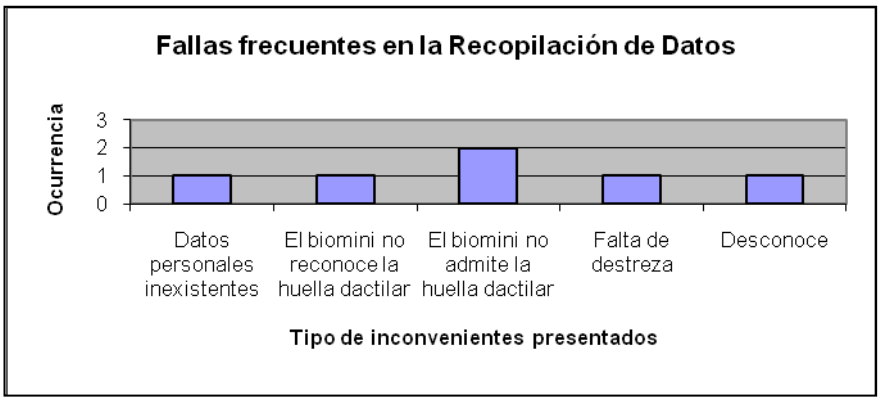


Figura 4.15: Frecuencia en la recopilación de Datos.

La elaboración de registros personales en la base de datos ha presentado ciertos inconvenientes (Figura 4.16).

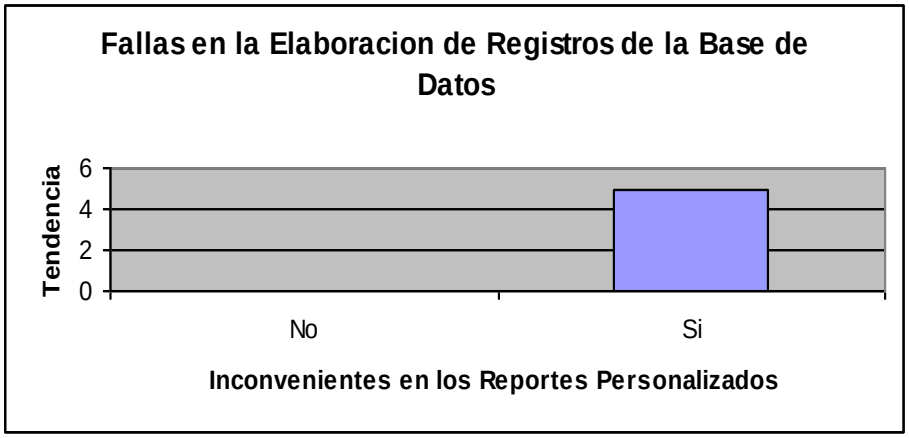


Figura 4.16: Inconvenientes para realizar los reportes personalizado.

Estos inconvenientes se muestran en la Figura 4.17, en dicha elaboración de los reportes ocurren la inexistencia de datos del personal, una mala operación en el software al momento de realizar la carga o de realizar el reporte, además, de presentase fallas en la conexión de red y la predominante falta de destrezas del personal de otros departamento que tienen acceso al sistema al momento de manejarla.

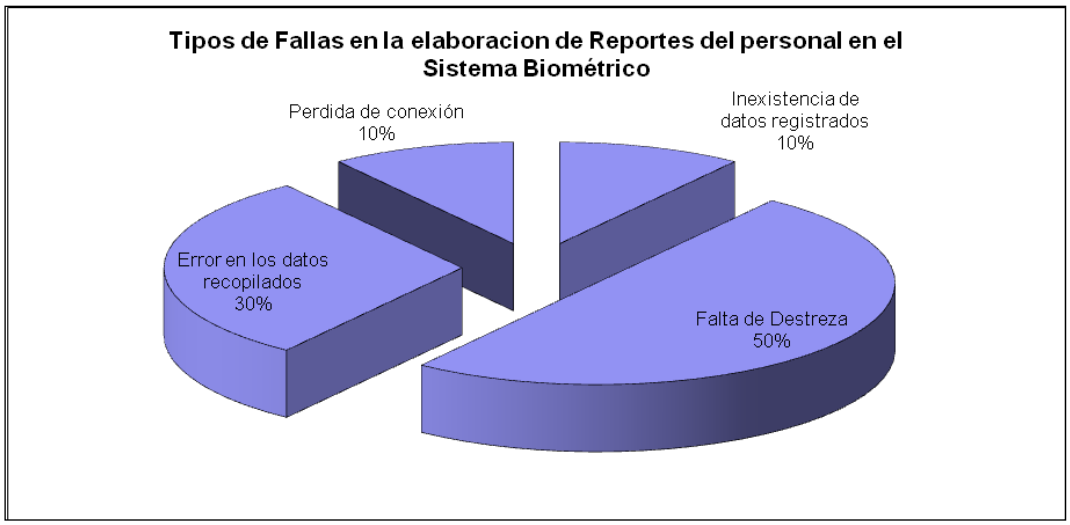


Figura 4.17. Fallas frecuentes en la elaboración de reportes.

4.3 Dispositivos biométricos defectuosos

Se ha presentado de forma recurrente en los equipos biométricos BioEntry Plus, tanto usados como nuevos, un inconveniente particular muy común: *El relé de salida no funciona*, por tanto no es posible, instalar de forma correcta el equipo biométrico, esto trae como consecuencia la imposibilidad de controlar las cerraduras en las puertas, ya que, no reciben la señal del relé para abrir la cerradura, a pesar de que el reconocimiento de la huella dactilar del usuario fue leído, comprobado y verificado por el sistema.

4.3.1 Evidencia de los equipos con fallas

a) Realización de pruebas de continuidad con el tester.

Esta prueba se refiere a una prueba de continuidad en la salida de los contactos del relé, el cual permite notar, si abren o cierran sus contactos. La siguiente figura 4.18, muestra los cables de prueba para comprobar la continuidad en los contactos del relé, en este caso el equipo BioEntry Plus, sino ocurren cambios óhmicos el relé no funciona.

Esta prueba se realiza en equipos conectados a la red con fallas o cuando se realiza la configuración del dispositivo biométrico. Una vez que se ha añadido el dispositivo al Sistema Biométrico, por medio del Software de configuración BioStar 1.8, se anexa a una puerta para permitir el acceso, se añaden usuarios para que permitan comprobar el estado del relé. Al colocar una huella dactilar de la base de datos en el lector, se activa el relé y por tanto pueda ser “medible” la continuidad y el valor óhmico de la bobina del relé de salida.

Los cables donde se realiza esta prueba se conectan con la salida del relé, según la Tabla 3.4, "*Descripción del cable de conexión de entrada digital y salida de relé*". El cable azul (relé común) se une al cable negro del tester (común o GND) y se prueba la continuidad en el cable naranja (si se trata de la cerradura electromagnética) con la otra punta (roja) del tester

La continuidad con la cerradura eléctrica de hembrilla también se refiere a la Tabla 3.4. El cable azul (relé común) se une al cable negro del tester (común o GND) y el blanco con la punta roja del tester.

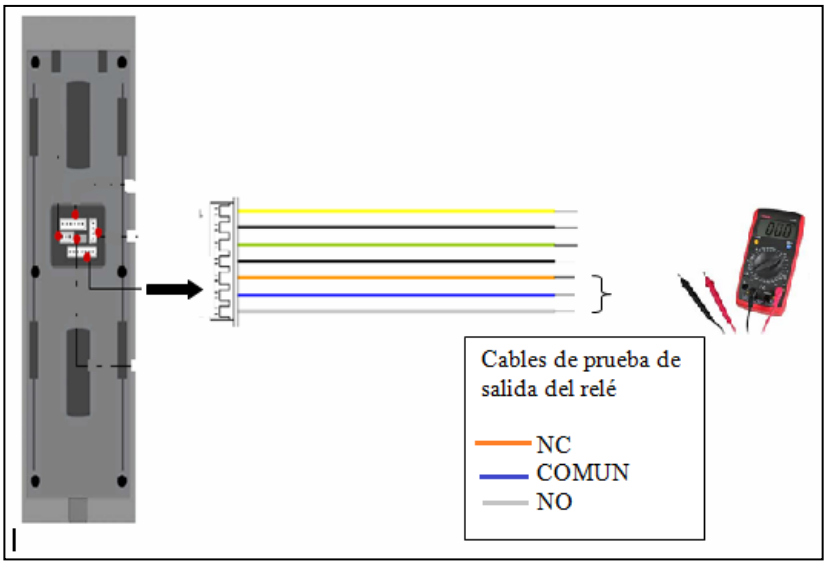


Figura 4.18: Cables y conexiones usadas para probar el relé de salida en el BioEntry Plus.

Las salidas normalmente cerradas y normalmente abiertas del relé en funcionamiento tienen que presentar variación óhmica y se debe observar el cambio óhmico de la siguiente tabla:

Tabla 4.1 Valores óhmicos de salida del relé

Cable	Especificación	Ohmios (Ω)	Ohmios (Ω)
Naranja (+) Azul (-)	Normalmente Cerrado	0	10
Blanco (+) Azul (-)	Normalmente Abierto	10	0

De no presentarse dichas variaciones el relé se encuentra dañado.

b) El sonido característico de apertura del relé no fue audible.

Esta prueba se realiza en equipos conectados con fallas o cuando se realiza la configuración del dispositivo biométrico. Una vez que se ha añadido el dispositivo al Sistema Biométrico, por medio del Software de configuración BioStar 1.8, se anexa a una puerta para permitir el acceso, con usuarios para que permitan comprobar el estado del relé colocando la huella dactilar. Por lo general, en esta prueba se coloca la huella dactilar para reconocimiento y si es aprobada por el equipo, se activa el relé del equipo biométrico, el cual emite el sonido característico de un relé.

c) Prueba utilizando los cables usados para el pulsador

El primer switch del relé de salida, según la Tabla 3.4, "*Descripción del cable de conexión de entrada digital y salida de relé* ", es usado para colocar un pulsador que activa la cerradura de una puerta, si se unen las dos puntas entre sí (pin entrada **1** y GND **2**), de color negro y amarillo respectivamente, con los pines del pulsador, al activarse, debe ser audible el accionamiento del relé. Si no se escucha está dañado, la figura 4.19 muestra los cables que deberán unirse para esta prueba.

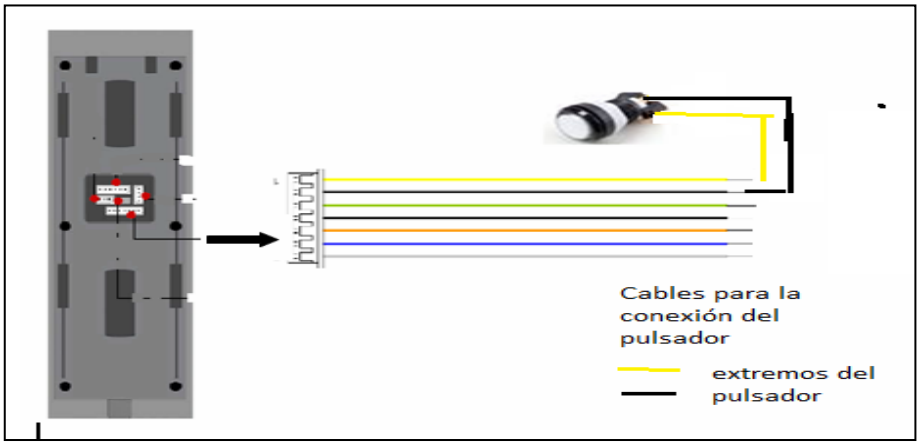


Figura 4.19: Cables y conexiones usadas para probar el relé de salida usando el circuito del pulsador de salida en el BioEntry Plus.

En los casos donde el relé del equipo biométrico este dañado, solo es posible utilizarlos como equipo de control de asistencia, llegada y salida de los trabajadores, ya que, funciona su conexión de red para verificar y comprobar el reconocimiento de la huella dactilar, aunque no será posible la apertura de alguna puerta.

d) Problemas de corriente en la conexión del modelo BioEntry Plus

El modelo Biostation no presento problemas con cerraduras en las puertas de hembrilla, pero al sustituir los biométricos por los modelos del BioEntry Plus como son: BEPL, BEP, BEPH se presentaron inconvenientes con el relé de salida.

El equipo Bioentry Plus tiene un circuito impreso en el cual se usa un relé identificado con el código AGN 2004H (figura 4.20) el cual es un DPDT (Doble polo doble tiro, de sus siglas en inglés, Double Pole Double Throw) con las siguientes especificaciones eléctricas:

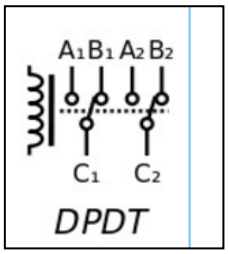


Figura 4.20 .Especificaciones eléctricas del relé AGN 2004H.

Según el manual del componente (Datasheet del AGN2004H que se encuentra en el apéndice I)

El potencia nominal de operación de 100 mW

Operaciones por minuto: 20 cpm (ciclos por minuto)

Potencia nominal de operación máxima 140 mW

El relé AGN2004H, el cual en algunos casos se observo un daño completo por carbonizarse (Figura 4.21), debido principalmente al circuito de conexión eléctrica con las puertas de hembrilla, el cual es de 120 VAC@60Hz, la mayoría de estas puertas son de accesos libres o de mucho personal.

Figura 4.21. Daños del relé de salida

La figura 4.22 muestra el siguiente es el circuito que presenta fallas porque sobrecalienta el relé interno del BioEntry Plus y quema el relé AGN2004H

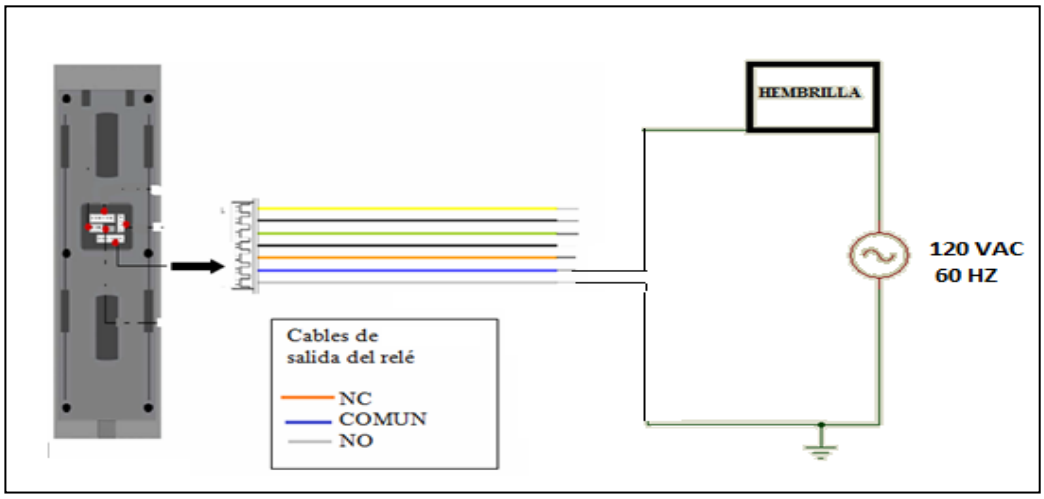


Figura 4.22 .Circuito con la puerta de hembrilla

4.4 Puesta a Tierra inexistente en los equipos de transmisión de Datos

Actualmente no existe conexión de Puesta a Tierra en los rack, ni tampoco en los equipos de transmisión de carcasa metálica en la red de Transmisión de Datos en el cuarto de cableado de OTI. El sistema de Puesta a Tierra para un cableado estructurado está diseñado para asegurar una misma referencia eléctrica para todos los sistemas electrónicos contenidos en los diferentes espacios de un edificio o un Centro de Datos. Este sistema está normado por el estándar ANSI/J/STD-607-A.

