UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS EN LOS REGISTROS DEL PERSONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DETERMINADAS EMPRESAS DE AMBATO".

Proyecto de Trabajo de Graduación. Modalidad: SEMINARIO, presentado previo a la obtención del título de Ingeniero en Sistemas Computaciones e Informáticos.

AUTOR: GEOVANNY FERNANDO FONSECA VELASCO.

PROFESOR REVISOR: ING RENE TERÁN.

AMBATO – ECUADOR

2013

Aprobación del tutor

En mi calidad de Tutor del trabajo de investigación sobre el tema: "**VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS EN LOS REGISTROS DEL PERSONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DETERMINADAS EMPRESAS DE AMBATO**", del señor GEOVANNY FERNANDO FONSECA VELASCO egresado de la carrera de INGENIERÍA EN SISTEMAS INFORMÁTICOS Y COMPUTACIONALES, de la FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL, de la UNIVERSIDAD TÉCNICA DE AMBATO, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de Tercer Nivel de la UNIVERSIDAD TÉCNICA DE AMBATO.

Ambato, Noviembre 4 del 2013

Atentamente,

…….

Ing. Rene Terán

Autoría del trabajo

Los criterios emitidos en el trabajo de investigación titulada "VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS EN LOS REGISTROS DEL PERSONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DETERMINADAS EMPRESAS DE AMBATO", es absolutamente original, autentico y personal en tal virtud los contenidos, ideas, análisis, conclusiones y propuesta son de exclusiva responsabilidad de mi persona, como autor de este trabajo de grado.

Ambato, Noviembre 4 del 2013

Atentamente,

…….

Geovanny Fernando Fonseca Velasco

C.I. 1600521825

Aprobación de la comisión

La comisión calificadora del presente trabajo conforma por los señores docentes ……..……, reviso y aprobó el informe final del trabajo de graduación titulado **"VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS EN LOS REGISTROS DEL PERSONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DETERMINADAS EMPRESAS DE AMBATO",** presentado por el señor **GEOVANNY FERNANDO FONSECA VELASCO** de acuerdo al Art. 17 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Edison Álvarez
PRESIDENTE DEL TRIBUNAL

Ing. Clay Aldas
DOCENTE CALIFICADOR

Ing. Teresa Freire
DOCENTE CALIFICADOR

Dedicatoria

Dedico el presente trabajo de investigación a mis Padres, quien con su amor, sacrificio, y paciencia, han sabido Orientarme para caminar por las difíciles etapas de mi vida, Nexo que ha sido vital en mis estudios; y a mi querido Incondicional hermano quien con su cariño siempre me ha incentivado en mi desarrollo como persona y así terminar mi carrera profesional con éxito y satisfacción.

Geovanny Fonseca

Agradecimiento

Dedico esta tesis a DIOS porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar, a mis padres y mi hermano quien con sus apoyos me incentivaron para mi desarrollo personal y profesional, a lo largo de mi vida han velado por mi bienestar y educación siendo pilares fundamentales en cada momento, es por ello que soy lo que soy ahora, también quiero agradecer a mis compañeros de curso que supieron brindarme sus conocimientos y experiencias, para poder realizar este proyecto, y a la Universidad Técnica de Ambato que me dio la oportunidad de especializarme e incrementar mis conocimientos en lo que concierne a Ingeniero en Sistemas Computacionales.

También exteriorizo un agradecimiento especial a mí Director de Tesis ya que gracias a su profesionalismo y experiencia me ha sabido orientar y dirigir en el desarrollo de este proyecto de investigación.

Geovanny Fonseca

Índice

Índice de figuras

Índice de tablas

Resumen Ejecutivo

El presente trabajo de investigación tiene como objetivo principal Analizar las posibles vulnerabilidades de los Relojes Biométricos en el registro del personal a fin de realizar un manual para su uso procedimientos de utilización y configuraciones.

La investigación se fundamenta en información necesaria para obtener los resultados de las posibles vulnerabilidades existentes en los relojes biométricos mediante estudios de campo y experimentos como la suplantación de una huella dactilar y su comprobación en los dispositivos. De igual manera se utilizaron herramientas informáticas para la identificación de vulnerabilidades.

Como parte de la experimentación se ha realizado la suplantación de una huella dactilar dando como conclusión que si se puede realizar marcaciones con huellas falsas siempre y cuando estén hechas de material flexible.

El trabajo es de gran importancia porque contribuirá con la información de las posibles vulnerabilidades que tiene los Relojes Biométricos, para la cual se ha planteado un manual de configuración y de procedimientos de utilización y configuración del dispositivo y su software de control ATTENDANCE MANAGEMENT.

Introducción

El objetivo de cualquier sistema de control de acceso es permitir la entrada del personal autorizado a sitios o lugares específicos. Los sistemas de acceso basados en tarjetas de proximidad o carnets pueden autorizar pero no pueden distinguir quien porta el carnet o tarjetas de proximidad. Los sistemas que usan números de identificación personal sólo requieren que un individuo se sepa un número específico para otorgarle acceso. Los dispositivos biométricos verifican la identidad de una persona mediante características físicas únicas e inalterables como las dimensiones, características o medidas de las huellas digitales u otros tipos de identificaciones como son el reconocimiento de la voz, Iris, Palma de la mano Rostros faciales.

El presente trabajo de investigación se centra en el diseño de un "Manual de buenas prácticas de los Sistemas Biométricos" para definir y organizar las funciones que debe cumplir los usuarios finales. Los sistemas biométricos se pueden definir como dispositivos o equipos para el control de personal que son utilizados por muchas empresas para controlar la asistencia de sus empleados.

La implantación de un Manual se convierte en el objetivo primordial de este trabajo; con el fin de que el gerente guie correctamente todas y cada una de las, funciones en la utilización del reloj biométrico debido que todo sistema esta propenso a vulnerabilidades por ende puede causar daño. Estas vulnerabilidades no solo se refieren a ataques realizados por software pues también se involucra el factor humano.

La información presentada a continuación, se ha dividido en capítulos para facilitar la comprensión del contenido de este trabajo:

- **En el primer capítulo** se describe de manera general el tema de investigación del análisis de las vulnerabilidades del reloj biométrico, iniciando desde la problemática general que presenta sus respectivas variables.

- **En el segundo capítulo** se detalla el marco teórico, el mismo que contiene toda la información general, comenzando con los antecedentes y el problema de investigación.

- **El tercer capítulo** hace referencia a la metodología aplicada en la investigación, los estudios necesarios a realizarse para sustentar la correcta ejecución, el establecimiento del campo, la población, muestra y un análisis contencioso de las variables de investigación.

- **En el cuarto capítulo** se establecen los parámetros necesarios con el objetivo de obtener resultados, los cuales permitirá tener la información suficiente para interpretar y verificar la hipótesis, por lo tanto se pueden confirmar que las vulnerabilidades a los sistemas biométricos puede alterar la información registrada en los dispositivos biométricos.

- **En el quinto capítulo** se desarrollan las conclusiones y recomendaciones que se obtuvieron de los resultados de la ejecución de la investigación.

- Finalmente en el **capítulo seis** se enmarca la propuesta del investigador, lo cual está desarrollada en base a una investigación de las vulnerabilidades de los sistemas biométricos.

CAPÍTULO I

El Problema

1.1. Tema

"Vulnerabilidades de los relojes biométricos en los registros del personal para proteger la información en determinadas empresas de Ambato".

1.2. Planteamiento del problema

1.2.1. Contextualización

Los sistemas biométricos para ser eficaces tienen que disponer de una configuración correcta; los empleados deben sentirse motivados para llevar a cabo de manera satisfactoria el registro en los relojes biométricos.

El conocimiento de uso de los dispositivos y su configuración es una parte fundamental para un buen funcionamiento de los sistemas biométricos, los mismos que disponen de procesos complejos en el cual se relacionan los mecanismos psicofisiológicos con el aspecto intelectual de la comprensión, puesto que se trata del reconocimiento de características.

En el mundo moderno cada vez hay una mayor necesidad de mejorar los métodos de seguridad informática y del control de personal, entre otras. Actualmente los sistemas son

eficaces pero aún le falta aceptación en el medio, estando limitado principalmente por los costos de algunos productos.

Los relojes biométricos a nivel mundial cada día van adquiriendo nuevas tecnologías como el reconocimiento de voz y rasgos faciales, por este motivo las empresas deberán estar preparadas y predispuestas a la utilización de estos dispositivos para el control de personal. Considerando que en nuestro medio existen diversas empresas importantes que disponen de sistemas biométricos por ende se ha visto la necesidad de realizar el estudio de análisis de vulnerabilidades y guías de buenas prácticas para minimizar posibles impactos, pérdidas y manipulación de información.

Se tuvo conocimientos qué en varias empresas ecuatorianas como: ESUMAN CIA. LTDA., CASA PAZMIÑO S.A., ATIEMPOFFICE CIA. LTDA., entre otras las cuales distribuyen relojes biométricos, las mismas que se esfuerzan en comprender las necesidades de cada empresa las cuales ofrecen dispositivos biométricos de huellas dactilares o de diferentes características para el control de asistencia al personal**.**

Los sistemas biométricos seguirán creciendo en toda institución pública o privada para controlar a sus empleados viéndose reflejado en un notable crecimiento de adquisición de relojes biométricos por parte de empresas ambateñas.