4.5 Ausencia de Normalización en la Canalización de la instalación de los equipos biométricos

No existe normalización del cableado para instalar los dispositivos biométricos en cuanto a calibre, corriente eléctrica, tensión, canaletas. Las siguientes son las conexiones requeridas en la instalación del cableado de un dispositivo: cables de alimentación, de red, la puerta de acceso (cerradura de la puerta y pulsador) tal como lo muestra el diagrama esquemático de la figura 3.18 del Capítulo 3 del subtema *Características de las Instalaciones de los dispositivos biométricos*.

A partir de este diagrama esquemático, se observa que son 3 conexiones de cableado que tiene el equipo BioEntry Plus para estar habilitado en la puerta donde se controla el acceso. La alimentación de voltaje y corriente podrá ser de calibre 18 AGW según normas CEN [12].

4.6 Instalación y configuración del Servidor BioStar

El Servidor BioStar actual esta configurado como una Maquina Virtual en el Servidor Principal de la Empresa, es indispensable instalarlo en una PC física, debido a las fallas presentadas en el puerto de salida del Servidor Principal. Por lo tanto se requiere la licencia o llave de instalación para culminar dicho proceso.

Además el Servidor BioStar presenta limitaciones para activar la red en línea conectada con el servidor Principal, ya que la versión gratuita solamente

permite 2 accesos para los operadores del Sistema. Por lo tanto, hay que esperar que salga un operador o usuario para tener acceso. Lo cual incide de forma negativa en la administración de los departamentos que tienen que acceso al Sistema Biométrico.

Formato de Análisis de Modos y Efectos de Fallas (AMEF)

Los siguientes formatos AMEF mostrados en los cuadros 4.2 y 4.3 contienen las fallas potenciales en los dispositivos biométricos: BioEntry Plus. En los accesorios: Adaptador de Alimentación; En inconvenientes de configuración de los equipos: Retardo en apertura de las puertas; En la canalización eléctrica para la instalación: cableado deteriorado; En la cerradura de las puertas: de hembrilla eléctrica; En la Base de Datos.

Formato de Análisis de Modos y Efectos de Fallas (AMEF)														Fecha:			
Nombre del Sistema (Título): Sistema Biométrico de Empresa Conviasa																	
Responsable (Dpto. / Area): Domingo Rodríguez (Redes y Telefonía / OTI)														Fecha Revisión:			
Responsable de AMFE (persona): Pasante Juana Lara																	
Sistema o Dispositivo	Modo potencial de la falla	S severidad	Efecto potencial de la Falla	O ocurrencia	Causa potencial de Falla	D Detección	NPR	Acción de Control Recomendada	S	O	D	NPR
Base de Datos	Inconvenientes para registrar huella dactilar	6	Inexistencia de información del personal en la base de datos	3	Datos personales inexistentes	6	108	Revisión de datos almacenados	3	2	3	18
					El biomini no reconoce la huella dactilar	3	54	Revisión del lector del biomini	5	2	3	30
					El biomini no admite la huella dactilar	2	36	Carga de huella dactilar con otro dedos de la mano	5	2	2	20
					Falta de destreza en la utilización de BioStar	1	18	Realizar jornadas de formación al personal que opera la base de datos	3	2	2	12
	Error en la elaboración de registros personalizados	5	No puede procesar los datos	3	Datos personales inexistentes	2	30	Revisión de datos almacenados	3	2	2	12
					Falta de destreza en la utilización de BioStar	1	15	Realizar jornadas de formación al personal que opera la base de datos	3	2	2	12
					Perdida de conexión de la red con la base de datos del servidor BioStar	6	90	Revisión del cableado estructurado de la red	3	2	3	18

Valores de S entre 1 y 10; Valores de O entre 1 y 6; Valores de D entre 10 y 1.(Ver Tablas de valoración 2.3.6.1, tabla 2.3.6.2 y tabla 2.3.6.3)

Cuadro 4.2: Formato AMEF aplicado a la Base de Datos.

Formato de Análisis de Modos y Efectos de Fallas (AMEF)															Fecha:			
Nombre del Sistema (Título): Sistema Biométrico de Empresa Conviasa																		
Responsable (Dpto. / Área): Domingo Rodríguez (Redes y Telefonía / OTI)															Fecha Revisión:			
Responsable de AMFE (persona): Pasante Juana Lara																		
Dispositivo	Modo potencial de la falla	S: Gravedad	Efecto potencial de la Falla	O Ocurrencia	Causa potencial de Falla	D Detección	NPR	Acción de Control Recomendada	S:	O	D	NPR
BioEntry Plus	No escanea la huella digital	7	No escanea la huella digital	2	Circuito impreso dañado	9	126	No tiene				0
	Inconvenientes con el Lector Óptico		No reconoce la huella dactilar	6	Huella dactilar sin registrar	6	252	Revisión por un operador	5	3	2	30
			Restricciones de acceso	3	Restricciones de acceso	2	42	Revisión por un operador	6	3	2	36
Adaptador de Alimentación	Inservible	8	No enciende el dispositivo Biométrico	5	Calidad del Adaptador		200	Control de calidad en compras	6	4	7	168
			No activa la cerradura magnética	4		5	160		6	3	7	126
Retardo en apertura de puerta	Tiempo de apertura superior a los 8 segundos	3	Daño en las cerraduras de las puertas	4	Mala configuración del relé de salida	6	72	Configuración correcta	2	3	9	54
Cableado deteriorado	Continuidad inexistente en la instalación de cableado.	8	Desconexión de los equipos biométricos en la red	3	Baja calidad de los cables	4	96	No Existe				
			No permite apertura de las cerraduras	4	Ambiente inadecuado para el cableado	2	64					
			Dispositivo sin funcionamiento	5	Inexistencia de canalización	2	80					
Cerradura para puerta de Hembrilla	Daño irreversible de la cerradura	10	Carbonización total	5	Pulsador dañado	6	300	No existe				
					Roce excesivo con el marco de la puerta	7	350	No existe				
					Nivel de voltaje inadecuado	5	250	Circuito A1				

Valores de S entre 1 y 10; Valores de O entre 1 y 6; Valores de D entre 10 y 1.(Ver Tablas de valoración 2.3.6.1, tabla 2.3.6.2 y tabla 2.3.6.3)

Cuadro 4.3: Formato AMEF aplicado al BioEntry Plus, cableado y Cerraduras de las puertas de Hembrilla.

CONCLUSIONES

La experiencia que tiene el personal de la división Redes y Telefonía con el sistema biométrico de la red Conviasa oscila entre 1≤ años≤ 3.

Referente a los dispositivos biométricos, el equipo que se utiliza más a menudo es el BioEntry Plus, debido a la sustitución del dispositivo Biostation, cabe destacar que de forma general, tanto el lector óptico, como los equipos, han presentado fallas exclusivas, que impiden su correcto funcionamiento en la apertura de puertas, tal como: no escanea la huella dactilar, no permite acceso, hay retardo para abrir la puerta.

En cuanto a la canalización del equipo el cableado del pulsador presenta poca frecuencia de deterioro, el adaptador que permite alimentar eléctricamente el equipo, es el que se daña con mas frecuencia y el cableado que presenta fallas dañinas para el sistema es el realizado con la cerradura eléctrica de hembrilla.

Por otra parte, existen inconvenientes en la recopilación de datos, ya que falta renovar las destrezas del personal para operar la Base de Datos, sobretodo para la realización de reportes personalizados y recolección de datos.

Existen ciertas contrariedades con respecto a la conexión de la cerradura eléctrica de hembrilla y con el relé de salida, ya que afecta ha dicho componente de forma directa, por lo tanto se debe realizar una nueva conexión. Hay pruebas para comprobar que el relé esta operativo o en todo caso con desperfectos, y el dispositivo biométrico debe utilizarse en actividades específicas dentro del Sistema.

Además, el Cableado Estructurado presenta una desatención en la aplicación de la norma ANSI/J/STD-607-A referente a la Puesta a Tierra en los equipos de transmisión de datos en los cuartos de cableado.

El Código Eléctrico Nacional normaliza el cableado para las instalaciones de acuerdo al voltaje y amperaje utilizado, en el Sistema Biométrico ocurre la omisión.

En lo relativo al Sistema Biométrico está administrado por medio del Software BioStar instalado en el Servidor Principal el cual contiene distintas aplicaciones y maquinas virtuales con distintos sistemas operativos.

La privación de dicha licencia no permite utilizar otra forma de monitorear el Sistema, como es el formato de mapas visuales, otra especificación BioStar.

Se encuentra en proceso una propuesta de instalación de un relé externo entre la fuente de alimentación de 120VAC, los terminales del relé de salida del dispositivo biométrico y la hembrilla eléctrica de la puerta, que protejan el dispositivo biométrico en caso de ocurrir una falla, en ese circuito.

El formato AMEF permite enmarcar el modo potencial de las fallas en 5 fases desde Bajo -nivel de falla hasta Alto nivel de falla, donde realizar acciones de control recomendadas disminuye el riesgo de las fallas detectadas.

RECOMEDACIONES

6.1 Problemas de corriente en la instalación de los dispositivos biométricos modelo BioEntry Plus

El modelo de dispositivo biométrico Biostation no presento problemas con las cerraduras eléctricas de hembrilla, pero al sustituirlo por los modelos del BioEntry Plus como son: BEPL, BEP, BEPH se presentaron inconvenientes eléctricos serios con el relé de salida.

El equipo Bioentry Plus tiene un circuito impreso en el cual se usa un relé AGN 2004H el cual es un DPDT (Doble polo doble tiro, de sus siglas en inglés, Double Pole Double Throw).

Según el manual del componente AGN 2004H su potencia nominal de operación es de 100mW, tiene alta fiabilidad del contacto. Máxima velocidad de un funcionamiento (a carga nominal) 20 cpm (contacto por minuto). Potencia nominal de operación máxima: 140 mW

La figura 6.2 muestra el componente electrónico dañado, en la tarjeta interna de circuito impreso del dispositivo biométrico figura 6.3, el relé de salida AGN 2004H, el cual se encuentra directamente conectado a la cerradura de hembrilla la cual maneja 120V AC.

Figura 6.2. Daños en el relé de salida

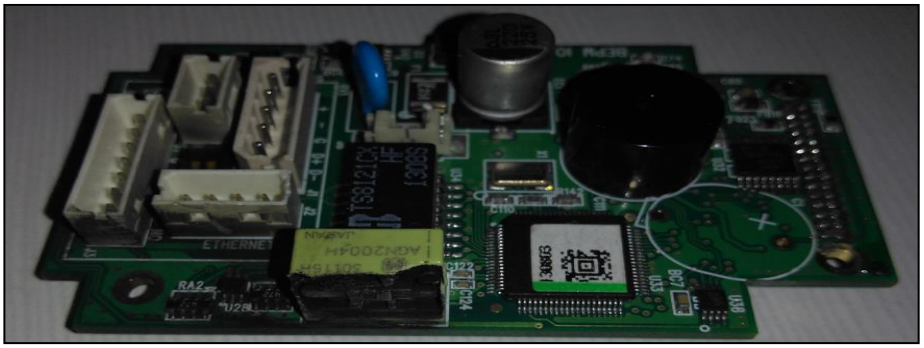


Figura 6.3 Tarjeta de circuito impreso, con componentes electrónicos carbonizados

Esta falla solo se ve reflejada en los biométricos con alimentación de: 12VDC y 1,5 A conectados en la cerradura eléctrica de hembrilla. En las cerraduras electromagnéticas no ha ocurrido esta falla porque entre sus terminales solo hay 12 VDC. La figura 6.4 enseña el circuito que presenta fallas porque sobrecalienta del BioEntry Plus y quema el relé AGN2004H

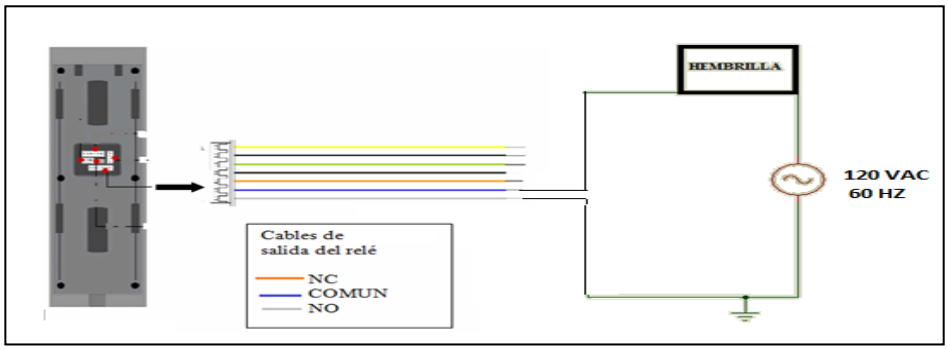


Figura 6.4. Conexión de la cerradura eléctrica de hembrilla

Consideraciones para colocar un relé externo

Los contactos son el componente más importante de un relé. Sus características se ven afectadas significativamente por factores como el material de los contactos, los valores de tensión y corriente que se les aplican (especialmente las formas de onda de tensión y corriente al activar y desactivar los contactos), el tipo de carga, la frecuencia de funcionamiento y el rebote. Si cualquiera de estos factores no satisface un valor predeterminado, pueden producirse problemas tales como la degradación del metal entre contactos, soldadura por contacto, el desgaste o un aumento rápido de la resistencia de

contacto. La cantidad de corriente eléctrica que fluye a través de los contactos influye directamente en las características de los contactos.

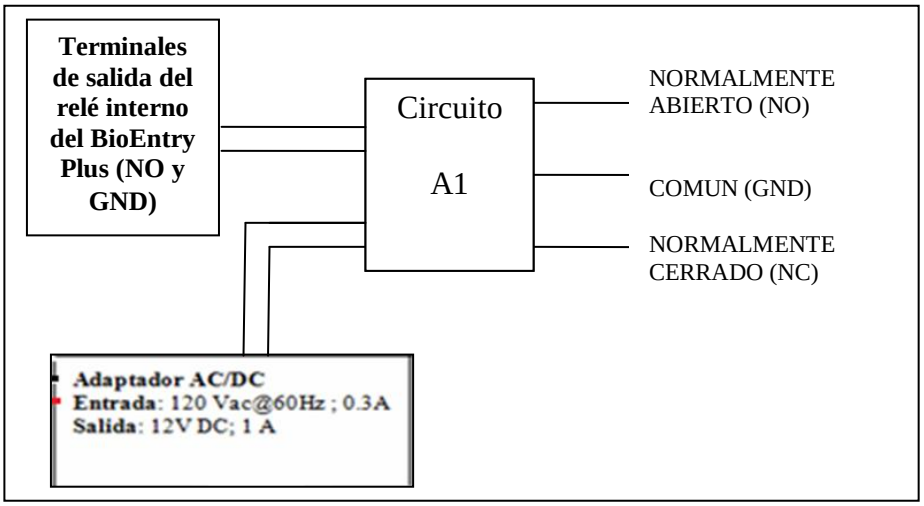
Para prolongar la vida útil de un relé, se usa un circuito de protección de contacto. Esta protección eliminará el ruido y evitará la generación de carbono en la superficie de contacto cuando se abra el relé. Ejemplos de estos componentes sinérgicos que proporcionan protección de circuito de contacto incluyen condensadores de resistencias, diodos, Zener y varistores.

Sustitución y reemplazo del nuevo relé

El esquema de la figura 6.5 contiene el modulo A1, el cual requiere en su entrada una alimentación eléctrica y la conexión de los pines de salida del relé AGN 2004H (pines 6 y 7, colores azul y blanco respectivamente) y en su salida se obtienen los pines de conexión con la cerradura de hembrilla. Cuando el relé esta desactivado hay un contacto normalmente cerrado (NC) y otro normalmente abierto (NO), al activarse el relé los contactos cambian su posición. Este circuito requiere las salidas del relé AGN 2004 y de la alimentación eléctrica. Dentro de sus especificaciones eléctricas están:

Tensión de bobina: 12 VDC

La capacidad de los contactos: 30 operaciones por minuto



6.5 Esquema del funcionamiento del modulo A1

El modulo A1 consta de los siguientes componentes electrónicos mostrados en el circuito de la figura 6.6, un diodo 1N4007, una resistencia, un diodo led y el relé SRD-12VDC-SL-C.

El nuevo relé es SRD 12 VDC-SL-C, se añadió un diodo led para visualizar el estado del modulo A1 (encendido o apagado) y el diodo 1N4007 de protección, además sirve para hacer de elemento antiretorno. El diodo de protección se conecta en paralelo a la bobina del relé. La corriente que fluye a través de la bobina del relé crea un campo magnético el cual cesa en cuanto la corriente deja de circular por ella. El diodo de protección permite al voltaje inducido conducir una breve corriente a través de la bobina (y el diodo) así el campo magnético se desvanece rápidamente.

El diodo led y la resistencia de 3,8KΩ están para indicar el funcionamiento del relé.

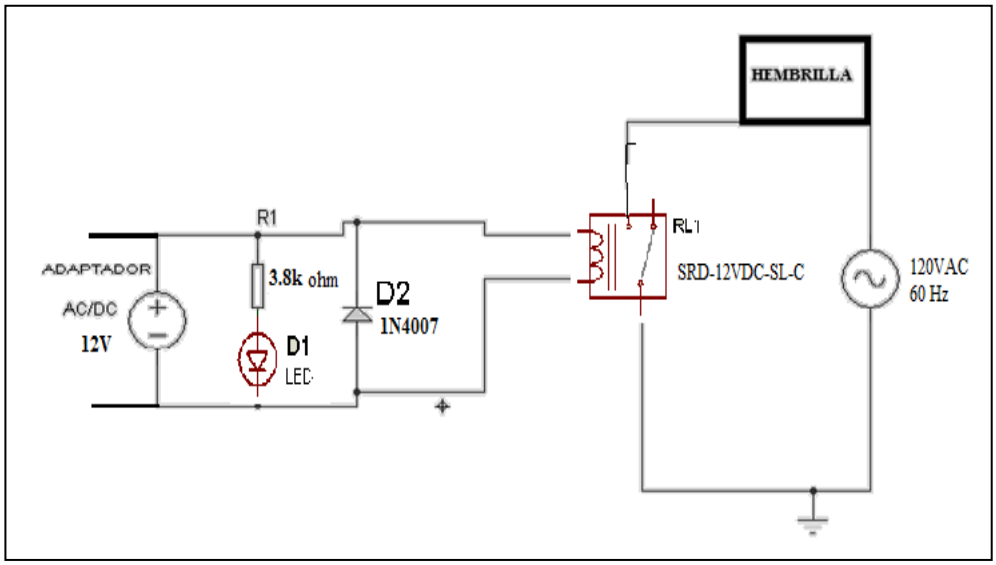


Figura 6.6. Circuito del modulo A1.

El circuito con los componentes electrónicos, fue puesto a prueba, luego de realizar el montaje del circuito en una placa de polietileno, tal como se muestra en la figura 6.7

Figura 6.7 Circuito de prueba con relé de 12V.

Es un simple circuito pero protege principalmente al equipo BioEntry Plus, su relé interno específicamente, ya que sin este circuito se colocan 120Vac entre sus terminales lo cual lo daña. Se protege del ambiente externo por medio de una caja de plástico PVC (policloruro de vinilo) que envuelve por completo el circuito de la figura 6.8.

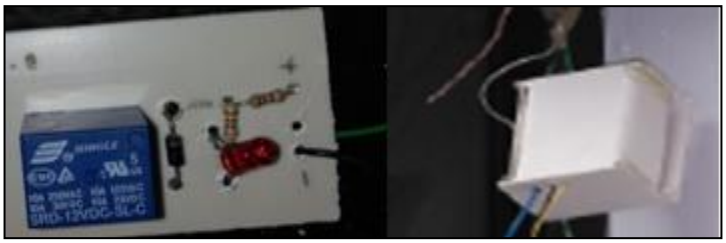


Figura 6.8 Circuito de prueba y la caja que lo contiene.

La conexión completa (Figura 6.9) debe alimentarse eléctricamente con dos fuentes individuales: una que permite encender el Bioentry Plus y otra que activa al circuito A1, que permite energizar la bobina del relé con 12 V DC. El relé cambia de posición al comprobar y verificar la huella del usuario y se activa el relé de la cerradura en la puerta, el cual acciona la hembrilla.

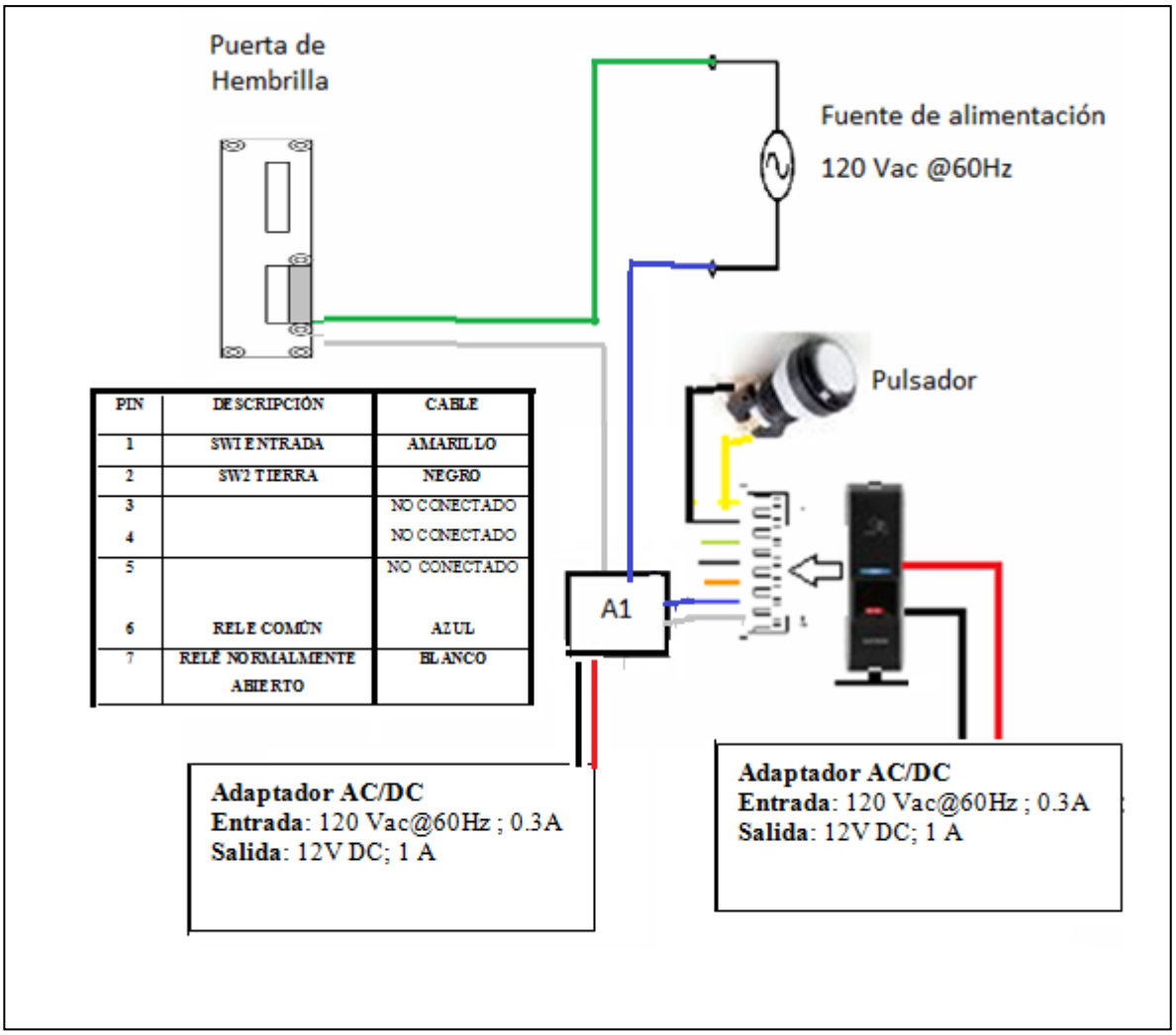


Figura 6.9. Conexión completa del circuito de hembrilla y de del modulo A1

La tarjeta con montura superficial SMD del inglés Surface Mount Device (Figura 6.9) y que activa el relé SRD-12VDC-SL-C realizará el mismo funcionamiento que el circuito de la figura 6.6, se le tendría que realizar su caja de protección.

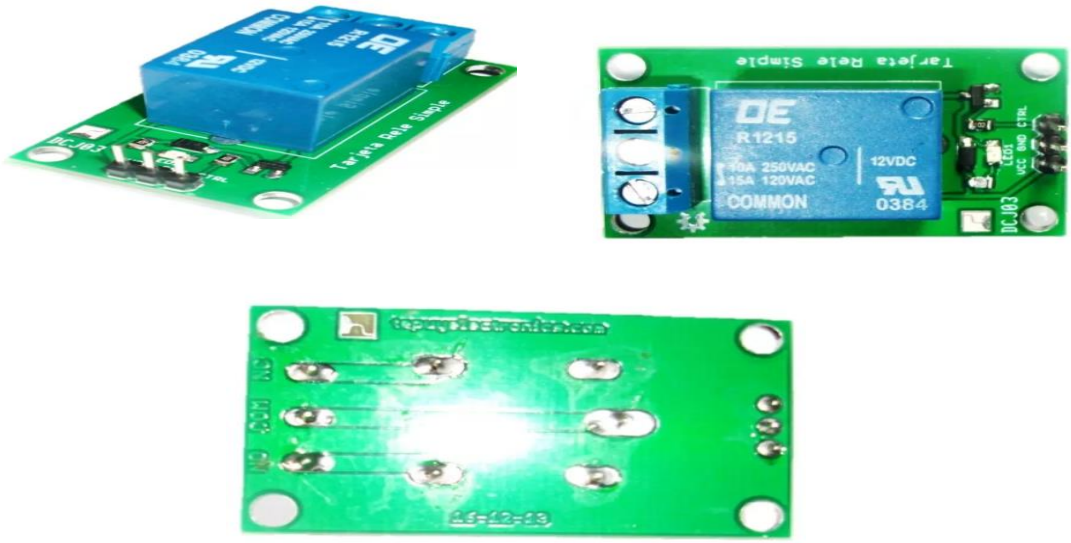


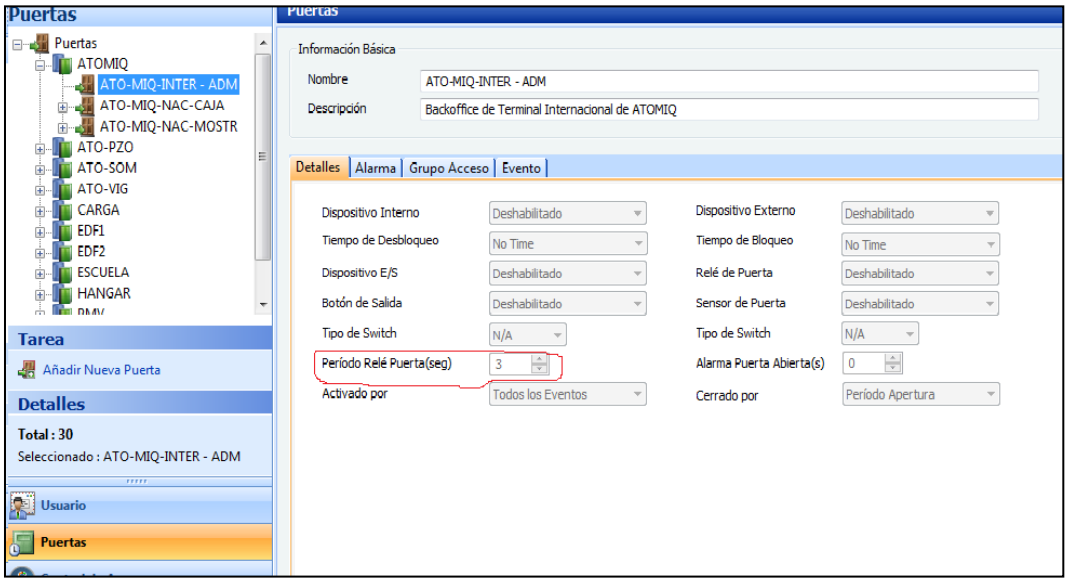
Figura 6.9: Distintos ángulos de la tarjeta SMD que contiene el nuevo Relé

Se debe convenir con el proveedor pruebas para verificar, que el fabricante presente garantía exclusiva para los productos biométricos que presenten el relé dañado, específicamente cuando están nuevos.

6.2 Disminución del tiempo de duración de apertura de las puertas por medio de la configuración usando el Software BioStar

Se ha notado un retardo en algunas puertas de acceso de la red del Sistema Biométrico, el cual puede durar entre 6 y 10 segundos para abrir o cerrar la puerta. Esta falla puede dañar la hembrilla de la puerta o los terminales del relé interno del dispositivo.

Una forma de solucionar la falla es cuando se realiza la configuración del equipo BioEntry Plus en el programa BioStar version 1.8.



Se selecciona **Puertas** en la pestaña **Detalles** se configura el **Periodo Relé Puerta(segundos)** y se cambia los segundos de duración

REFERENCIAS BIBLIOGRAFICAS

[1] Cortés O., Jimmy A. *Sistemas de Seguridad basados en Biometría.*--EN: Revista Scientia et Technica Año XVII, No 46, Diciembre 2010. p.p. 98-102 Revisión 2017

[2] Fernández G., Juan. *Diseño de una interfaz gráfica de evaluación de algoritmos de firma manuscrita (2010),* (Tesis). Madrid: Universidad Carlos III de Madrid. 2017 p 17

[3] Pallás A. Ramón. *Sensores y acondicionadores de señal*.4ta Edición. Marcombo Boixaren Editores. Barcelona, España. 2003, p.p 401-408; 423-425. Revisión 2017

[4] Durán, Federico y Otros. *Redes cableadas e inalámbricas para transmisión de datos*
Revista Científica- Instituto Politécnico Nacional, vol. 12, núm. 3, julio-septiembre, año 2008, Mexico. pp. 113-118

[5] Seijas T. José y Otros. *Instalación de una Red Estructurada para un Centro de Datos bajo los estándares y mejores prácticas de Gerencia de Proyectos del PMI (2013*), Caracas: Universidad Simón Bolívar. 2017 p 12-18

[6] American National Standards Institute. *ANSI-J-STD-607. Normas y requerimientos de Puesta a Tierra Y Puenteado para edificios Comerciales.* Consulta 2017

[7] Turmero A, Iván J**.** *Análisis de modos y efectos de falla.* Monografía 18/10/2012. Consulta Abril 2017

[8] Guía del Administrador del Software BioStar [en línea] disponible en https://www.supremainc.com/es/node/755.

[9] Guía de Instalación del Software BioStar [en línea] disponible en https://www.supremainc.com/es/node/1622

[10] Guía de Especificaciones del Software BioStar [en línea] disponible en http://www.supremasolution.com/BioStar.php

[11] Guía de Configuración del dispositivo biométrico BioEntry Plus [en línea] disponible en http://www.supremasolution.com/brochure/BioEntry_Plus.pdf

[12] Guía de Configuración del dispositivo biométrico Biostation [en línea] disponible en http://www.supremasolution.com/BioStation.php

[13] Guía de Configuración del accesorio BioMini [en línea] disponible en https://www.supremainc.com/es/node/130

[14] CODELECTRA, "Código eléctrico nacional. FONDONORMA 200:2004 (7a Revisión)". 2004.

BIBLIOGRAFIA

American National Standards Institute. ANSI-J-STD-607. Normas y requerimientos de Puesta a Tierra Y Puenteado para edificios Comerciales.

CODELECTRA, "Código eléctrico nacional. FONDONORMA 200:2004 (7a Revisión)". 2004.