Algunos de los principales problemas de los relojes biométricos es la incertidumbre de vulnerabilidades, la disponibilidad de la información de las marcaciones, la falta de seguridad de acceso con los relojes, entre otros por lo que existe la necesidad de disponer de una guía para la utilización correcta del software del reloj y la manipulación de la información, él mismo que ayudará a realizar un estudio exhaustivo de las políticas de seguridad así como mejorara los procesos y por ende la calidad de servicios.

1.2.2. Análisis Critico

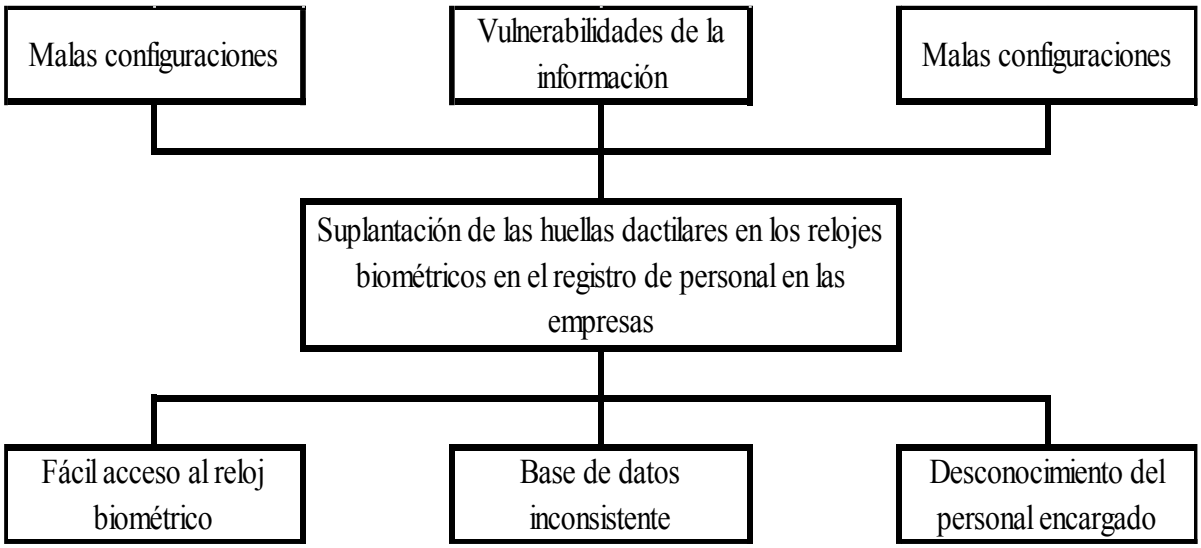


Figura 1.1. Árbol de Problemas
Fuente: Investigador

El fácil acceso a los relojes biométricos puede provocar alteraciones, manipulaciones y daños, los mismos como pueden ser lógicos y físicos causando incertidumbre a los administradores y a los empleados por no contar con una información adecuada de los registros y disponibilidad del reloj biométrico.

Considerando que el reloj biométrico almacena temporalmente los registros, la mayoría de los sistemas biométricos disponen de una base de datos centralizada en un computador personal, que puede ser manipulada fácilmente si no se cuenta con un adecuado control de acceso.

1.2.3. Prognosis

La falencia del análisis de vulnerabilidades de los relojes biométricos podría provocar la manipulación de los registros y presentar datos falsos en los ingresos y salidas del personal, causando molestias ante el personal y posibles pérdidas económicas.

Por esta razón es necesario implementar políticas y controles que permitan proteger al equipo e información en las empresas.

1.2.4. Formulación del Problema

¿Cómo influye la vulnerabilidad de los relojes biométricos en el registro del personal para la protección de la información de las empresas de Ambato en el último trimestre del año 2011?

1.2.5. Preguntas Directrices

¿Cómo controlar el fácil acceso a los relojes biométricos que pueden provocar alteraciones, manipulaciones y daños, los mismos como pueden ser lógicos y físicos causando incertidumbre a los administradores y a los empleados?

¿Cómo almacena temporalmente los registros en los relojes biométricos que disponen de una base de datos centralizada en un computador?

1.2.6. Delimitación

- **Teórico**
  - **Campo:** Tecnología y la informática
  - **Área:** Tecnología
  - **Aspecto:** Análisis de los relojes biométricos

Tiempo

La presente investigación se desarrollara en un periodo de 6 meses a partir de la aprobación del proyecto.

Espacio

La presente investigación se desarrolla en la empresa ATIEMPOFFICE CIA. LTDA. De la ciudad de Ambato donde cuentan con los sistemas biométricos Marca BIOSYSTEM.

1.3. Justificación

El proyecto desde el punto de vista técnico es realizable, ya que está la disposición en el mercado los relojes biométricos de la marca BIOSYSTEM, como también del software de control de personal ATTENDANCE MANAGEMENT que dará soporte a la implementación de los objetivos.

Además existe en la actualidad el personal técnico capacitado para el manejo de los equipos, los mismos que se encuentra ubicados específicamente en el área de soporte técnico de la empresa ATIEMPOFFICE CIA. LTDA. Que permite atender de manera oportuna los requerimientos de los clientes.

Los sistemas biométricos desempeñan un papel de vital significación en las empresas o instituciones privadas y públicas en su actividad, ya que es un medio fundamental de reconocimiento de huellas para el registro del personal siendo de gran importancia.

Finalmente se cuenta con el apoyo de las empresas que disponen de equipos biométricos, sus empleados, docentes los conocimientos adquiridos durante la carrera universitaria y la experiencia lograda durante las prácticas. Se posee además bibliografía y recursos para la investigación de campo, aspectos que hacen viable la investigación.

Los sistemas biométricos nos ayudan a corregir las deficiencias que se tienen en los registros de información de cada empleado, así como a desarrollar los mecanismos de configuración pero estos sistemas pueden ser mal manipulados o disponer de vulnerabilidades que afecten los registros.

1.4. Objetivo

1.4.1. General

Analizar las vulnerabilidades de los Relojes Biométricos en el registro del personal para la protección de la información en determinadas Empresas de Ambato.

1.4.2. Específicos

- Realizar un estudio de campo para determinar las vulnerabilidades más comunes que presentan los relojes biométricos en el registro de personal en determinadas Empresas de Ambato.

- Analizar, estudiar y seleccionar las posibles herramientas de búsqueda de vulnerabilidades para los relojes biométricos.

- Plantear una propuesta que permita el diseño de un manual de procedimientos y configuración de utilización y configuración de los relojes biométricos y del software que lo administra para evitar la manipulación de la información.

CAPÍTULO II

Marco Teórico

2.1. Antecedentes investigativos

Al revisar en los archivos de trabajos de investigación en las bibliotecas de la UNIVERSIDAD TÉCNICA DE AMBATO no se han encontrado investigaciones similares.

2.2. Fundamentación legal

Según la **CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR DEL 2008** dice en la sección tercera de **"Comunicación e Información".**

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

- El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

- Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior."

Mientras en la sección novena – "Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

Art. 53.- Las empresas, instituciones y organismos que presten servicios públicos deberán incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras, y poner en práctica sistemas de atención y reparación."

Y en el capítulo octavo – "Derechos de protección"

Art. 78.- Las víctimas de infracciones penales gozarán de protección especial, se les garantizará su no revictimización, particularmente en la obtención y valoración de las pruebas, y se las protegerá de cualquier amenaza u otras formas de intimidación. Se adoptarán mecanismos para una reparación integral que incluirá, sin dilaciones, el conocimiento de la verdad de los hechos y la restitución, indemnización, rehabilitación, garantía de no repetición y satisfacción del derecho violado.

Sección octava - Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

- Generar, adaptar y difundir conocimientos científicos y tecnológicos.
- Recuperar, fortalecer y potenciar los saberes ancestrales.
- Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento.

Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo."