Cortés O., Jimmy A. *Sistemas de Seguridad basados en Biometría.*--EN: Revista Scientia et Technica Año XVII, No 46, Diciembre 2010. p.p. 98-102 Revisión 2017

Durán, Federico y Otros. *Redes cableadas e inalámbricas para transmisión de datos*

Fernández G., Juan. *Diseño de una interfaz gráfica de evaluación de algoritmos de firma manuscrita (2010),* (Tesis). Madrid: Universidad Carlos III de Madrid. 2017 p 17

Suprema Inc. *Guía de Configuración del accesorio BioMini* [en línea] disponible en https://www.supremainc.com/es/node/130

Suprema Inc. *Guía de Configuración del dispositivo biométrico BioEntry Plus* [en línea] disponible en http://www.supremasolution.com/brochure/BioEntry_Plus.pdf

Suprema Inc. *Guía de Configuración del dispositivo biométrico Biostation* [en línea] disponible en http://www.supremasolution.com/BioStation.php

Suprema Inc. *Guía de Especificaciones del Software BioStar* [en línea] disponible en http://www.supremasolution.com/BioStar.php

Suprema Inc. *Guía de Instalación del Software BioStar* [en línea] disponible en https://www.supremainc.com/es/node/1622

Suprema Inc. *Guía del Administrador del Software BioStar* [en línea] disponible en https://www.supremainc.com/es/node/755.

Madrigal G, Carlos A. *Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares.* Revista Facultad de Ingeniería Universidad de Antioquia, núm. 39, marzo, 2007, pp. 21-32. Universidad de Antioquia. Medellín, Colombia

Pallás A. Ramón. *Sensores y acondicionadores de señal*.4ta Edición. Marcombo Boixaren Editores. Barcelona, España. 2003, p.p 401-408; 423-425. Revisión 2017

Revista Científica- Instituto Politécnico Nacional, vol. 12, núm. 3, julio-septiembre, año 2008, Mexico. pp. 113-118

Seijas T. José y Otros. *Instalación de una Red Estructurada para un Centro de Datos bajo los estándares y mejores prácticas de Gerencia de Proyectos del PMI (2013*), Caracas: Universidad Simón Bolívar. 2017 p 12-18

Turmero A, Iván J**.** *Análisis y detección de fallas y método del análisis de modos y efectos de falla.* Monografía 18/10/2012. Consulta Abril 2017

GLOSARIO

ANSI/INCITS 378: Comité Internacional de Normas de Tecnología de la Información, de sus siglas en ingles, International Committee for Information Technology Standards) y el American National Standards Institute (ANSI Instituto Americano de Estándares Nacionales de sus siglas en ingles American National Standards Institute). Esta norma define un método para representar la información de huellas dactilares utilizando el concepto de minucias.

Bioidentidad: Es una empresa especializada en sistemas biométricos de alto desempeño para el control e identificación de personas. Brinda consultoría, soluciones y productos en las áreas de biometría, documentos de identidad, tarjetas inteligentes, proximidad, control de acceso, control de asistencia, identificación en radiofrecuencia, PKI (una infraestructura de clave pública, en inglés, Public Key Infrastructure), firmas digitales, integración de sistemas, desarrollo de software y equipamiento especializado, así como en normas y estándares técnicos internacionales relacionados.

BioMini: es un escáner de huellas dactilares que se puede utilizar para el registro de usuarios.

BioStar: Es el sistema de control de acceso de última generación de Suprema Inc., basado en conectividad IP (Protocolo Internet, de sus siglas en inglés, Internet Protocol) y en seguridad biométrica. Es un exhaustivo software para administración de control de accesos que incorpora una arquitectura eficiente basada en sistema TCP/IP con lectores inteligentes IP.

FIPS 201: Publicación estándar de procesamiento de información federal 201, de sus siglas en ingles, Federal Information Processing Standard Publication 201) es un estándar del gobierno federal de los Estados Unidos que especifica los requisitos de Verificación de Identidad Personal (PIV) para empleados y contratistas federales.

HSPD-12: Política para una norma de identificación común para empleados federales y contratistas, existen amplias variaciones en la calidad y la seguridad de la identificación utilizadas para obtener acceso a instalaciones seguras donde existe la posibilidad de ataques terroristas.

Maquina Virtual: es un software que emula a un computador y puede ejecutar programas como si fuese uno real. Los procesos virtuales que se hagan allí están limitados por los recursos.

MINEX: Intercambio de Interoperabilidad de Minucias, de sus siglas en ingles, Minutiae Interoperability Exchange llevada a cabo por el NIST evalúa el funcionamiento y la interoperabilidad de los algoritmos de huella dactilar sobre el formato estándar de la huella dactilar de la base ANSI/INCITS 378.

NIST: Instituto Nacional de Estándares y Tecnología, de sus siglas en ingles, National Institute of Standards & Technology es requerida por el Gobierno de USA para la identificación y la autentificación de empleados y de contratistas federales. La misión del instituto es promover la innovación en USA y la competitividad industrial por medio de mediciones científicas, estándares, y tecnología que realcen la seguridad económica y mejoren la calidad de la vida.

OpenSSL: Sirve para cifrar los datos que se transmiten desde el servidor o al servidor con el fin de que si una cadena de datos fuese interceptada por un hacker mientras se transmite dichos datos son ilegibles ya que el hacker debería desencriptar esa información para poder sacar algún dato útil.

SFinGe: Es un método novedoso para la generación de imágenes de huellas dactilares sintéticas

Suprema Inc.: Es líder mundial en tecnología biométrica y de seguridad. Se fundamenta en algoritmos biométricos de renombre mundial e ingeniería superior. Fabrica productos de gama alta a los más altos estándares de calidad. Como proveedor de soluciones integrales. Apoya una red mundial de ventas que abarca más de 120 países de todo el mundo

ANEXOS

Apéndice A

A.1 Cableado Horizontal

El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones o viceversa. El cableado horizontal consiste de dos elementos básicos, cable horizontal y hardware de conexión tal como se observa en la figura A.1, que proporcionan los medios básicos para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones.

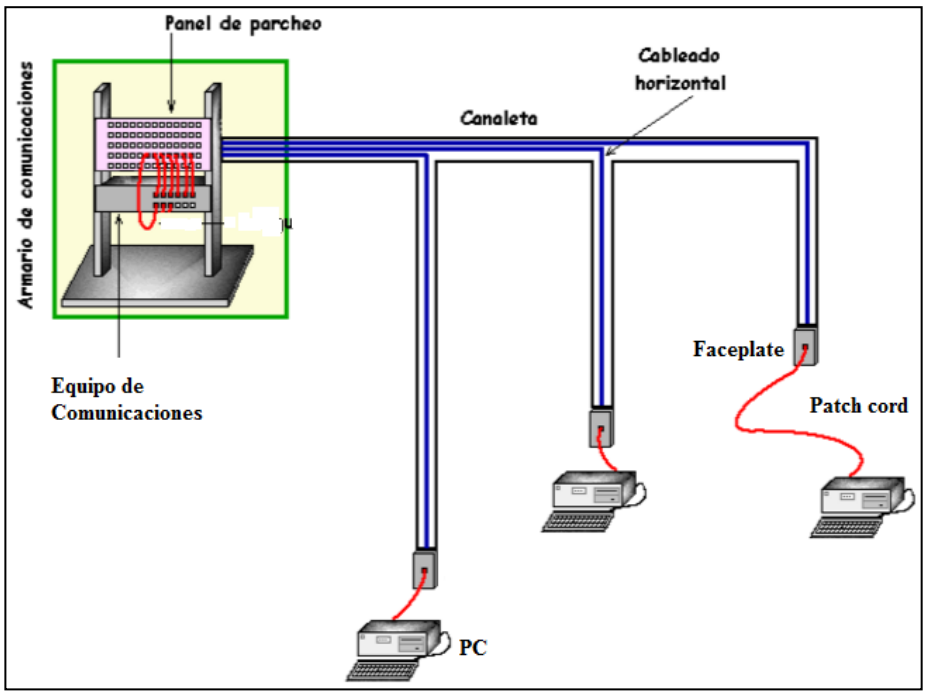


Figura A.1: Cableado Horizontal

A.2 Cableado Vertical

El Cableado Vertical o backbone es el encargado de las interconexiones entre el o los cuartos de cableados y el Centro de Datos tal como muestra la figura A.2. Este cableado como su nombre lo indica incluye la conexión vertical entre los racks de telecomunicaciones que se encuentran en cada área o piso de la

estructura, así como las terminaciones mecánicas (Jack). El tendido del backbone se realiza bajo la topología estrella.

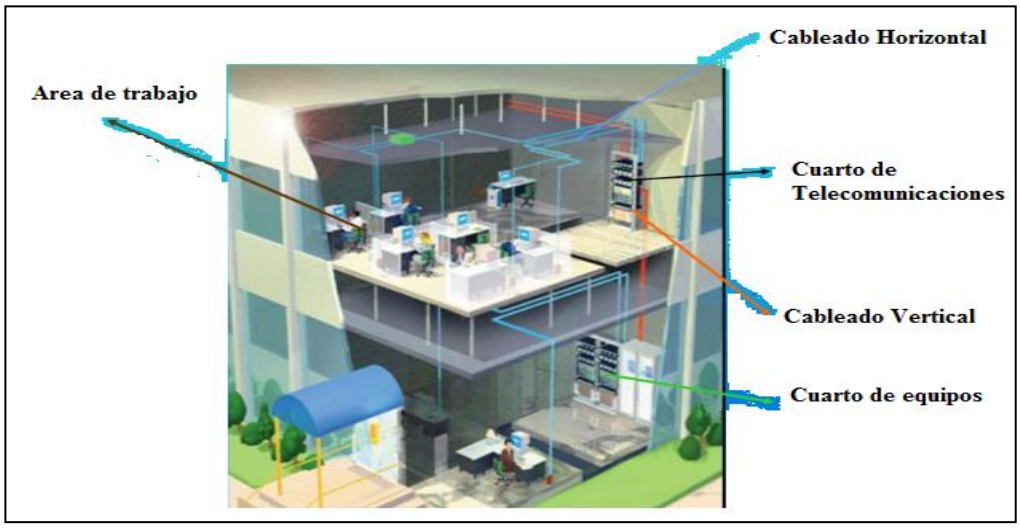


Figura A.2: Cableado Vertical

A.3 Componentes Pasivos de una Red

Son aquellos que no necesitan una fuente de energía para su correcto funcionamiento. No tienen la capacidad de controlar la corriente de un circuito.

Cableado de cobre

El cableado de cobre es un tipo de cable de par trenzado, es generalmente el más utilizado para el cableado horizontal y se pude encontrar de diferentes tipos como lo son UTP, F/UTP, S/FTP, tal como muestra la tabla A.1.

Tabla A.1: Categorías del cableado de Par Trenzado de Cobre.

Categoría de Cable	Clase	Ancho de Banda	Aplicaciones
3	C	16 MHz	10Base-T y 100Base-T4
5e	D	100 MHz	100Base-TX y 1GBase-T
6	E	250 MHz	10GBase-T
6ª	EA	500 MHz	10GBase-T
7	F	600 MHz	Teléfono, CCTV , 1GBase-TX en el mismo cable. 10GBase-T
7ª	FA	1200 MHz	Teléfono, televisión por Cable, 1GBase-TX en el mismo cable; 10GBase-T

Cableado de Fibra Óptica

Estos cables transportan por medio de pulsos modulados de luz, señales digitales, la fibra óptica cuenta con un delgado cilindro de vidrio, llamado núcleo, cubierto por un revestimiento de vidrio y sobre este se encuentra un forro de goma o plástico. Como los hilos de vidrio sólo pueden transmitir señales en una dirección, cada uno de los cables tiene dos de ellos con diferente envoltura, mientras que uno de los hilos recibe las señales, el otro las transmite. La fibra óptica resulta ideal para la transmisión de datos a distancias importantes y se puede conseguir de varios tipos: Monomodo y Multimodo (Figura A.3)

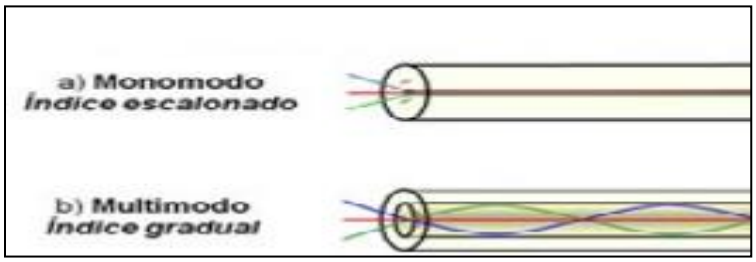


Figura A.3: Tipos de Fibra Óptica

Cable de Conexión (Patch Cord)

Son componentes pasivos del sistema de distribución de telecomunicaciones, que son utilizados para conectar los extremos del sistema. Conectan el cableado horizontal con los equipos finales en las áreas de trabajo y a su vez con los equipos que dan servicio a la red en los cuartos de cableado, la figura A.4.. Sus medidas son comprendidas entre 1 y 20m, siempre tomando en cuenta que el canal debe medir como máximo 100m. La categoría del patch cord siempre deberá ser de igual o mayor a la categoría del cableado horizontal.

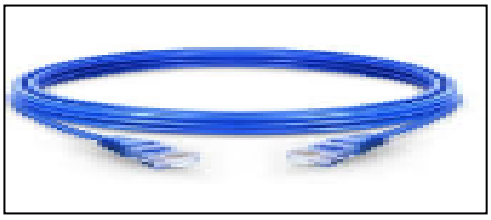


Figura A.4 Patch Cord

Faceplate

El faceplate o Placa de Pared es un accesorio para el montaje de los puntos de voz y datos en las WAN, de esta manera los puntos quedan instalados de manera estética y practica en las paredes o escritorios de las WAN (figura A.5).

Figura A.5: Faceplate

Gabinetes

Son armarios diseñados para instalar equipos activos y pasivos, este es capaz de alojar dispositivos de distintos fabricantes, principalmente: Servidores, ya que el gabinete brinda una mayor seguridad, por estar provisto de cerradura, lo cual lo hace una excelente opción para Centros de Datos (figura A.6).

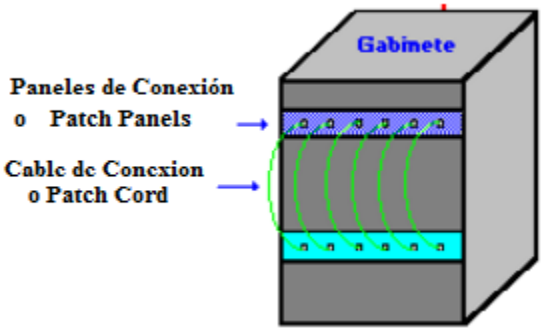


Figura A .6: Gabinete

Organizadores Horizontales y Verticales

Como su nombre lo indica, este accesorio está diseñado para organizar en los rack y gabinetes los cables, es de gran importancia y utilidad para mantener los rack y gabinetes bien organizados y la administración de los mismos sea más eficiente al momento de un mantenimiento adecuado de la Red. Los organizadores verticales van ubicados a los lados del rack de forma vertical como su nombre lo

indica, y están destinados para organizar los patch cord que interconectan los servicios en el rack, en cuanto a los organizadores. Los organizadores horizontales, son colocados de manera horizontal como su nombre lo indica bajo los patch panel y son utilizados para organizar los patch cord y darles la ruta hacia los organizadores verticales (figura A.7).

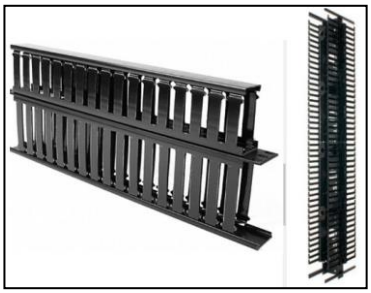


Figura A.7: Organizador Horizontal y Vertical

Paneles de Conexión (Patch Panel)

Es un soporte metálico, que recibe todos los cables del sistema de distribución del cableado horizontal en los racks o gabinetes. Estos patch panels pueden presentarse de dos formas, modulares o pre-configurados, ambos albergan los conectores finales del cableado en el cuarto de telecomunicaciones, los cuales sirven para organizar las conexiones de todo el sistema de cableado estructurado, ayudando a la mejor administración de la red (Figura A.8).

Figura A.8: Organizador Horizontal y Vertical

Estantes o Rack

Los Racks (estantes) de piso utilizados, son estructuras metálicas que permiten alojar equipos de telecomunicaciones tales como patch panels, organizadores, switches, entre otras.

Apéndice B

B.1 Funciones de Control de Acceso

Para la autenticación de usuario los dispositivos de control de acceso BioEntry Plus y Biostation incorpora avanzados y premiados algoritmos de reconocimiento de huellas dactilares para ofrecer un control de acceso seguro. El sistema combina la identificación mediante huella dactilar, con la posibilidad de utilizar tarjetas de acceso configurables, reconocimiento facial e identificación de usuario (cedula de identidad). El sistema permite una amplia variedad de modos de identificación de usuario. Aunque en el Sistema Biométrico solo es utilizada la lectura de una huella dactilar de forma exclusiva, tanto por el tipo de biométrico usado como por el costo de nuevos accesorios.

El software permite manejar toda la estructura a nivel de conexión de dispositivos biométricos instalados en las puertas de las oficinas administrativas o áreas comunes. Además de administrar a los usuarios de la base de datos para crear los distintos accesos a los grupos formados dentro de la empresa. Las siguientes gestiones enmarcan las principales funciones que se realizan con la base de datos que usa BioStar.

- Gestión de usuarios
- Gestión del grupo de acceso
- Gestión de dispositivos
- Gestión de puertas

B.2 Gestión de usuarios

El software BioStar permite gestionar usuarios de forma manual o automática. La sincronización manual está disponible para registrar diferentes subgrupos de usuarios en dispositivos particulares o cuando el número total de usuarios en la base de datos de BioStar supera los límites de un dispositivo Biostation, BioEntry Plus.

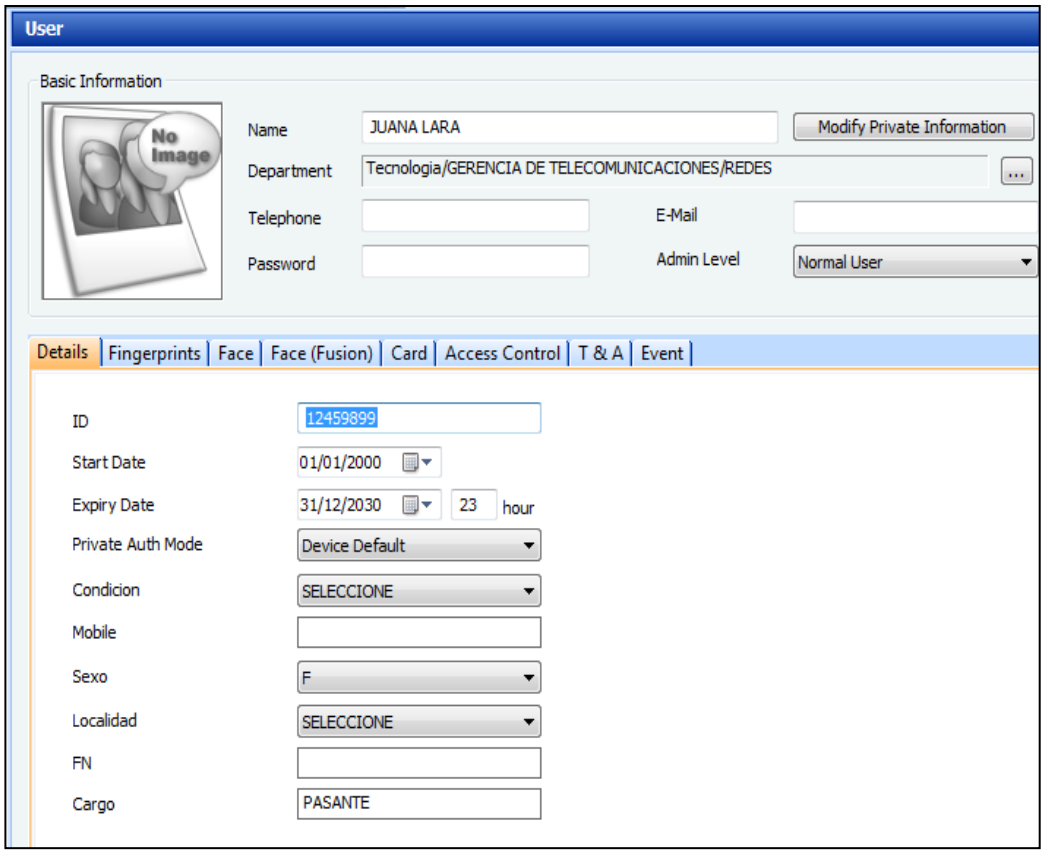


Figura B.1 Gestión de usuarios por medio del software BioStar

La sincronización automática está disponible cuando no es necesario, o no se desea, gestionar los registros de usuarios del dispositivo. El software BioStar recopila los registros de los dispositivos y permite exportar los datos a un archivo de texto para reportes personalizados, la figura B.1 muestra la etiqueta para realizar la gestión de los usuarios en este software, el cual permite un número ilimitado de registros de usuarios, la cantidad máxima de datos almacenados sólo depende de las capacidades de la base de datos subyacente y de la configuración del hardware.

B.2 Gestión del grupo de acceso

BioStar permite a los administradores crear grupos de acceso personalizados combinando permisos para zonas horarias y puertas. Con esta función, se proporciona un control de acceso personalizable y programado. BioStar permite hasta 128 zonas horarias que están formadas por un programa de siete días y dos programas vacacionales. Cada día de la zona horaria puede incluir hasta cinco períodos de tiempo diferentes. La figura B.2 permite observar la etiqueta representativa del control de acceso donde a cada dispositivo se le puede transferir la zona horaria.

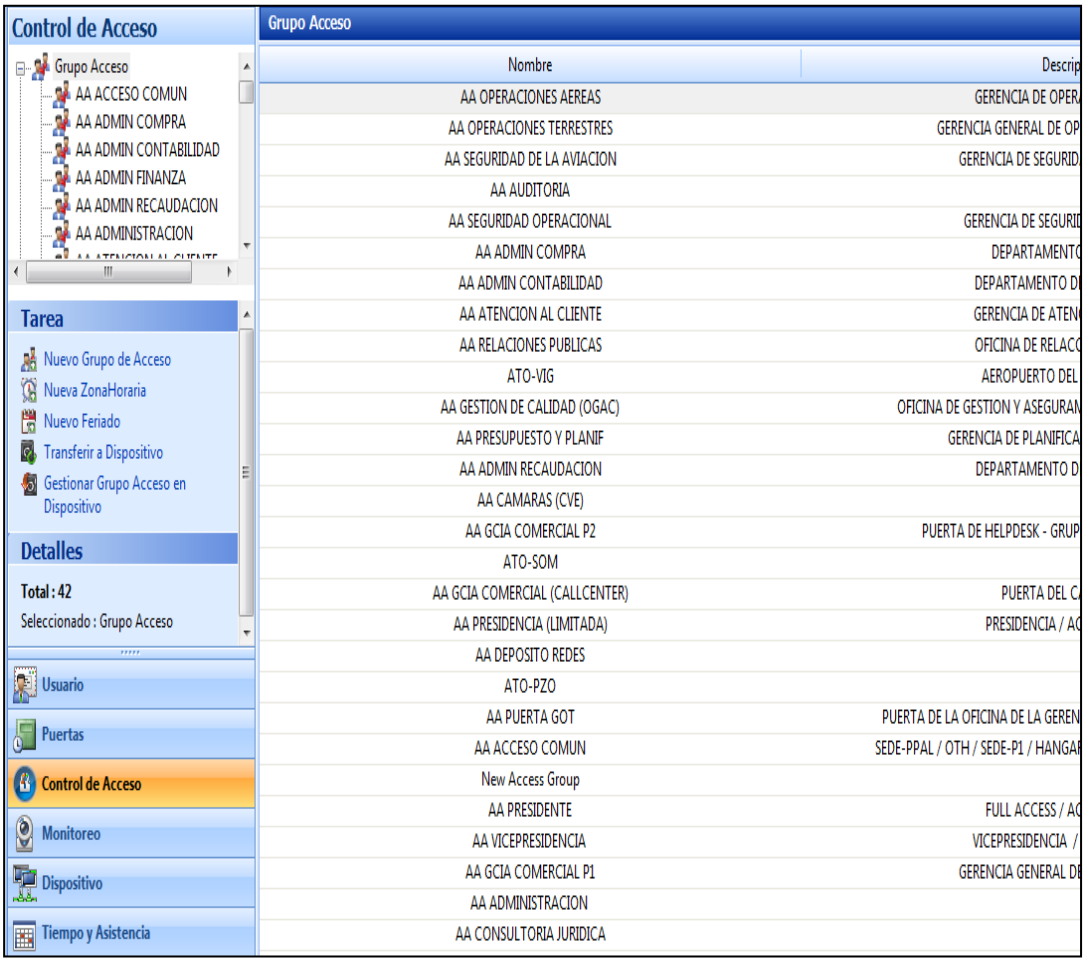


Figura B.2: Gestión del grupo de acceso

B.3 Gestión de dispositivos

BioStar permite configurar los equipos BioEntry Plus y BioStation, los relays internos, las acciones, los sonidos de entrada y salida. El sistema incluye opciones para personalizar la configuración de sonido y de pantalla de los dispositivos Biostation y la configuración del LED y del zumbido de otros dispositivos. El sistema proporciona opciones de configuración para controlar dispositivos externos, tales como cerraduras de puertas y sirenas de alarma. La figura B.3 muestra la etiqueta con las pestañas de uso frecuente: Modo de Operación, Huella, Red, Control de Acceso, Entrada, Salida.

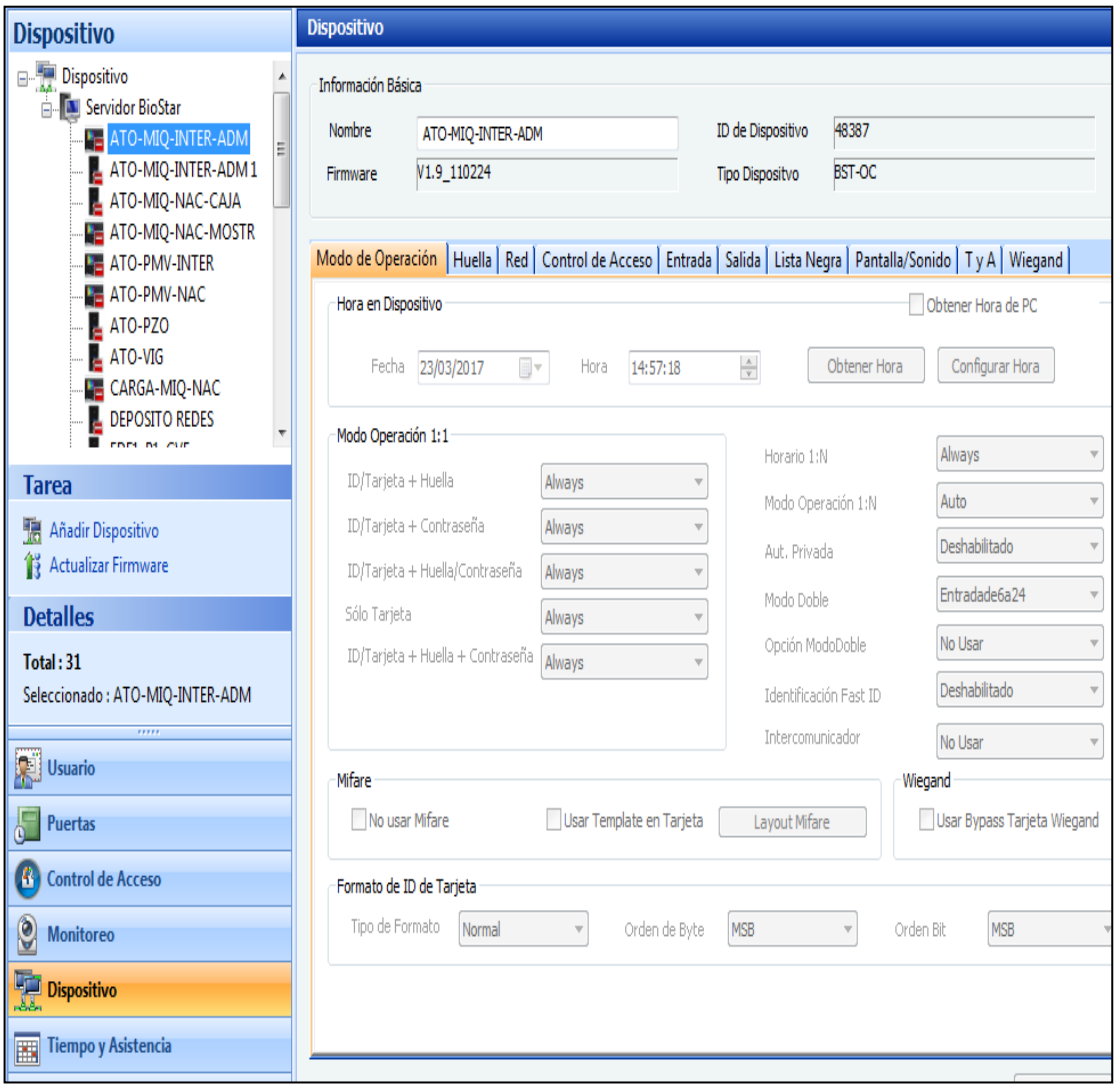


Figura B.3: Gestión de dispositivos

B.4 Gestión de Puertas

BioStar permite un control integral de puertas y de los dispositivos conectados, tales como los relays de puertas y alarmas. BioStar permite configurar de forma específica, la visualización de advertencias en la interfaz de usuario de BioStar. En la figura B.4 se observa la etiqueta **Puertas** con el árbol de cada una activa. Se observa además, las pestañas que son utilizadas para realizar la configuración: Detalles y Grupo Acceso por medio de los administradores o los operadores. los cuales pueden bloquear y desbloquear las puertas o reiniciarlas de forma remota.