2.3. Fundamentación teórica

2.3.1. Fundamentación variable independiente

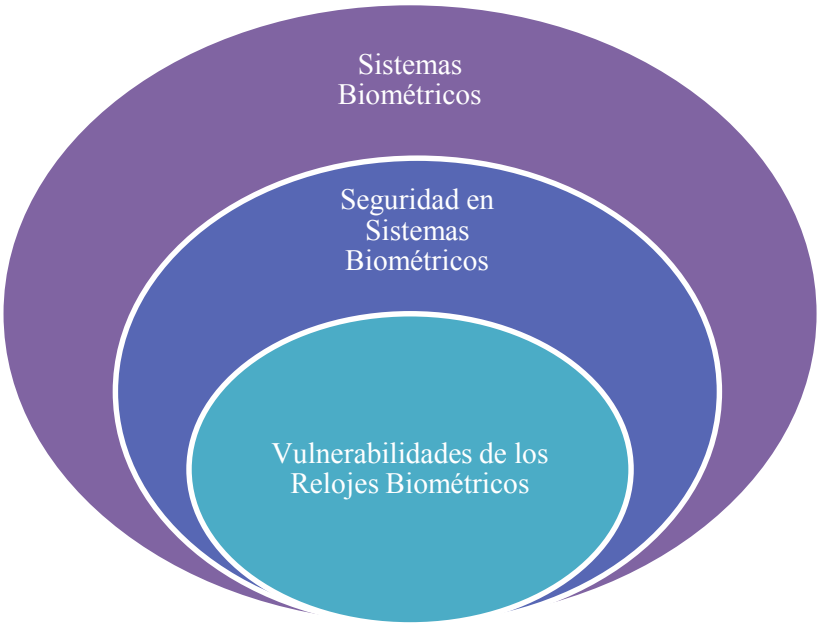


Figura 2.1. Subordinación de la variable independiente

Fuente: Investigador

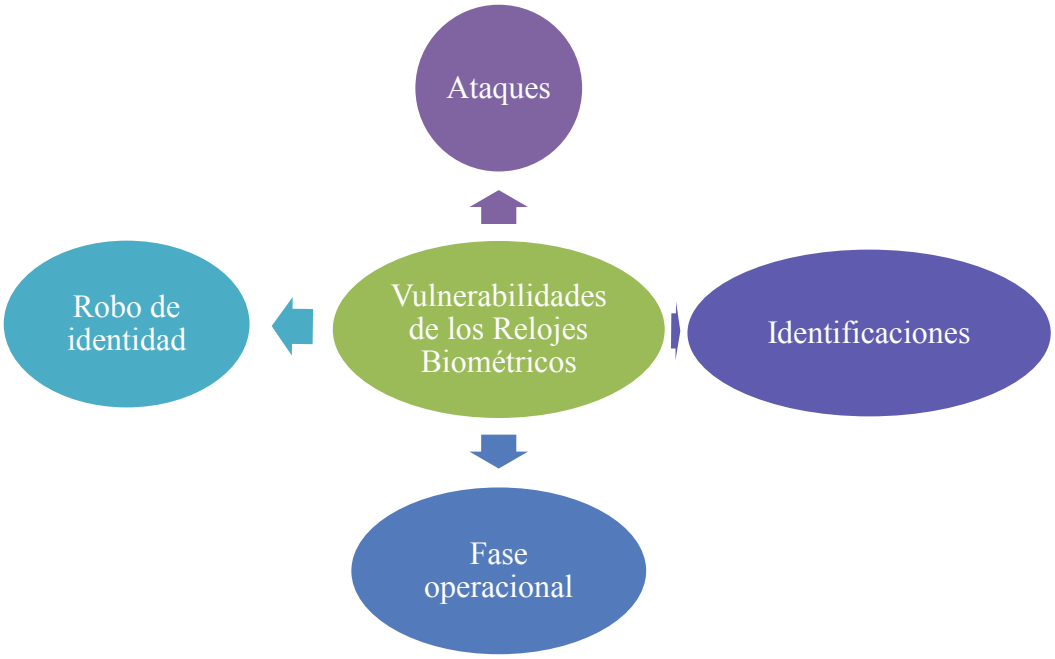


Figura 2.2. Análisis de la variable independiente

Fuente: Investigador

Sistemas Biométricos

La biometría aplicada al campo de la seguridad consiste en la utilización de tecnologías que hacen uso de métodos automáticos para el reconocimiento de seres humanos basados en uno o más rasgos físicos intrínsecos. La palabra biometría tiene dos significados:

- El concepto tradicional de biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas;
- Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos.

El término se deriva de las palabras griegas "bios" de vida y "metron" de medida por lo que se refiere a todo los equipos biométricos que mide e identifica las características propias de las personas.

El propósito de las tecnologías biométricas es fundamentalmente la identificación y la autentificación en control de accesos. Las huellas dactilares y los patrones faciales son las características físicas más fiables y empleadas en la actualidad en sistemas de seguridad.

Aunque no son las únicas: las retinas, el iris, las venas de la mano, la geometría de la palma de la mano o la voz son otras que también se emplean.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Otros autores:

Entenderemos por sistema biométrico a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. [1]

Un sistema biométrico es básicamente un sistema reconocedor de patrones que opera del siguiente modo: captura un rasgo biométrico, extrae un conjunto de características y lo comprar con otro conjunto de características almacenado en una base de datos. Dependiendo de su finalidad, en un sistema biométrico puede actuar en dos modos: verificación e identificación [2]

La biometría no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas es procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso.

El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autenticación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se refieren para medir características corporales o de comportamiento de las personas con el objeto de establecer identidad.

La biometría busca la automatización de tareas que involucran el reconocimiento del individuo. Las maquinas no evalúan ningún otro factor al tomar una decisión, solo se evalúa la identidad. Esto resta cualquier factor sujeto que pueda comprometer la seguridad.

Los sistemas de seguridad o sistemas biométricos utilizan tres métodos de autenticación:

- Contraseña.
- Unas llaves o tarjeta de proximidad.
- Huellas dactilares.

Funcionamiento

En un sistema de Biometria típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías

actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 999,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa:

- Tasa de falso positivo (False Acceptance Rate o FAR),
- Tasa de falso negativo (False NonMatch Rate o FNMR,
- Tasa de falso rechazo (False Rejection Rate o FRR), y
- Fallo de tasa de alistamiento (Failure-to-enroll Rate, FTR o FER).

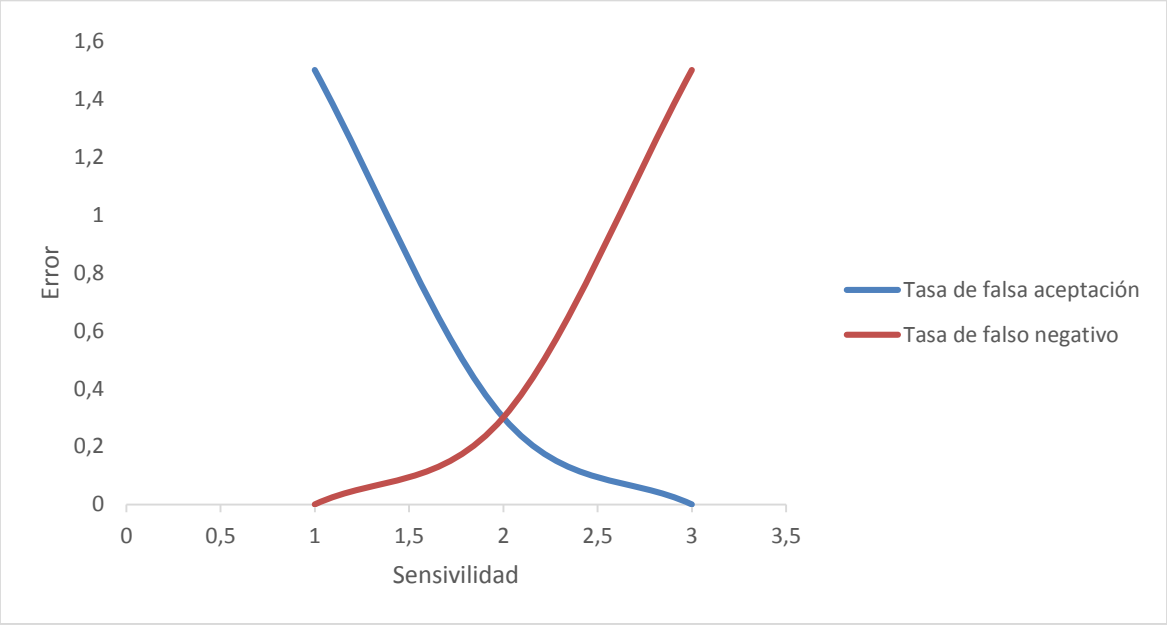


Figura 2.3. Tasa de medidas biométricas

Fuente: Investigador

En los sistemas biométricos reales el FAR y el FRR pueden transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los relojes biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (Equal Error Rate o EER), también conocida como la tasa de error de cruce (Cross-over Error Rate o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto [3].

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de relojes biométricos fijó el umbral de aceptación alto, para reducir

al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo. Si entro a un sistema de verificación de firmas usando mi inicial y apellido, ¿puedo decir legítimamente que se trata de un falso rechazo cuando rechace mi nombre y apellido?

A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un grado de certeza muy alto. La prueba forense del ADN goza de un grado particularmente alto de confianza pública actualmente (ca. 2004) y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

Para realizar la autenticación biométrica, primero se debe registrar a los individuos que van a hacer uso del sistema. Para el registro se utiliza el dispositivo biométrico para examinar el atributo físico o de comportamiento elegido. Un software o firmware se encarga de cuantificar los datos examinados y transformarlos en datos matemáticos. El conjunto de estos datos matemáticos se llama plantilla que identifica al individuo.