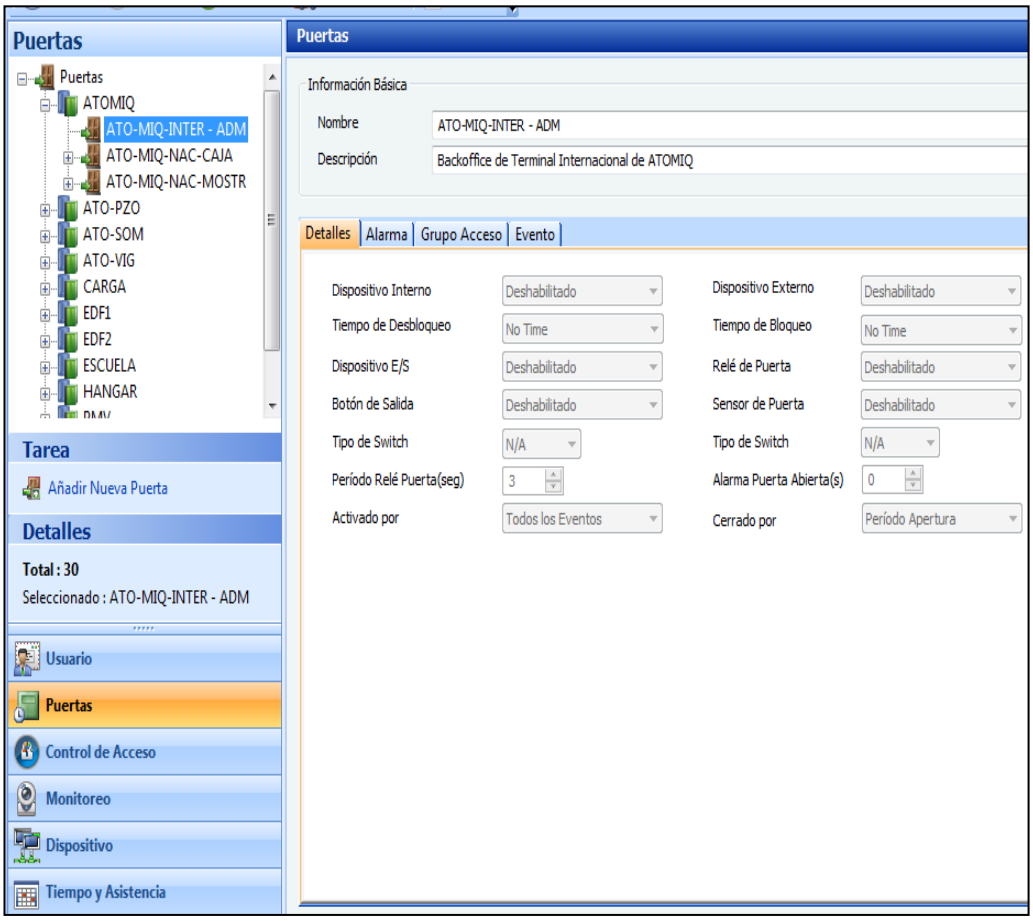


Figura B.4: Gestión de Puertas

Apéndice C

C.1 El Software BioStar Server

El Software BioStar Server Config, permite realizar un monitoreo en tiempo real actualizado de cada dispositivo conectado, el cual debe estar configurado con una IP asignada. Muestra el estado de la conexión, el puerto y clientes activos. Además de la base de datos, tipo de base de datos y autenticación de Windows. Cuando se realiza la conexión con el servidor el estatus debe de inicializarse (figura C.1) y luego cambia a conectado (figura C.2)

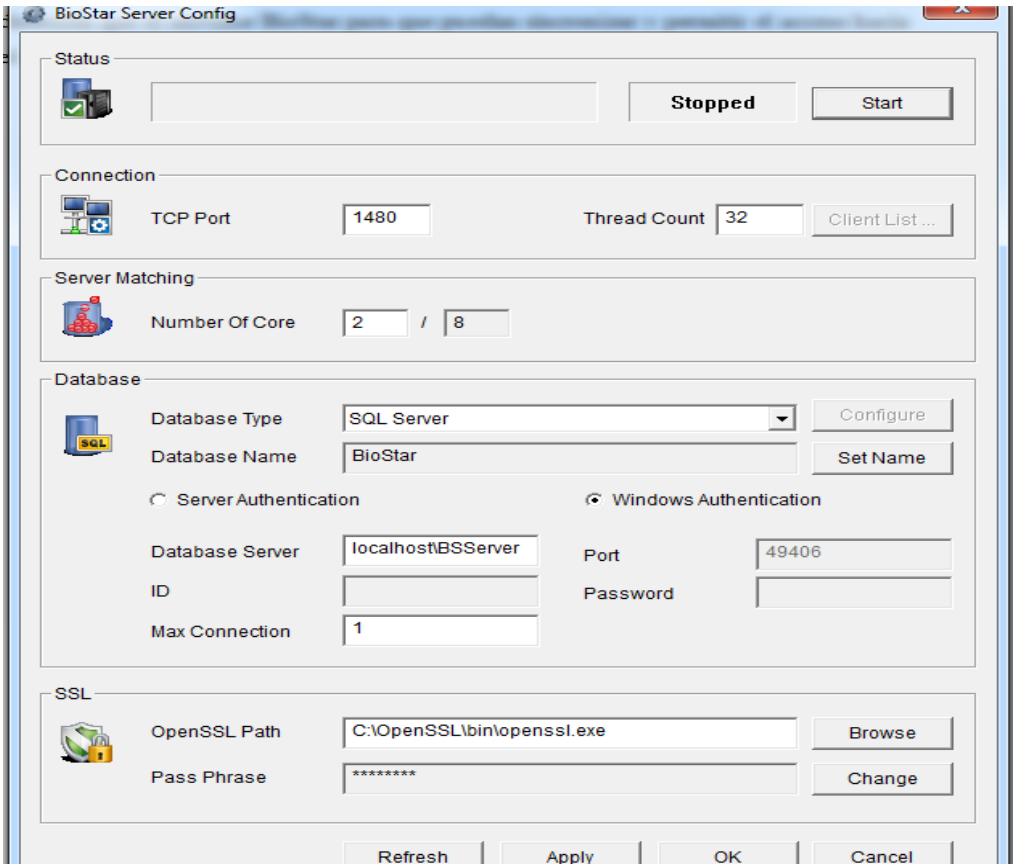


Figura C.1: Servidor BioStar Config sin conexión

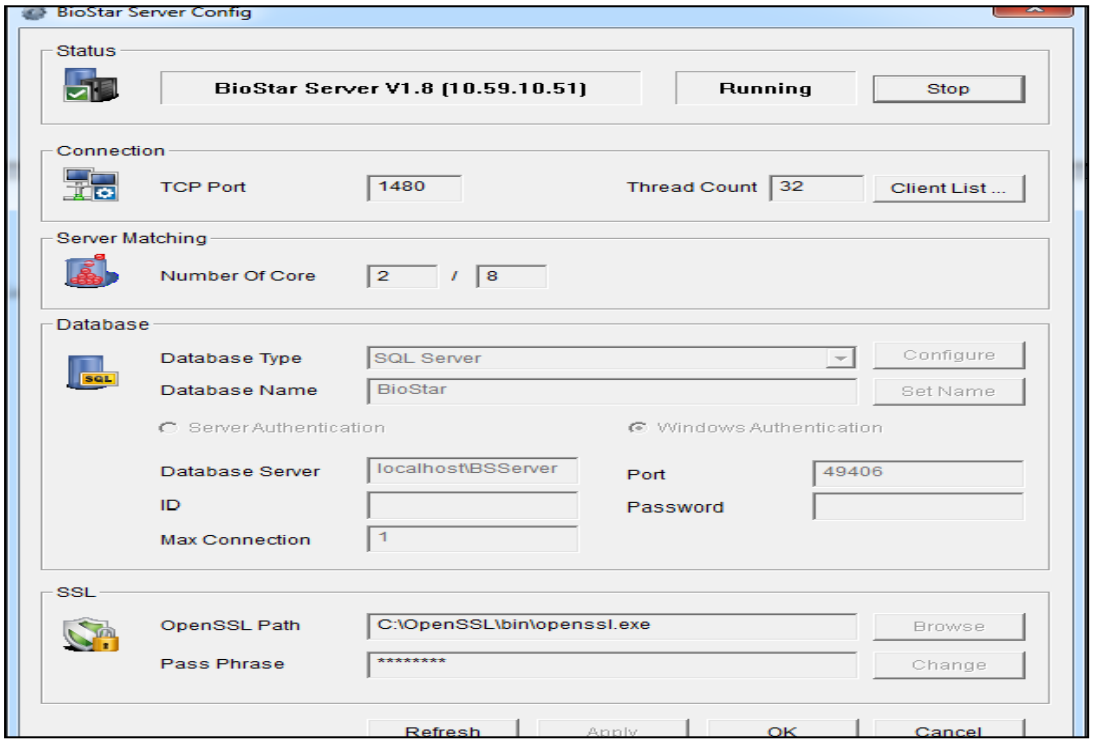


Figura C.2: Servidor BioStar Config conectado

Las versiones de BioStar usadas en una PC configurada como Cliente, son 1.3 y 1.8, todas requieren de un usuario y un password. Además, usan la configuración del adaptador de red de la PC, la ruta para configurar la dirección IP es la siguiente:

Panel de control\Redes e Internet\Conexiones de red\Estado de Conexion de area local\ Propiedades de Conexion de area local\Propiedades: Protocolo de Internet version 4 (TCP/IPv4), tal como se muestra en la figura C.3.

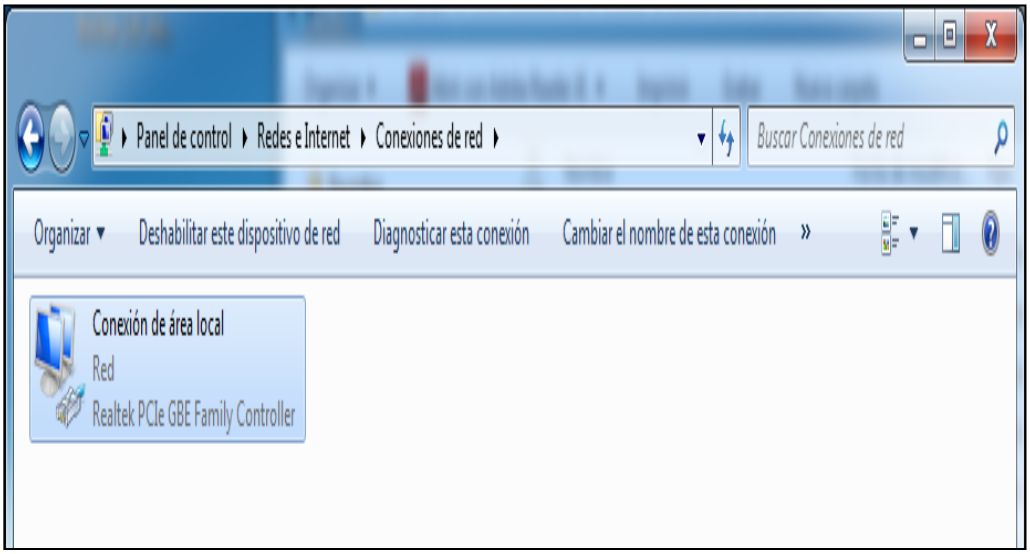


Figura C.3: Ruta para configurar la dirección IP en el adaptador de red

Luego de acceder al adaptador de red se configura la dirección IP, la mascara de subred y la puerta de enlace de la PC y se podrá accede al servidor luego de almacenar la dirección en el BioStar 1.8 (figura C.4).

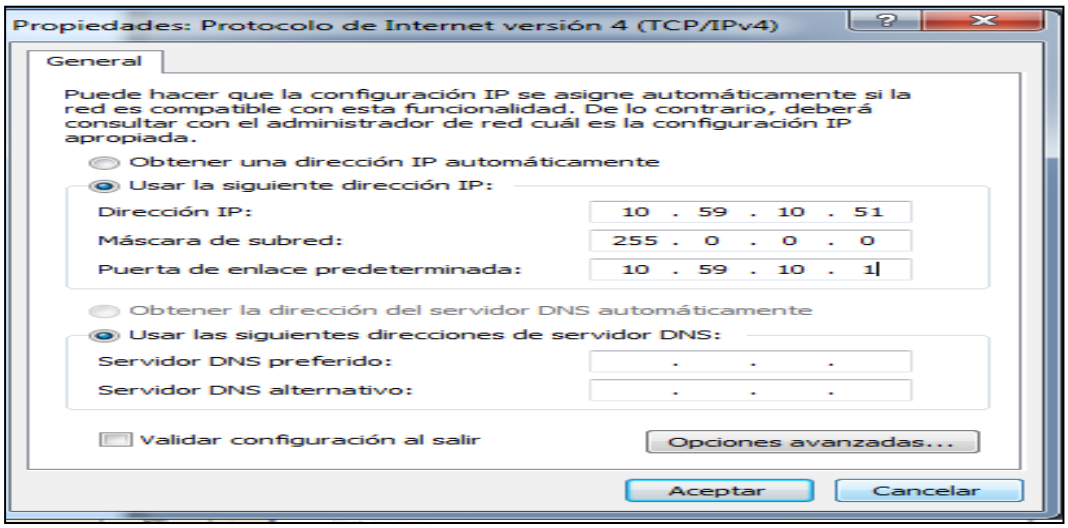


Figura C.4: Adaptador de red con la dirección IP, mascara de subred y puerta de enlace

Apéndice D

D.1 Características del modelo BioEntry Plus

- Terminal biométrico integrado con funciones avanzadas
- Comunicación TCP/IP simplifica la gestión y reduce la complejidad de la instalación
- Alta velocidad de identificación adecuado para grandes flujos de gente
- Puertos de entrada/salida configurables para sensor de puerta, alarma y cerradura
- Tamaño compacto adecuado para marcos de puertas
- Almacena información dactilar en la memoria de la tarjeta, en forma de plantilla digital.

La siguiente tablas muestra los modelos de BioEntry Plus, los tipos de sensores que escanean la huella dactilar (tabla D.1) y las especificaciones del dispositivo (tabla D.2)

Tabla D.1. Tipos de Sensor de Huella Dactilar

Tipo de sensor Captahuella		
Tipo de Sensor	Óptico	Capacitivo
Resolución (dpi)	500	508
Area de captura (mm)	16.0 x 18.0	12.8 x 18.0
Tamaño de Imagen (pixel)	288 x 288	

Tabla D.2: Especificaciones del BioEntry Plus

Especificaciones	
CPU	DSP especializado
Memoria	4 MB flash + 8MB RAM
Velocidad de identificación	Identificación contra 2000 huellas en un segundo
Capacidad de dedos	5.000 dedos
Capacidad de eventos	50.000 eventos
Interfase de red	Ethernet TCP/IP, RS485
Relay integrado	Para cerradura eléctrica o magnética, puerta automática, torniquete
Puertos E/S	Wiegand entrada/salida, 2 puertos TTL de entrada
Modos de operación	Huella, Tarjeta, Tarjeta + Huella
Interfase de usuario	LED multicolor y sonido
Temperatura de operación	-20 °C ~ 50 °C
Tamaño	50 x 160 x 37mm

Apéndice E

E.1 Características del Modelo Biostation

Figura E.1: Modelo Biostation

— Pantalla LCD de 2.5” y 16M colores muestra mensajes y fotos para fines informativos (figura E.1)..

— Comunicación TCP/IP simplifica la gestión y reduce la complejidad de la instalación Puerto de memoria USB (pendrive) simplifica la transmisión de información en entornos sin red.

— Sonido de 16 bit Hi-Fi (alta fidelidad) para efectos auditivos e instrucciones.

Tabla E.1: Tipos de Biostatión

Modelo	Biostation	V(v)	I(A)
BST-OC	V2	12	2.5

Tabla E.2: Tipos de Sensor de Huella Dactilar

Tipo de sensor Captahuella		
Tipo de sensor	Óptico	Capacitivo
Resolución (dpi)	500	508
Área de captura (mm)	16.0 x 18.0	12.8 x 18.0
Tamaño de imagen (pixel)	288 x 288	256 x 360
Tipo de sensor	Óptico	Capacitivo

Apéndice F

F.1 Características y especificaciones del BioMini

F.1. Biomini

F.2 Beneficios

- Sensor de alta calidad y durabilidad
- Sensor captahuella óptico de 500 dpi y resistente a rayaduras
- Compacto y elegante
- Diseño ergonómico y elegante
- Alta velocidad de comparación
- Compara 100000 huellas en 1 segundo (velocidad basada en procesador Core2 Duo)
- Algoritmo biométrico dactilar rápido y preciso
- Algoritmo premiado a nivel internacional (No.1 en FVC2006 y NIST MINEX)
- Tecnología biométrica estándar
- Integración sencilla y eficiente
- Kits de desarrollo para sistemas Windows 98, Me, XP, Vista, 2000, 2003, 7 y Linux

Tabla F.1 Especificaciones del BioMini

Especificaciones	
Sensor de huellas dactilares	Óptico (superficie del sensor libre de arañazos)
Resolución	500 DPI / 256 gris
Área de detección	16 x 18 mm
Tamaño de la imagen	288 x 320 píxeles
Interfaz	USB 2.0 de alta velocidad / velocidad completa, Plug & Play
O/S	Microsoft Windows, Linux
Temperatura de funcionamiento	-10 ~ 50 ℃
Certificación	CE, FCC, KCC, WHQL
Tamaño	66 x 90 x 58 mm (ancho x alto x alto)

F.3 Aplicaciones

- Seguridad en PC y redes (control de acceso biométrico en computadoras)
- Comercio electrónico (protección de transacciones)
- Control de asistencia (control de horarios de entrada y salida)
- AFIS (Sistemas Automáticos de Identificación de Impresiones Dactilares, de sus siglas en ingles, Automated Fingerprint. Identification System)
- Salud y atención médica (verificación de identidad de asegurados)
- Control de alumnos (exámenes de admisión, matrícula)
- Control de asociados (clubes, asociados civiles)
- Banca y seguros (fe de vida, cheque persona, cobranzas)

F.4 Algoritmo Utilizado para identificación de huellas dactilares

Algoritmo premiado a nivel internacional (No.1 en FVC2006 y NIST MINEX)

El algoritmo que utiliza el equipo BioEntry Plus es de vanguardia fue clasificado en primer lugar en FVC, como la mejor tecnología de reconocimiento de huellas dactilares del mundo.