La autenticación posterior se realiza cuando el individuo presenta su rasgo corporal o muestra su comportamiento ante un dispositivo biométrico. Nuevamente se cuantifica los datos del rasgo en una nueva plantilla para compararlos contra la plantilla guardada. La búsqueda de la plantilla guardada puede realizarse de dos maneras. La primera es una búsqueda de uno a muchos (1:N), solamente se presenta el rasgo y el sistema se encarga de buscar entre todas las plantillas guardadas, quien es el individuo, esto es conocido como identificación. Este método requiere un mayor tiempo de búsqueda y es utilizado en bases de datos pequeñas. El segundo método es una búsqueda uno a uno (1:1), donde el individuo presenta adicionalmente su identificación. El sistema se encarga de buscar la plantilla guardada que este bajo el nombre o número de identificación solamente, y realiza la comparación. Esto es como verificación, y es utilizado en mayoría de las aplicaciones biométricas.

Los relojes biométricos pueden almacenar un número determinado de huellas dactilares que generalmente puede ser como máximo diez por persona las mismas que son utilizadas para el control de registro.

Las huellas dactilares son registradas mediante el lector conocida como prisma, donde el usuario coloca sus dedos uno a uno por un determinado tiempo las misma que el reloj biométrico le da una señal de verificación (ACCESO CORRECTO) o negación (INTENTE DE NUEVO) .

Seguridad en Sistemas Biométricos

Hoy en día la palabra seguridad es muy importante a la hora de hablar de almacenamiento de información crítica en un sistema informático, esto debido, en gran parte, a la roliferación de virus, fallos de seguridad de distintos softwares (Bugs) y programas espías (spyware).

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, que puede ser el reconocimiento del iris, la identificación del tono de voz o la utilización de la huella dactilar, algo similar a la firma digital pero en este caso el password es una característica física única e irrepetible como las mencionadas anteriormente; A demás del importante salto en seguridad que representa, debemos tener en cuenta una mejora sustancial para el usuario de la PC, no caeremos en el viejo error de olvidar la clave o simplemente perderla como pasaba o aun sucede hoy en día.

La **seguridad informática**, en el área de la informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Por lo que existen estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos entre otras

y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Vulnerabilidades de los Relojes Biométricos

Se han comentado extensamente las virtudes que poseen los sistemas biométricos frente a los sistemas tradicionales, pero no nos podemos olvidar de las vulnerabilidades que poseen los sistemas de reconocimiento automático. A continuación se citan las diferentes amenazas a las que se expone un sistema de seguridad en general:

- **Puenteo del sistema:** un usuario no autorizado logra acceso fraudulento al sistema y a los datos que éste posee
- **Repudio:** el usuario que intenta acceder legítimamente, obtiene negación de acceso al sistema.
- **Contaminación o adquisición encubierta:** los medios de reconocimiento del usuario se ven comprometidos por ser usados por el impostor sin conocimiento del usuario legítimo.

Una **vulnerabilidad** por el contrario no es en modo alguno un programa, aunque muchas de ellas se suelen crear precisamente en la creación de otros programas. Una vulnerabilidad es un fallo generalmente en un software que hace que este sea susceptible a un ataque de algún tipo.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits).

Las vulnerabilidades en las aplicaciones suelen corregirse con parches o cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

Las vulnerabilidades se descubren muy seguidas en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.

Algunas vulnerabilidades típicas suelen ser:

- **Vulnerabilidad de desbordamiento de buffer.-** Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

En esta situación se puede aprovechar para ejecutar código que nos de privilegios de administrador.

- **Vulnerabilidad de condición de carrera (race condition).-** Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.
- **Vulnerabilidad de Cross Site Scripting (XSS).-** Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero

en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- **Vulnerabilidad de denegación del servicio.-** La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.
- **Vulnerabilidad de ventanas engañosas (Window Spoofing).-** Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

Para elaborar el análisis de las vulnerabilidades de forma correcta, se deberá primero analizar las herramientas que se emplearan y se presentará de una manera global y detallada los aspectos que interesan saber sobre las vulnerabilidades de los Relojes Biométricos, procurando tener una mejor información y así llegar a optar por posibles soluciones adecuadas.

Estas amenazas son generalmente el resultado de posibles ataques al sistema sobre distintos puntos vulnerables de un sistema de reconocimiento biométrico llevados a cabo por un agente externo.

Ataques

Diversos grupos de investigación han hecho un esfuerzo por catalogar y clasificar diferentes tipos de ataques a los que puede ser sometido un sistema de reconocimiento biométrico basado en huella dactilar.

- Como es el de sensor
- A la base de datos

Los sistemas biométricos, a pesar de su aparente alto nivel de seguridad para los usuarios, presentan un elevado número de puntos en los que pueden ser atacados. Recientemente, ante la proliferación de los sistemas de reconocimiento biométrico en aplicaciones de autenticación para dispositivos electrónicos y control de acceso, su seguridad ha cobrado gran relevancia. [4]

Definición: los sistemas biométricos igual que cualquier sistema tienes sus ataques como el suplantar el dedo a través de gelatina, silicona entre otros.

Identificaciones

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos. Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como variaciones intraclase. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema [1]:

- Una persona autorizada es aceptada,
- Una persona autorizada es rechazada,
- Un impostor es rechazado,
- Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores. [1]

Definición: todo sistema biométrico tiene sus propios patrones de reconocimientos e identificación como son el “Acceso Correcto”, el “Acceso Incorrecto” o “Intente De Nuevo” y “Huella duplicada”.

Fase operacional

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con el template que está asociado al usuario. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?

Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda exhaustiva en la base de base de datos con los templates. Esto conduce a una comparación del tipo uno-a-muchos para establecer la identidad del individuo. [1]

Robo de identidad

Las preocupaciones acerca del robo de identidad por el uso de la Biometria aún no han sido resueltas. Si el número de tarjeta de crédito de una persona es robado, por ejemplo, puede causarle a esa persona grandes dificultades. Si sus patrones de escaneado de iris son robados, sin embargo, y eso permite a otra persona acceder a información personal o a cuentas financieras, el daño podría ser irreversible. Frecuentemente, las tecnologías biométricas han sido puestas en uso sin medidas adecuadas de seguridad para la información personal que es resguardada a través de las mismas.

2.3.2. Fundamentación variable dependiente

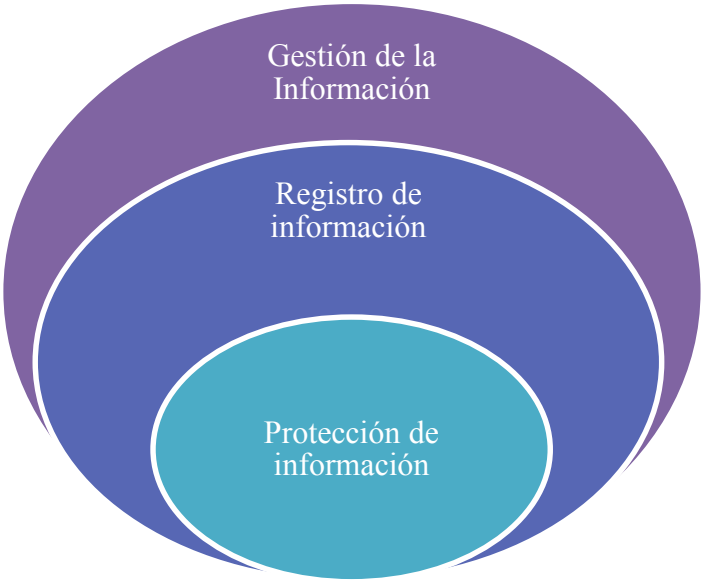


Figura 2.4. Subordinación de la variable dependiente

Fuente: Investigador

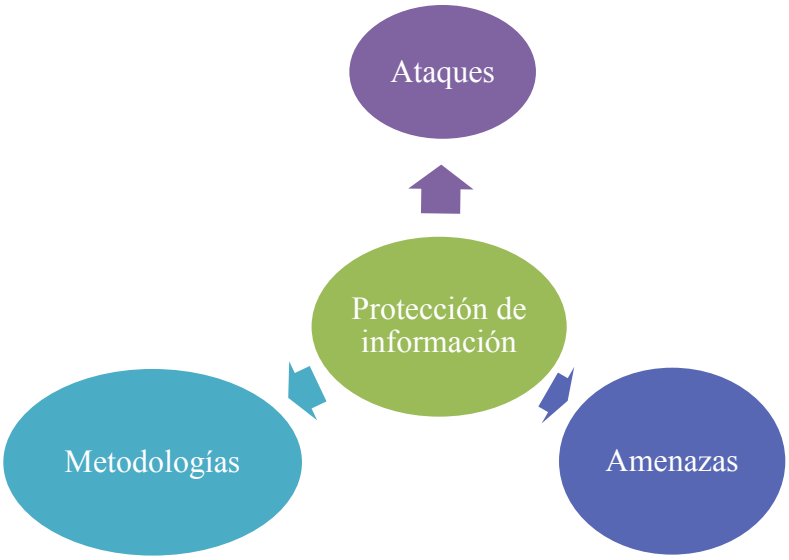


Figura 2.5. Análisis de la variable dependiente

Fuente: Investigador

Gestión de la Información

La finalidad de la Gestión de la información es ofrecer mecanismos que permitieran a la organización adquirir, producir y transmitir, al menor coste posible, datos e informaciones

con una calidad, exactitud y actualidad suficientes para servir a los objetivos de la organización.

En términos perfectamente entendibles sería conseguir la información adecuada, para la persona que lo necesita, en el momento que lo necesita, al mejor precio posible para toma la mejor de las decisiones.

En el momento actual parece indiscutible que el éxito de la empresa no dependerá únicamente de cómo maneje sus activos materiales, sino también de la gestión de los recursos de información. La importancia de este recurso es tal que algunos autores estiman que las organizaciones deben ser consideradas como sistemas de información.

Es frecuente confundir un sistema de información con la tecnología que lo soporta. Las Tecnologías de la información han supuesto una auténtica revolución en la capacidad de manejo de los recursos de información, permitiendo un rápido y eficiente proceso de adquisición, enriquecimiento y acceso a la misma, aunque nunca hay que olvidar que un Sistema de Gestión de Información va más allá de las propias herramientas utilizadas.

El Sistema de Gestión de Información es el encargado de seleccionar, procesar y distribuir la información procedente de los ámbitos interno, externo y corporativo.

- Información interna. La producida en la actividad cotidiana de la institución
- Información externa. La adquirida por la institución para disponer de información sobre los temas de su interés
- Información corporativa o pública. La que la institución emite al exterior

Las funciones de la Gestión Información abarcarían:

1. Determinar las necesidades de información en correspondencia a sus funciones y actividades
2. Mejora de los canales de comunicación y acceso a la información

3. Mejora de los procesos informativos
4. Empleo eficiente de los recursos.

En este contexto, la información es considerada un recurso, un producto y un activo

- La información como activo tiene un coste y debe tener un rendimiento.
- La información como producto deberá tener unas exigencias de calidad.
- La información como activo implica que la organización se preocupe por poseerla, gestionarla y utilizarla.

Gestión de la Información (GI), es un conjunto de procesos por los cuales se controla el ciclo de vida de la información desde su creación o captura, hasta su disposición final, archivada o eliminada.

Los procesos también comprenden la extracción, combinación, depuración y distribución de la información a los interesados. El objetivo de la Gestión de la Información es garantizar la integridad, disponibilidad y confidencialidad de la información.

La gestión de la información es clave para la toma de decisiones dentro de una organización es una realidad que ningún directivo niega, sin embargo, pese a ser un axioma reconocido, pocas son las compañías que han logrado desarrollar sistemas eficaces de gestión de su información.

Las ingentes cantidades de datos generados cada día en las empresas están dispersos en diferentes almacenes y repositorios y se gestionan por plataformas diferentes. En muchas ocasiones estos datos son de difícil acceso y están “contaminados” por otros inservibles. Al no disponer de soluciones analíticas, las bases de datos utilizadas que han conseguido almacenar información de calidad no pueden rentabilizarse al máximo.

Disponer de los datos adecuados es un imperativo a la hora de realizar análisis predictivos (predecir comportamientos futuros a partir de comportamientos pasados). El Business Intelligence es la plataforma que transforma datos, a través de técnicas analíticas para cuantificar los elementos clave de la estrategia empresarial permitiendo a quien los usa ser más competitivo y proactivo en el diseño de su futuro.

El gran reto por tanto de las organizaciones, ya sean empresariales, o de otra naturaleza, es conseguir una gestión de los datos que los transforme en información inteligente que sea la clave para la toma de decisiones.

Existen formas diferentes de afrontar el reto de una buena gestión de la información, pero para garantizar el éxito es fundamental acometer el proceso siguiendo tres pasos claramente definidos.

- En primer lugar, como ocurre con otros procesos empresariales estratégicos, está la fase de la planificación. En ocasiones las empresas se olvidan de este paso previo y se lanzan a la adquisición de soluciones y herramientas tecnológicas sin tener claro los objetivos que alcanzarán. Antes de nada es vital fijar unos objetivos claros y diseñar una estructura tecnológica que permita obtener los objetivos marcados. En esta primera fase se deben definir dos criterios fundamentales, que el sistema de información elegido sea el mismo para toda la organización y que permita la máxima facilidad de acceso según las diferentes necesidades de cada departamento o segmento de negocio. Una mala planificación puede hacer que la empresa se ahogue en sus propios datos porque no sea capaz de gestionarlos, o que disponga de demasiadas soluciones tecnológicas que no tengan ninguna utilidad.
- La segunda fase del proceso es la de almacenamiento de los datos. En esta fase son imprescindibles las soluciones de extracción, transformación y carga de datos, ETL. Estas soluciones son capaces de detectar los datos, integrarlos y limpiarlos antes de almacenarlos. Una de las características exigibles a los almacenes de datos es también que proporcionen una gran flexibilidad en la acumulación de datos e iguales prestaciones para el acceso a esos datos. Los almacenes de datos deben incluir tecnología de

seguridad, reserva y recuperación, necesarios para el manejo de grandes volúmenes de información.

- El tercer paso que completa el proceso es la implementación de soluciones de inteligencia que permitan analizar esos datos para obtener conocimiento inteligente a partir de los mismos. En esta fase existen diferentes soluciones con distintos grados de complejidad, comenzando por sencillas soluciones de reporting capaces de elaborar informes predeterminados con tan solo pulsar una tecla. Estas aplicaciones no proporcionan por ejemplo datos como cuáles han sido las diez mayores operaciones por volumen de ingresos de un periodo determinado. En un nivel más avanzado se sitúan las aplicaciones OLAP (online analytical processing) que permiten a los usuarios diseñar sus propios procesos de gestión de datos para obtener conocimientos muy precisos. Las aplicaciones OLAP permiten hacer diferenciaciones de ingresos por zonas geográficas o comparativas con periodos anteriores por ejemplo. Pero existen aún soluciones más sofisticadas de gestión de datos, la implementación de soluciones analíticas de minería de datos. [5]

Estas soluciones ofrecen respuestas a las preguntas clave para tomar decisiones a través de la aplicación de modelos matemáticos (estadística, detección de valores extremos, redes neuronales, árboles de decisión, regresiones, etc.). La potencia de las soluciones analíticas no deja de crecer y el conocimiento que se obtiene de ellas repercute directamente en la operativa de las organizaciones. La minería de datos nos da información tal como quiénes son nuestros diez mejores clientes, qué segmentos de negocio generan mayores beneficios y cuáles pérdidas, cuál es la probabilidad de que determinados clientes nos abandonen o qué propensión tiene cada uno de nuestros clientes a ampliar la gama de productos que nos compra.

Registro de información

Mediantes las características leídas de cada usuario por el prisma el sistema registra en su propia base de datos para ser leída después de su verificación.

En el modo de registro, los usuarios son dados de alta en el sistema. Para ello, se introducen sus rasgos biométricos en el sistema a través de los sensores correspondientes al rasgo empleado y se dan de alta en la base de datos quedando almacenada así la plantilla de usuario. En la base de datos se podrán almacenar además otros datos personales de los usuarios. [4]

Protección de la información

Definición: Es defenderse de alguien o algo para evitarle un daño en nuestra información a través de software o métodos de seguridad aplicables a la información.

Ataques

En este tipo de ataques estarían contemplando los casos en los que el atacante tuviera acceso privilegiado a la base de datos o al canal de comunicación entre el comparador y la base de datos. En ese caso sería necesario que conociese el formato concreto en que se almacenan los patrones en la misma y los modificase introduciendo nuevos patrones, cambiando o eliminando alguno ya existente [4].

Definición: del mismo modo como atacan a las bases de datos tiene sus ataques a la base de datos el sistema biométrico siempre y cuando alguien tenga el acceso como administrador al biométrico.

Amenazas

Las amenazas están compuestas por una persona, la máquina y un suceso o idea en los sistemas de información que dada una oportunidad se puede producir una violación de la seguridad como es la confidencialidad, integridad, disponibilidad.

Las categorías generales de amenazas o ataques son las siguientes:

- Interrupción:
- Modificación
- Fabricación
- Control de acceso
- Autenticación
- No repudio
- Disponibilidad

Metodologías

Para crear una metodología de políticas de seguridad se debe desarrollar procedimientos y planes que resguarden los recursos; para desarrollar una metodología se debe considerar:

- De quienes debemos protegernos.
- Cuáles son las amenazas
- Que recursos son los que se van a proteger
- Entre otros.

Papiloscopia

La lofoscopia o papiloscopía denominada dermatoglifia en el ámbito de la medicina y la zoología o en textos traducidos de otras lenguas (generalmente como traducción del término inglés dermatoglyphics), es la ciencia que estudia los diseños formados por las crestas papilares situados en la superficie de la piel especializada para la locomoción, la función prensil y la percepción de estímulos táctiles [6].

Estos diseños se presentan en todos los primates, desde los prosimios hasta el ser humano y esporádicamente se encuentra en otros mamíferos como la ardilla común; en algunos insectívoros, que pueden presentar patrones específicos; y en algunos marsupiales se pueden observar algunas zonas de la piel profusamente trazada aunque con poca especialización (sin diseños específicos, solo líneas algo curvas y paralelas entre sí).