El evento FVC (Fingerprint Verification Competition) es la mayor competición mundial para la evaluación de algoritmos de verificación de huellas dactilares. Esta competición tiene lugar cada dos años y es organizada por la Universidad de Bolonia (Italia), la Universidad Estadal de San José (USA), la Universidad Estatal de Michigan (USA) y la Universidad Autónoma de Madrid (España). La última edición de este evento fue realizada a finales de 2006 con la evaluación de 70 algoritmos presentados por 53 participantes de los medios industrial y académico de todo el mundo. La competencia FVC consiste en ejecutar los algoritmos participantes sobre cuatro bancos de imágenes de huellas dactilares. Para cada ejecución son calculadas un conjunto de métricas que describen la precisión y el desempeño computacional de esos algoritmos. Cada banco de imágenes es creado utilizando un sensor o lector de tecnología diferente que produce imágenes con características y calidad diferente. Los sensores utilizados en la edición FVC 2006 fueron los siguientes:

Base 1: sensor de campo eléctrico
Base 2: sensor óptico
Base 3: sensor de barredura térmica
Base 4: software SFinGe (imágenes generadas artificialmente)

La métrica más importante para evaluar un algoritmo biométrico es el EER (Igualdad de error, de sus siglas en ingles, Equal Error Rate). Esta métrica mide la probabilidad del algoritmo cometer error al decidir si dos imágenes de huellas corresponden o no al mismo dedo, o sea, estima cual es la tasa de error de verificación. El desempeño y precisión del algoritmo va a ser diferente dependiendo del tipo de sensor utilizado pues las imágenes de sensores diferentes

presentan características diferentes. Como resultado, la tasa de error de verificación puede ser muy pequeña para un sensor y muy grande para otros.

La métrica fundamental utilizada por el FVC para definir la posición de los algoritmos en la competición es el EER medio. El EER medio es el promedio de los EER en cada uno de los bancos y puede ser interpretado como la tasa media de error del algoritmo. El EER medio mide la robustez del algoritmo, o sea, su capacidad de adaptarse y funcionar correctamente cuando cambian los sensores y por tanto las características de las imágenes que tiene que comparar. En el FVC2006 el algoritmo de verificación de la Griaule obtuvo la menor tasa de EER medio entre todos los competidores, conquistando de esta manera el primero lugar.

Resultados del EER del FVC 2006 (diez primeros competidores están en la tabla F.2

Tabla F.2.Resultados del EER del FVC 2006 (diez primeros competidores)

Posición	**Algoritmo**	**ERR medio**
1	Griaule Biometrics (P066)	2,155%
2	Beijing Baixin Tong Electric Tech Co., Ltd (P045)	2,227%
3	Independent developer (Anonymous) (P009)	2,345%
4	***Suprema Inc. (P017)***	***2,481%***
5	Industry (Anonymous) (P015)	2,504%
6	Innovatrics (P074)	2,529%
7	Neurotechnologia (P058)	2,549%
8	Institute of Automation, Chinese Academy of Sciences (P131)	2,687%
9	Siemens IT Solutions and Services Biometrics Center (P067)	2,751%
10	Independent developer (Anonymous) (P101)	2,940%

Algoritmo de la prueba NIST MINEX

Suprema Inc., proveedor líder mundial de tecnología y sistemas de reconocimiento de huellas dactilares, posee el algoritmo de coincidencia y extracción de huellas dactilares ubicada en los primeros lugares de la prueba MINEX del NIST. Es una de las pruebas biométricas más importantes del mundo, la MINEX (Intercambio de Interoperabilidad de Minucias, de sus siglas en ingles, Minutiae Interoperability Exchange) llevada a cabo por el NIST (Instituto Nacional de Estándares y Tecnología, de sus siglas en ingles, National Institute of Standards & Technology) del gobierno de USA. Los resultados de la prueba del NIST, publicados el 3 de noviembre de 2008, revelaron que el algoritmo "matcher" de Suprema Inc. mostraba una tasa falsa de 0,23%, superando todos los 21 algoritmos de comparación 17 vendedores. Además, el algoritmo 'extractor' de la compañía registró una tasa falsa de 0,30%, superando los 23 algoritmos de extracción de 20 vendedores tal como se ve en la tabla F.3. Lo cual describe una mejor precisión biométrica en base a normas de inteoperación.

Tabla F.3. Resultados de la prueba del NIST

Extractor Category

Rank	Organization	False Rate
1	SUPREMA	0.30%
2	Motorola	0.32%
3	Sagem Morpho Inc.	0.32%
4	Bio Vision Co.	0.35%
5	NEC Corporation	0.35%

Matcher Category

Rank	Vendor	False Rate
1	SUPREMA	0.23%
2	Bio Vision Co.	0.25%
3	Sagem Morpho Inc.	0.27%
4	Motorola	0.29%
5	NEC Corporation	0.33%

La prueba de MINEX evalúa el funcionamiento y la interoperabilidad de los algoritmos de huella dactilar sobre el formato estándar de la huella dactilar de

la base ANSI/INCITS 378. La certificación de MINEX es requerida por el Gobierno de USA para la identificación y la autentificación de empleados y de contratistas federales. Esta certificación proporcionará a Suprema y a sus socios una ventaja en el momento de proponer sistemas biométricos relacionados con el Estándar Federal para el Tratamiento de la Información (FIPS 201) y la Directiva Presidencial 12 (HSPD 12) para la Seguridad de USA.

Acerca de la prueba MINEX

MINEX es una evaluación en curso de la plantilla de la huella dactilar INCITS 378. El programa de la prueba tiene dos premisas:

- Proporcionar medidas del funcionamiento e interoperabilidad de las capacidades de codificación y comparación de la plantilla base a los usuarios, a los vendedores y a las partes interesadas.
- Establecer la conformidad para los codificadores y las unidades de comparación de la plantilla para el Programa de Verificación de Identidad del Personal del Gobierno de Estados Unidos (PIV).

Suprema Inc. planea aplicar su tecnología certificada por MINEX a toda la gama de módulos integrados y sistemas de control de accesos de la compañía.

Acerca del NIST

Es un laboratorio de mediciones estándar que, aunque no establece normativa, depende del Departamento (Ministerio) de Comercio de los Estados Unidos. La misión del instituto es promover la innovación en USA y la competitividad industrial por medio de mediciones científicas, estándares, y tecnología que realcen la seguridad económica y mejoren la calidad de la vida.

INCITS 378

En Estados Unidos organizaciones regulatorias para elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático fueron creadas para establecer el INCITS (Comité Internacional de Normas de Tecnología de la Información, de sus siglas en ingles, International Committee for Information Technology Standards) y el American National Standards Institute (ANSI Instituto Americano de Estándares Nacionales de sus siglas en ingles American National Standards Institute). Esta norma define un método para representar la información de huellas dactilares utilizando el concepto de minucias. Define la colocación de las minucias en una huella dactilar, un formato de registro para contener los datos de minucias y extensiones opcionales para el conteo de crestas y la información de núcleo / delta.

Estándar ANSI 378: creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

FIPS 201

(Publicación estándar de procesamiento de información federal 201, de sus siglas en ingles, Federal Information Processing Standard Publication 201) es un estándar del gobierno federal de los Estados Unidos que especifica los requisitos de Verificación de Identidad Personal (PIV) para empleados y contratistas federales.

En respuesta a la HSPD-12, la División de Seguridad Informática de NIST inició un nuevo programa para mejorar la identificación y autenticación de empleados federales y contratistas para acceso a instalaciones federales y sistemas de información. FIPS 201 fue desarrollado para satisfacer los requisitos técnicos de HSPD-12, aprobado por el Secretario de Comercio, y emitido el 25 de febrero de 2005.

HSPD-12

Política para una norma de identificación común para empleados federales y contratistas, existen amplias variaciones en la calidad y la seguridad de la identificación utilizadas para obtener acceso a instalaciones seguras donde existe la posibilidad de ataques terroristas. Con el fin de eliminar estas variaciones, la política de los Estados Unidos es mejorar la seguridad, aumentar la eficiencia del Gobierno, reducir el fraude de identidad y proteger la privacidad personal estableciendo un estándar obligatorio y gubernamental para las formas seguras y confiables de identificación emitidas por el Gobierno Federal a sus empleados Y contratistas (incluyendo empleados contratistas). Esta directiva establece un estándar federal para formas seguras y confiables de identificación.

SFinGe

SFinGe es un metodo novedoso para la generación de imágenes de huellas dactilares sinteticas (“sfinge” es el italiano para “esfinge”)

¿Por qué un generador de huellas digitales sintéticas?

La prueba de un algoritmo de reconocimiento de huellas dactilares requiere una gran base de datos de muestras (miles o decenas de miles), debido a los pequeños errores que tienen que ser estimados, pero la recopilación de grandes bases de datos de las imágenes de huellas dactilares es:

- Caro tanto en términos de dinero y tiempo.
- Aburrido tanto para las personas involucradas como para los voluntarios, que suelen ser sometidos a varias sesiones de adquisición en diferentes fechas.
- Delicado debido a la legislación de privacidad que protege dichos datos personales.

SFinGe se puede utilizar para crear, a costo cero, grandes bases de datos de huellas dactilares, permitiendo así que los algoritmos de reconocimiento sean simplemente probados y optimizados. Por ejemplo, una base de datos que contiene 100.000 huellas dactilares puede ser generada por lotes en aproximadamente un día en una sola PC.

Las huellas digitales generadas por SFinGe son extremadamente realistas: en FVC2000 , FVC2002 , FVC2004 y FVC2006 , se generó sintéticamente una de las cuatro bases de datos utilizadas (DB4) y en los cuatro concursos los algoritmos participantes se desempeñaron en DB4 de forma similar a los otros DBs.

El método de generación

Los filtros de tipo espacial Gabor se utilizan para ampliar iterativamente una imagen inicialmente vacía que contiene solo una o pocas semillas. Un modelo de imagen direccional, cuyas entradas son el número y ubicación de los núcleos y deltas de huellas dactilares, se utiliza para ajustar los filtros. Las imágenes de huellas digitales muy realistas se obtienen después de la fase final de ruido y representación.

El método de generación realiza secuencialmente los siguientes pasos:

Generación de mapas direccionales (pasos 1-2 en la animación)

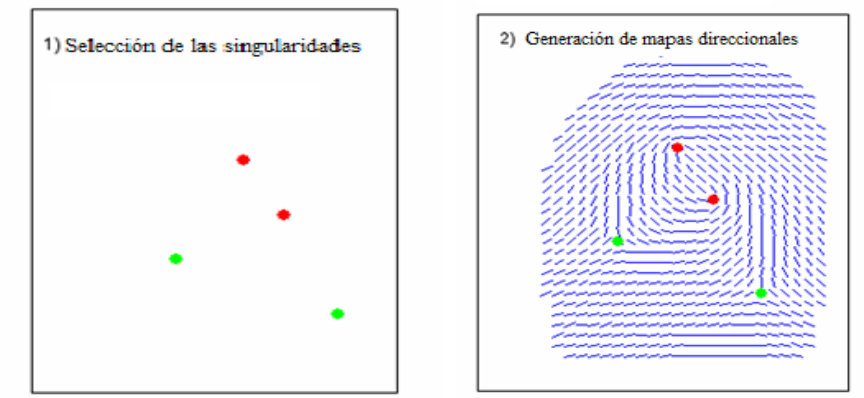


Figura F.2. Generación de mapas direccionales

En el paso 1) a partir de las posiciones de núcleos y deltas, explora un modelo de flujo matemático para generar un mapa direccional coherente. El paso 2 crea un mapa de direcciones sobre la base de algunos criterios heurísticos, es decir, conseguir objetivos fundamentales en algoritmos con buenos tiempos de ejecución y buenas soluciones, usualmente las óptimas (Figura F.2)

Generación de patrones de cresta (paso 3 en la animación)

Figura F.3. Generación de patrones de cresta

En la etapa 3, el patrón de línea de cresta y las minucias se crean a través de un filtrado lineal variante de espacio. La salida es una imagen de huella digital muy clara y casi binaria (Figura F.3).

Ruido y representación (Paso 4 en la animación)

El paso 4 agrega un cierto ruido específico y produce una representación realista de escala de grises de la huella digital (Figura F.4).

Figura F.4 Ruido y representación

Apéndice G

G.1 TIPOS DE BASES PARA LA INSTALACION DE CERRADURAS ELECTROMAGNETICAS

Base plana:

La cerradura electromagnética se instala en el marco de la puerta, utilizando el soporte plano que viene con la cerradura, el cual debe colocarse en la esquina opuesta a las bisagras, normalmente en posición horizontal, la colocación vertical podrá considerarse en situaciones donde el marco superior sea más débil que el perfil vertical, fijando la placa móvil a la puerta alineada con la cerradura.

Base L:

En esta base de la figura G.1 se coloca el electroimán cuando no puede colocarse directamente en el marco, fijando la placa móvil a la puerta alineada con la cerradura.

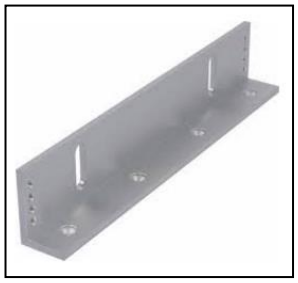


Figura G.1 Base tipo L

G.3 Base Tipo U:

Esta base es utilizada para puertas de vidrio completo sin marco, se coloca la base en el vidrio, asi como se indica en la figura G.2, donde a su vez se coloca la pieza móvil, esto ya que no podemos colocarla directamente al vidrio. El electroimán se coloca en el marco de forma antes explicada.

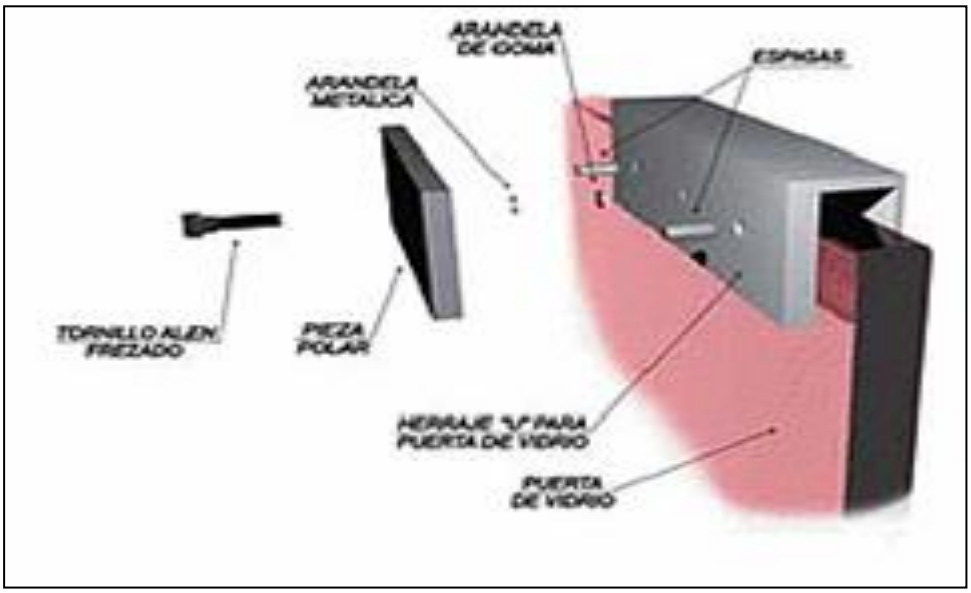


Figura G.2: Base tipo U

Base tipo Z:

Para instalar en puertas que abren hacia adentro, en aquellos casos que se requiera proteger el electroimán con una instalación interior, éste deberá colocarse sobre puesto en la pared arriba del marco de la puerta en la esquina opuesta a las bisagras, y un soporte en “Z”, como se indica en la figura G.3

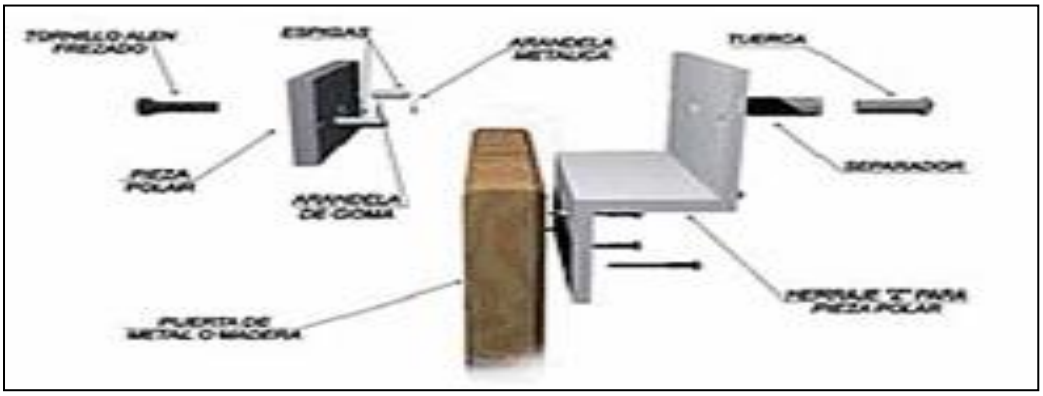
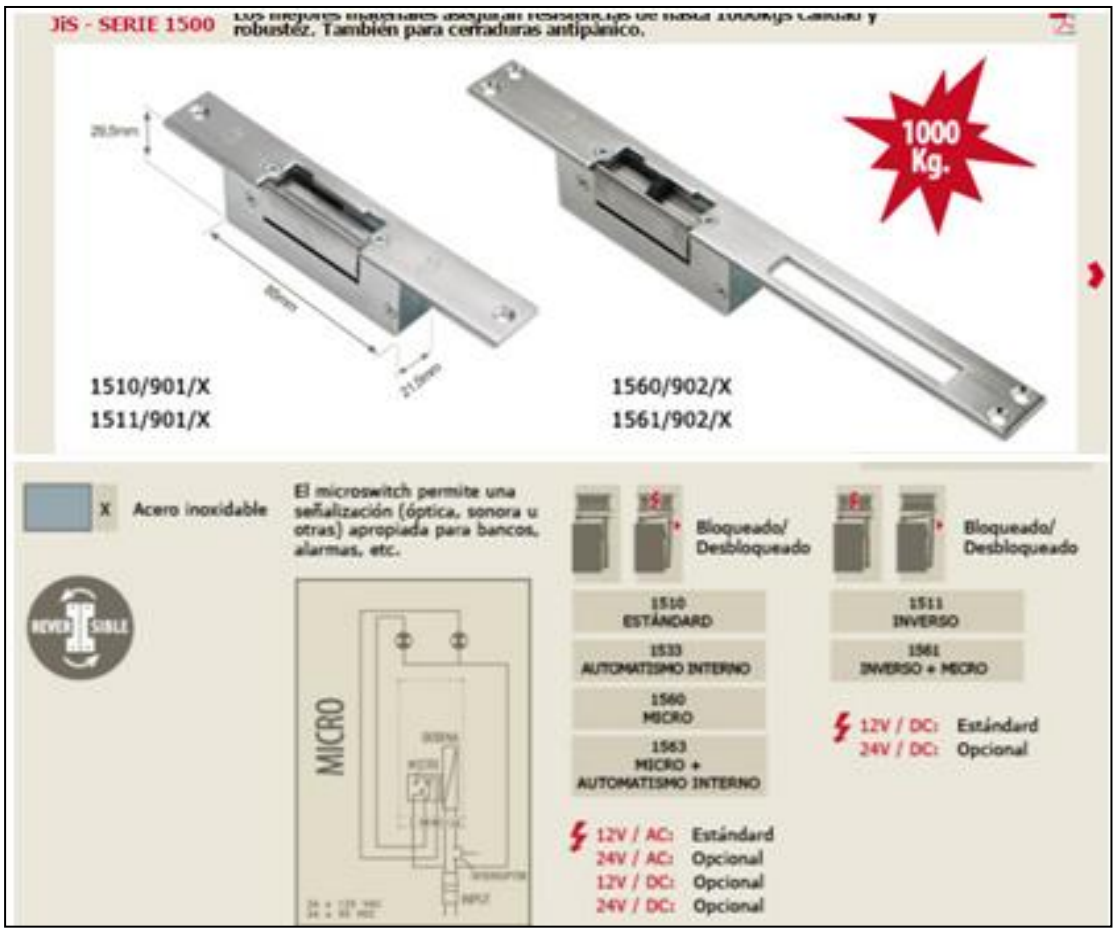


Figura G.3: Base tipo Z

Apéndice H

H.1 Especificaciones de la puerta de hembrilla Puerta de Hembrilla



Apéndice I

Manual del componente AGN 2004H

TYPES

1. Standard PC board terminal

Nominal coil voltage	Single side stable	1 coil latching	High sensitivity single side stable
	Part No.	Part No.	Part No.
1.5V DC	AGN2001H	AGN2101H	AGN2601H
3V DC	AGN20003	AGN21003	AGN26003
4.5V DC	AGN2004H	AGN2104H	AGN2604H
6V DC	AGN20006	AGN21006	AGN26006
9V DC	AGN20009	AGN21009	AGN26009
12V DC	AGN20012	AGN21012	AGN26012
24V DC	AGN20024	AGN21024	AGN26024

Standard packing: Tube: 50 pcs.; Case: 1,000 pcs.

2. Surface-mount terminal

1) Tube packing

Nominal coil voltage	Single side stable	1 coil latching	High sensitivity single side stable
	Part No.	Part No.	Part No.
1.5V DC	AGN200□1H	AGN210□1H	AGN260□1H
3V DC	AGN200□03	AGN210□03	AGN260□03
4.5V DC	AGN200□4H	AGN210□4H	AGN260□4H
6V DC	AGN200□06	AGN210□06	AGN260□06
9V DC	AGN200□09	AGN210□09	AGN260□09
12V DC	AGN200□12	AGN210□12	AGN260□12
24V DC	AGN200□24	AGN210□24	AGN260□24

□: For each surface-mounted terminal identification, input the following letter. A type: A, S type: S
Standard packing: Tube: 50 pcs.; Case: 1,000 pcs.

2) Tape and reel packing

Nominal coil voltage	Single side stable	1 coil latching	High sensitivity single side stable
	Part No.	Part No.	Part No.
1.5V DC	AGN200□1HZ	AGN210□1HZ	AGN260□1HZ
3V DC	AGN200□03Z	AGN210□03Z	AGN260□03Z
4.5V DC	AGN200□4HZ	AGN210□4HZ	AGN260□4HZ
6V DC	AGN200□06Z	AGN210□06Z	AGN260□06Z
9V DC	AGN200□09Z	AGN210□09Z	AGN260□09Z
12V DC	AGN200□12Z	AGN210□12Z	AGN260□12Z
24V DC	AGN200□24Z	AGN210□24Z	AGN260□24Z

□: For each surface-mounted terminal identification, input the following letter. A type: A, S type: S
Standard packing: Tape and reel: 500 pcs.; Case: 1,000 pcs.
Notes: 1. Tape and reel packing symbol "-Z" is not marked on the relay. "X" type tape and reel packing (picked from 1/2/3/4-pin side) is also available.
2. Please inquire if you require a relay, between 1.5 and 24 V DC, with a voltage not listed.

RATING

1. Coil data

1) Single side stable type

Nominal coil voltage	Pick-up voltage (at 20°C 68°F)	Drop-out voltage (at 20°C 68°F)	Nominal operating current [±10%] (at 20°C 68°F)	Coil resistance [±10%] (at 20°C 68°F)	Nominal operating power	Max. applied voltage (at 20°C 68°F)
1.5V DC	75%V or less of nominal voltage* (Initial)	10%V or more of nominal voltage* (Initial)	93.8mA	16Ω	140mW	150%V of nominal voltage
3V DC			46.7mA	64.2Ω		
4.5V DC			31mA	145Ω		
6V DC			23.3mA	257Ω		
9V DC			15.5mA	579Ω		
12V DC			11.7mA	1,028Ω		
24V DC			9.6mA	2,504Ω	230mW	120%V of nominal voltage

2) 1 coil latching type

Nominal coil voltage	Set voltage (at 20°C 68°F)	Reset voltage (at 20°C 68°F)	Nominal operating current [±10%] (at 20°C 68°F)	Coil resistance [±10%] (at 20°C 68°F)	Nominal operating power	Max. applied voltage (at 20°C 68°F)
1.5V DC	75%V or less of nominal voltage* (Initial)	75%V or less of nominal voltage* (Initial)	66.7mA	22.5Ω	100mW	150%V of nominal voltage
3V DC			33.3mA	90Ω		
4.5V DC			22.2mA	202.5Ω		
6V DC			16.7mA	360Ω		
9V DC			11.1mA	810Ω		
12V DC			8.3mA	1,440Ω		
24V DC			5.0mA	4,800Ω	120mW	

*Pulse drive (JIS C 5442-1996)

GN (AGN)

3) High sensitivity single side stable type

Nominal coil voltage	Set voltage (at 20°C 68°F)	Reset voltage (at 20°C 68°F)	Nominal operating current [±10%] (at 20°C 68°F)	Coil resistance [±10%] (at 20°C 68°F)	Nominal operating power	Max. applied voltage (at 20°C 68°F)
1.5V DC	80%V or less of nominal voltage* (Initial)	10%V or more of nominal voltage* (Initial)	66.7mA	22.5Ω	100mW	150%V of nominal voltage
3V DC			33.3mA	90Ω		
4.5V DC			22.2mA	202.5Ω		
6V DC			16.7mA	360Ω		
9V DC			11.1mA	810Ω		
12V DC			8.3mA	1,440Ω		
24V DC			5.0mA	4,800Ω	120mW	120%V of nominal voltage

*Pulse drive (JIS C 5442-1996)

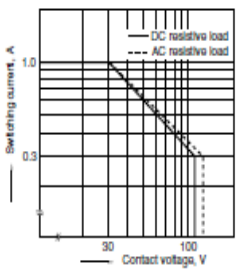
2. Specifications

Characteristics	Item		Specifications
Contact	Arrangement		2 Form C
	Initial contact resistance, max.		Max. 100 mΩ (By voltage drop 6 V DC 1A)
	Contact material		Stationary contact: AgPd+Au clad Movable contact: AgPd
Rating	Nominal switching capacity		1 A 30 V DC, 0.3 A 125 V AC (resistive load)
	Max. switching power		30 W (DC), 37.5 V A (AC) (resistive load)
	Max. switching voltage		110 V DC, 125 V AC
	Max. switching current		1 A
	Min. switching capacity (Reference value)*1		10μA 10 mV DC
	Nominal operating power	Single side stable	140mW (1.5 to 12 V DC), 230mW (24 V DC)
		High sensitivity single side stable type	100mW (1.5 to 12 V DC), 120mW (24 V DC)
		1 coil latching	
Electrical characteristics	Insulation resistance (Initial)		Min. 1,000MΩ (at 500V DC) Measurement at same location as "Initial breakdown voltage" section.
	Breakdown voltage (Initial)	Between open contacts	750 Vrms for 1min. (Detection current: 10mA)
		Between contact and coil	1,500 Vrms for 1min. (Detection current: 10mA)
		Between contact sets	1,000 Vrms for 1min. (Detection current: 10mA)
	Surge breakdown voltage (Initial)	Between open contacts	1,500 V (10×160μs) (FCC Part 68)
		Between contacts and coil	2,500 V (2×10μs) (Telcordia)
	Temperature rise (at 20°C 68°F)		Max. 50°C (By resistive method, nominal coil voltage applied to the coil; contact carrying current: 1A.)
	Operate time [Set time] (at 20°C 68°F)		Max. 4 ms [Max. 4 ms] (Nominal coil voltage applied to the coil, excluding contact bounce time.)
	Release time [Reset time] (at 20°C 68°F)		Max. 4 ms [Max. 4 ms] (Nominal coil voltage applied to the coil, excluding contact bounce time.) (without diode)
Mechanical characteristics	Shock resistance	Functional	Min. 750 m/s² (Half-wave pulse of sine wave: 6 ms; detection time: 10μs.)
		Destructive	Min. 1,000 m/s² (Half-wave pulse of sine wave: 6 ms.)
	Vibration resistance	Functional	10 to 55 Hz at double amplitude of 3.3 mm (Detection time: 10μs.)
		Destructive	10 to 55 Hz at double amplitude of 5 mm
Expected life	Mechanical		Min. 5×10^7 (at 180 cpm)
	Electrical		Min. 10^5 (1 A 30 V DC resistive), 10^5 (0.3 A 125 V AC resistive) (at 20 cpm)
Conditions	Conditions for operation, transport and storage*2		Ambient temperature: (Single side stable, 1 coil latching type) –40°C to +85°C –40°F to +185°F (High sensitivity single side stable type) –40°C to +70°C –40°F to +158°F Humidity: 5 to 85% R.H. (Not freezing and condensing at low temperature)
	Max. operating speed (at rated load)		20 cpm
Unit weight			Approx. 1 g .035 oz

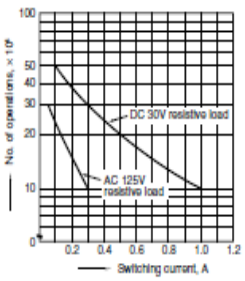
Notes: *1 This value can change due to the switching frequency, environmental conditions, and desired reliability level, therefore it is recommended to check this with the actual load.
*2 Refer to 6. Conditions for operation, transport and storage mentioned in AMBIENT ENVIRONMENT (Page 24).

REFERENCE DATA

1. Max. switching capacity

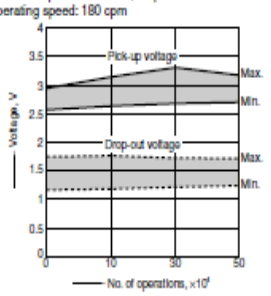


2. Life curve



3. Mechanical life

Tested sample: AGN2004H, 15 pcs.
Operating speed: 180 cpm



I.2 Manual del componente relé SRD-12VDC-SL-C.

SONGLE RELAY

松乐继电器 SONGLE RELAY	RELAY ISO9002	SRD

1. MAIN FEATURES

- Switching capacity available by 10A in spite of small size design for highdensity P.C. board mounting technique.
- UL,CUL,TUV recognized.
- Selection of plastic material for high temperature and better chemical solution performance.
- Sealed types available.
- Simple relay magnetic circuit to meet low cost of mass production.

2. APPLICATIONS

- Domestic appliance, office machine, audio, equipment, automobile, etc.
  (Remote control TV receiver, monitor display, audio equipment high rushing current use application.)

3. ORDERING INFORMATION

SRD	XX VDC	S	L	C
Model of relay	Nominal coil voltage	Structure	Coil sensitivity	Contact form
SRD	03, 05, 06, 09, 12, 24, 48VDC	S:Sealed type	L:0.36W	A:1 form A
				B:1 form B
		P:Plux free type	D:0.45W	C:1 form C

4. RATING

CCC	FILE NUMBER:CH0052885-2000	7A/240VDC
CCC	FILE NUMBER:CH0036746-99	10A/250VDC
UL/CUL	FILE NUMBER: E167996	10A/125VAC 28VDC
TUV	FILE NUMBER: R9933789	10A/240VAC 28VDC

5. DIMENSION(unit:mm) DRILLING(unit:mm) WIRING DIAGRAM