Debido a que ninguna otra especie presenta esta característica, se especula que el inicio de los hábitos arborícolas fueron los que favorecieron el desarrollo de patrones dermopapilares complejos. [6]

2.3.3. Fundamentación

Huellas dactilares

Una huella dactilar es la impresión visible de las crestas papilares de un dedo de la mano siendo una característica individual la misma que se utiliza como medio de identificación de las personas.

Se clasifican por sus características en:

- **Visibles o Positivas:** Son las que dejan los dedos al estar impregnados de algún colorante, este material puede ser sangre, tinta, polvo o cualquier otra sustancia con la que puedan quedar marcadas las crestas papilares y puedan ser observadas a simple vista.
- **Moldeadas:** Son las que aparecen impresas en forma de molde, estas se marcan en materia plástica, como la grasa, jabón, plastilina, etc.
- **Naturales:** Aparecen de forma natural en los pulpejos de ambas manos, desde los seis meses de vida intrauterina hasta la muerte e incluso en el proceso de putrefacción, y
- **Artificiales:** Son aquellas que se encuentran plasmadas en forma intencional con alguna sustancia, esencialmente con tinta para su estudio. El sistema de identificación de las personas a través de las huellas fue inventado por Juan Vucetich (nacido el 20 de Julio de 1858 en la actual Croacia, registrado inicialmente con el nombre Iván Vučetić y nacionalizado argentino), y el invento se desarrolló y patentó en Argentina, donde también se usó por primera vez el sistema de identificación de huellas para esclarecer un crimen. También El 1 de septiembre de 1891 Vucetich hizo las primeras fichas dactilares del mundo con las huellas de 23 procesados, y se estableció como Día Mundial de la Dactiloscopía, Luego de verificar el método con 645 reclusos de la cárcel de La Plata, en 1894 la Policía de Buenos Aires adoptó oficialmente su sistema. [7]

Figura 2.2. Juan Vucetich

Fuente: http://principiodeidentidad.blogspot.com/2008/01/biografa-de-juan-vucetich.html

Dactiloscopia es la ciencia que propone identificar a las personas físicamente por medio de la impresión o reproducción física de los dibujos formados por las crestas papilares en las yemas de los 10 dedos, que viene de los vocablos griegos daktilos (dedos) y skopia (observación o examen) [8].

En el sistema de la dactiloscopia se basa en principios fundamentales las cuales son:

- **Perennidad:** Las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver.
- **Inmutabilidad:** Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo y en caso de que llegase a presentarse un desgaste involuntario como por ejemplo una herida o quemadura; el tejido epidérmico que la conforma es capaz de regenerase tomando su forma original en un periodo de 15 días.
- **Diversidad Infinita:** Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales.

A simple vista toda persona puede observar que la piel no es enteramente lisa o uniforme, sino que está cubierta de rugosidades, protuberancias y depresiones en la dermis, a continuación se describen estas rugosidades:

a) **Papilas**: Son las pequeñas protuberancias que nacen en la dermis y sobresalen completamente en la epidermis, sus formas son muy variadas; unas son cónicas, otras hemisféricas y otras piramidales o simulando verrugas. El número de papilas agrupadas en cada milímetro cuadrado se calcula que es de 36 y su tamaño es de 55 a 225 milésimo de milímetro de altura.

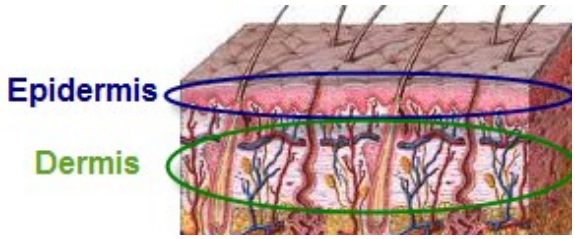


Figura 2.3. Epidermis y Dermis de una Huella
Fuente: Editada por el investigador

b) **Crestas:** Las crestas son los bordes sobresalientes de la piel que están formados por una sucesión de papilas, estos bordes siguen las sinuosidades de los surcos en todas direcciones y forman una infinidad de figuras en las yemas de los dedos, son más amplios en su base que en la cúspide, dan el aspecto de una montaña en miniatura y reciben el nombre de crestas papilares.

c) **Surcos:** Se les da el nombre de surcos a los espacios hundidos los que se encuentran entre papila y papila. También se les conoce con el nombre de surcos interpapilares debido a que al entintar los dedos, la tinta no cubre completamente las yemas, por ello al hacer la impresión de las huellas sobre cualquier superficie plana quedan espacios en blanco.

d) **Poros:** Los poros son los pequeños orificios que se encuentran situados en la cúspide de las crestas papilares o cerca de su vértice, tienen la función de segregar el sudor. Estos poros tienen diferentes formas que pueden ser circulares, ovoidales, triangulares, etc.

Los dibujos o figuras formadas por las crestas papilares reciben el nombre de dactilogramas palabra que deriva de los vocablos griegos; daktylos (dedos) y grammas (escrito). Se denominan dactilogramas papilares si provienen de los dedos de la mano, plantares si

provienen de la planta del pie y palmares cuando provienen de la palma de la mano. Los dactilogramas se pueden clasificar de tres formas:

- **Dactilograma natural:** es el que está en la yema del dedo, formado por las crestas papilares de forma natural.
- **Dactilograma artificial:** es el dibujo que aparece como resultado al entintar un dactilograma natural e imprimirlo en una zona idónea.
- **Dactilograma latente:** es la huella dejada por cualquier dactilograma natural al tocar un objeto o superficie. Este dactilograma queda marcado, pero es invisible. Para su revelación requiere la aplicación de un reactivo adecuado.

De igual forma un dactilograma se puede dividir en tres partes que se conocen como: sistemas dactilares los cuales son el Sistema basilar, el Sistema marginal y el Sistema nuclear.

A. **Región Basilar:** conformada por la impresión de crestas existentes entre la rama descendente del delta, el apéndice o cola y el límite inferior [9].
B. **Región Marginal:** conformada por el conjunto de crestas que están determinadas entre la rama ascendente, el apéndice o cola y el límite exterior. [9]
C. **Región Nuclear:** conjunto de crestas comprendidas entre la rama ascendente y descendente del delta. [9]

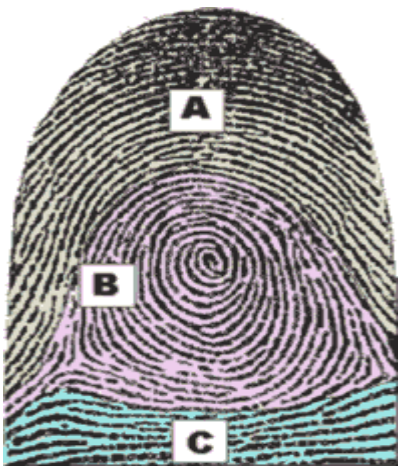


Figura 2.4. Sistemas dactilares
Fuente: Editada por el investigador

Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a constituir sistemas definidos por la uniformidad de su orientación y figura. Se pueden distinguir cuatro grupos o clases distintas de configuraciones dérmicas según la denominada Clasificación de Henry, pero antes debemos estudiar dos singularidades presentes en algunas huellas denominadas Núcleo (Core) y Delta.

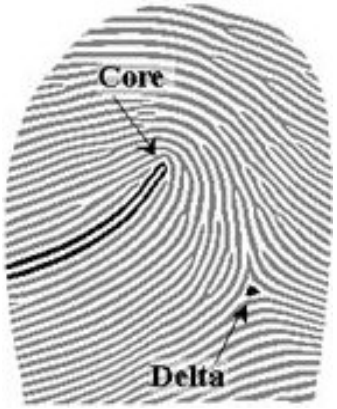


Figura 2.5. Puntos singulares de la huella dactilar

Fuente: Editada por el investigador

Tipos fundamentales de las Huellas

A continuación se detallan la clasificación de diseño de las huellas dactilares:

1. **Arco**: Se caracteriza porque las crestas son casi rectas y paulatinamente se van arqueando para dar forma aproximada de medio círculo, sin envolverse sobre sí misma.

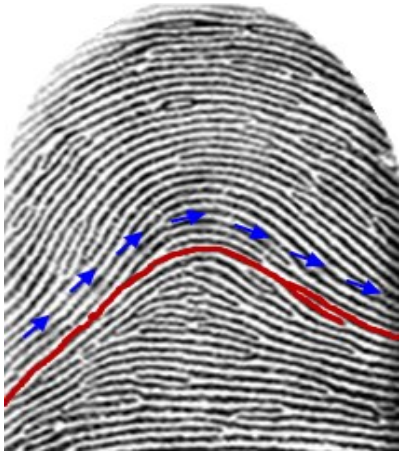


Figura 2.6. Arco

Fuente: Editada por el investigador

2. **Presillas Internas:** Se caracterizan porque las crestas que forman su núcleo nacen en el costado izquierdo y hace su recorrido a la derecha, para luego dar vuelta sobre sí mismas y regresar al mismo lado de partida; Cuenta con un punto Delta en la parte Derecha.

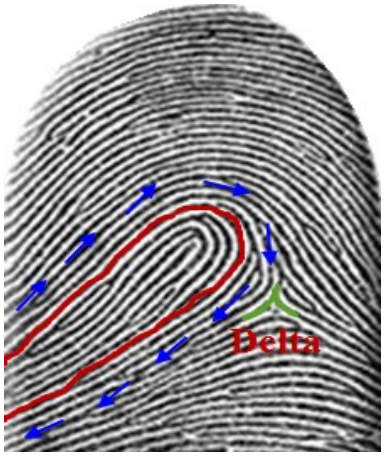


Figura 2.7. Presilla interna
Fuente: Editada por el investigador

3. **Presillas Externas:** Al igual que las presillas Internas, cuentan con un punto Delta, pero éste se ubica al lado izquierdo; y las crestas papilares que forman el núcleo nacen a la derecha y su recorrido es a la izquierda para dar vuelta sobre sí mismas y regresar al mismo punto de partida.

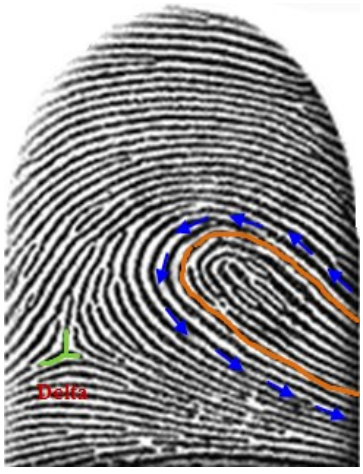


Figura 2.8. Presilla externa
Fuente: Editada por el investigador

4. **Verticilo**: Se denomina verticilo debido que su característica más importante es que cuenta con dos puntos Delta uno del lado derecho y otro del lado izquierdo, sus núcleo puede adoptar formas circulares, elípticas y espirales.

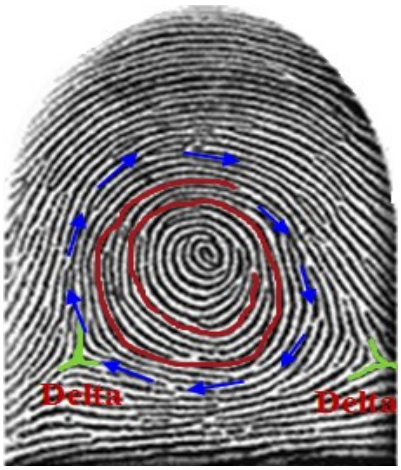


Figura 2.9. Verticilo

Fuente: Editada por el investigador

Numeración según tipo de huella

Las letras de los pulgares son:

- **Arco:** "A" y tiene el número 1
- **Presilla Interna:** "I" y tiene el número 2
- **Presilla Externa:** "E" y tiene el número 3
- **Verticilo:** "V" y tiene el número 4

Herramientas de búsqueda de vulnerabilidades para los relojes biométricos

A continuación se presenta una breve descripción de las herramientas con las cuales se pueden realizar análisis de vulnerabilidades en los sistemas biométricos.

NESSUS

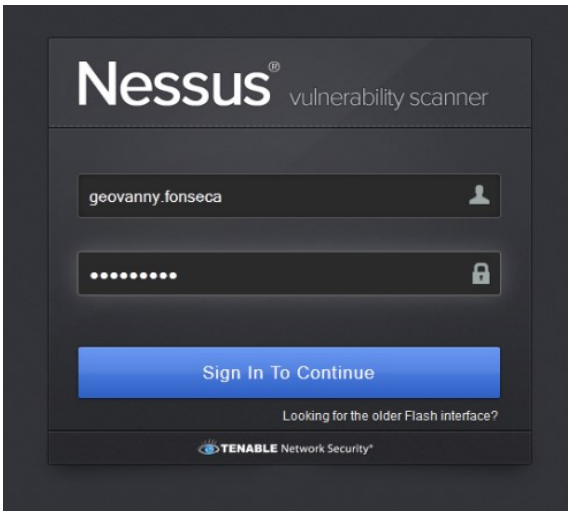


Figura 2.10. Logo Nessus

Fuente: Propia del Programa

La interfaz de usuario (UI) de Nessus es una interfaz web del analizador Nessus que está compuesta por un simple servidor http y cliente web, por lo que no requiere la instalación de ningún software además del servidor Nessus. Las características principales son las siguientes:

- Genera archivos .nessus que son usados por los productos de Tenable como estándar para directivas de análisis y datos de vulnerabilidades.

- Una sesión de directivas, una lista de destinos y los resultados de varios análisis pueden almacenarse todos juntos en un único archivo .nessus.

- La interfaz gráfica de usuario (GUI) muestra los resultados de los análisis en tiempo real, por lo que no deberá esperar que finalice el análisis para ver los resultados.

- Brinda una interfaz unificada para el analizador Nessus que es independiente de la plataforma base. Existen las mismas funcionalidades en Mac OS X, Windows y Linux.

- Los análisis seguirán ejecutándose en el servidor, aun si usted se desconecta por cualquier motivo.

CONEXIÓN CON LA GUI DE NESSUS

Para iniciar la GUI de Nessus, realice lo siguiente:

- Abra el explorador web de su preferencia.
- Introduzca https://[server IP]:8834/ en la barra de navegación.

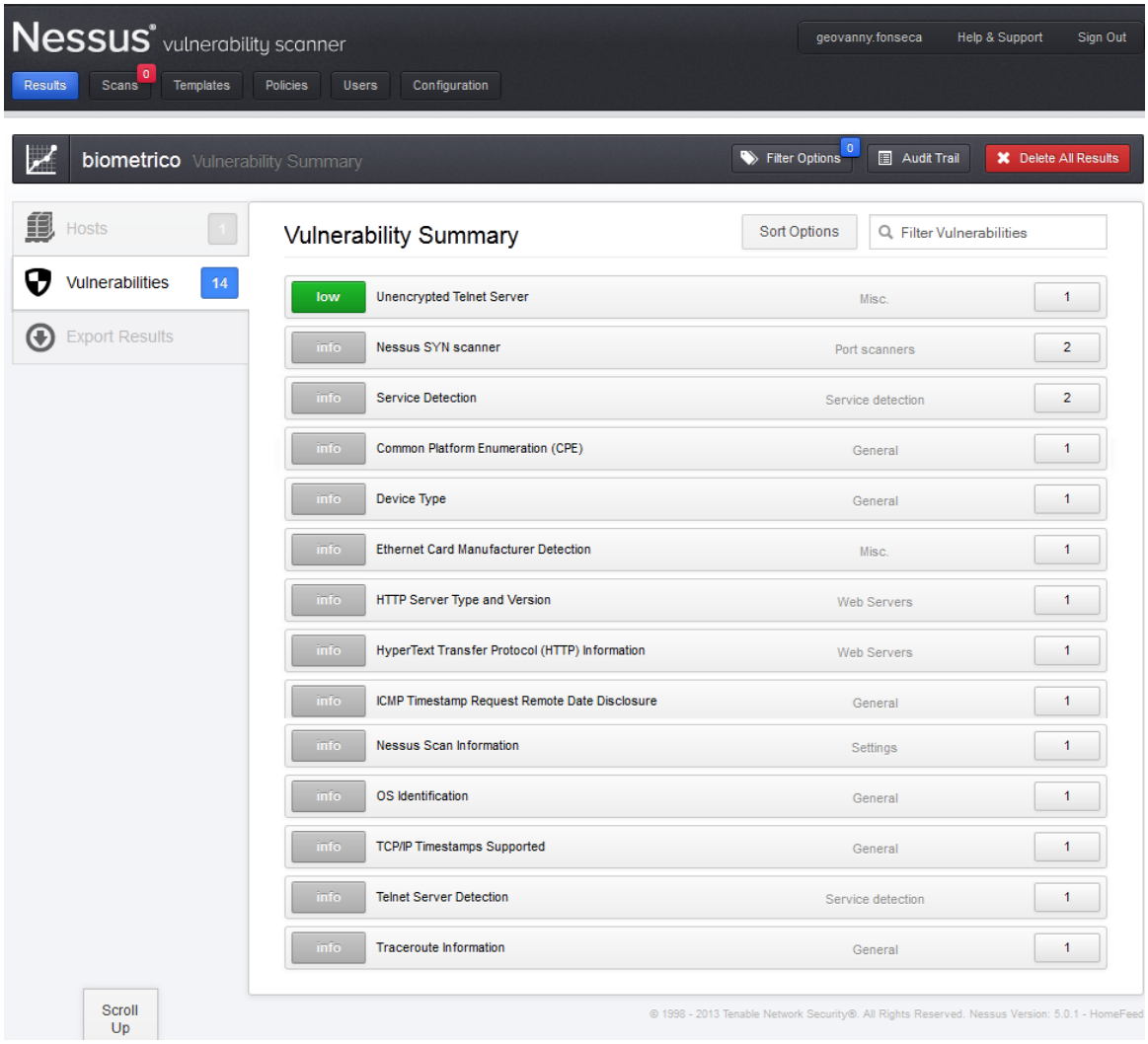


Figura 2.11. Análisis en Nessus

Fuente: Propia del Programa

Esta herramienta utilizamos para identificar las posibles vulnerabilidades existentes en los dispositivos biométricos trabajan.

ULTRA PORT SCANNER

Figura 2.12. Ultraport
Fuente: Propia del Programa

Scanner Ultra puertos le permite escanear direcciones IP´s y puertos que se encuentren abiertos en el host, además permite resolver rápidamente cualquier problema de conexión que puedan surgir con los puertos IP o asignaciones DHCP (Dynamic Host Configuration Protocol) que a menudo causan problemas para encontrar un determinado host (computadora conectada a una red). La cual dispone de una interfaz gráfica sencilla de manejar.

Esta herramienta utilizamos para identificar la dirección IP por medio del protocolo con el cual los dispositivos biométricos trabajan.

WIRESHARK

Figura 2.13. Wireshark
Fuente: Propia del Programa

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix.

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados; y todo ello por medio de una interfaz

sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark "entiende" la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico.

Esta herramienta utilizamos para identificar los protocolos, paquetes e información de los dispositivos biométricos.

BACTRAKING

Figura 2.14. Backtrack

Fuente: Propia del Programa

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix, el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu. [10]

Herramientas

Incluye varias herramientas de seguridad para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, entre otras por lo que no se requiere una instalación para poder usarse:

- Aircrack-ng, Herramientas para auditoría inalámbrica
- Kismet, Sniffer inalámbrico
- Ettercap, Interceptor/Sniffer/Registrador para LAN
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos
- Y una larga lista de otras herramientas, que se agrupan en 11 familias:
- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Análisis de redes de radio (WiFi, Bluetooth, RFID)
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso
- Forenses
- Ingeniería inversa
- Voz sobre IP

Esta herramienta utilizamos para identificar las posibles vulnerabilidades existentes en los dispositivos biométricos.

ATTENDANCE MANAGEMENT

Figura 2.15. Attendance Management

Fuente: Imagen del software de control.

ATTENDANCE MANAGEMENT es un software propio de los relojes biométricos que permite consolidar la información del Reloj Biométrico y se puede instalar en diferentes terminales para su utilización. Incorpora módulos de manejo de empleados, departamentos, horarios, turnos, asignación de turnos al personal, respaldos, manejo del dispositivo y reportes.

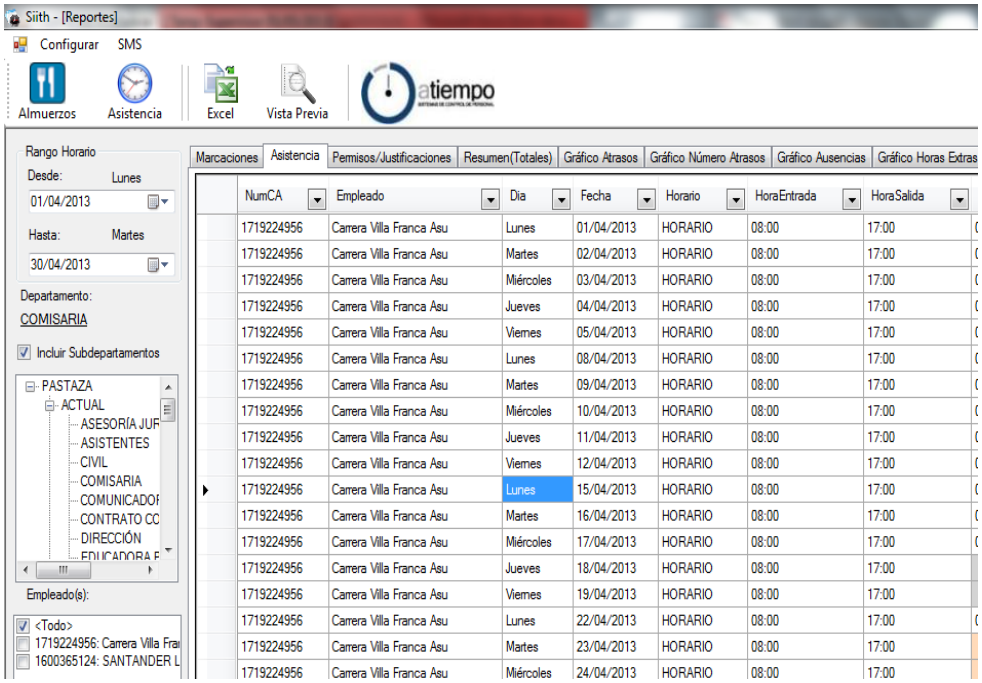


Figura 2.16. Reporte del sistema

Fuente: Imagen generada del software

Esta herramienta utilizamos para demostrar las posibles vulnerabilidades existentes en el software de control de los dispositivos biométricos.

Selección de herramientas

Para el análisis de las vulnerabilidades de los Relojes Biométricos se utilizaran las herramientas:

- BACTRAKING
- WIRESHARK
- NESSUS

Y para identificar al reloj biométrico mediante un puerto utilizamos:

- Nmap
- ULTRA PORT SCANNER

Las cuales se pusieron en práctica en el Seminario de Seguridades Informáticas en la Facultad de Ingeniería en Sistemas Computacionales, Además se utilizará el software ATTENDANCE MANAGEMENT un sistema propio de los sistemas biométricos para el control del personal.

2.4. Hipótesis

La determinación de las vulnerabilidades en los relojes biométricos en los registros del personal influye en la protección de la información de las empresas de Ambato.

2.5. Señalamiento de las variables

2.5.1. Variable independiente

Vulnerabilidades de los relojes biométricos

2.5.2. Variable dependiente

Protección de la información.

CAPÍTULO III

Marco Metodológico

3.1. Enfoque

El presente trabajo investigativo tomará un enfoque Cuali – Cuantitativo con las siguientes consideraciones:

- Naturalista debido a que no atenta contra la naturaleza, participativo ya que en él se considera a las personas que trabajan en el medio y quienes están dentro del mismo.

- Etnográfica debido a que se estudia las necesidades dentro del medio cultural dentro del medio en el que se va a desarrollar el proyecto y humanista Interna Interpretativa.

- Es normativa porque como método de solución se pretende diseñar un manual con procedimientos para una óptima configuración de los sistemas biométricos.

3.2. Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

- **Modalidad bibliográfica o documentada:** Se ha considerado esta modalidad porque se ha tomado información de Internet, libros virtuales, tesis de grados, videos, informes, proyectos, revistas, informes.

- **Modalidad experimental:** Se ha considerado la relación de la variable independiente "las vulnerabilidades del reloj biométrico" y su influencia, relación de la variable dependiente "proteger la información" para considerar sus causas y efectos.

- **Modalidad de campo:** Se ha considerado esta modalidad ya que el investigador ira a recoger la investigación primaria directamente de los involucrados a través de encuestas

3.3. Tipos de investigación

Se ha realizado la investigación Exploratoria, ya que permitió plantear el problema de la investigación como influye la vulnerabilidad del reloj biométrico y las incidencias en el registro del personal de las empresas de Ambato como de la misma manera nos ayudó a plantear la hipótesis. Es posible analizar las vulnerabilidades del reloj biométrico basándose en los registros del personal para proteger la información de los empleados de las empresas de Ambato.

Se ha considerado la investigación Descriptiva, por que permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación Correlacional, ya que ha permitido medir la compatibilidad de la variable independiente las vulnerabilidades del reloj biométrico con la dependiente registros de personal.

3.4. Población y muestra

La población que se va a considerar en la presente investigación es al personal de Recursos Humanos o de Control del Personal que se detalla en la siguiente tabla:

EMPRESAS	FUNCIONARIOS
CARROCERÍAS VARMA	5
CLINICA DURAN	3
ATIEMPOFFICE CIA. LTDA.	2
CLINICA TUNGURAHUA	2
BELINDA FLOWER	2
TOTAL	**14**

Tabla 3.1. Detalle de las Empresas de Ambato

Fuente: Investigador

3.5. Operacionalización de variables

Hipótesis: La determinación de las vulnerabilidades en los relojes biométricos en los registros del personal influye en la protección de la información de las empresas de Ambato. **Variable Dependiente:** Vulnerabilidades de los relojes biométricos				
CONCEPTO	**CATEGORÍA**	**INDICADORES**	**ÍTEMS**	**TÉCNICAS E INSTRUCCIONES**
Vulnerabilidad es la posibilidad de ocurrencia de la materialización de la amenaza sobre	Ocurrencia Sistemas biométricos	Ataques Suplantaciones Relojes	¿Ha sufrido ataques en el sistema biométrico? ¿Qué tipo de suplantaciones conoce? ¿Qué tipo de relojes cuentan en la empresa?	Encuesta con cuestionario al empleado

Hipótesis: La determinación de las vulnerabilidades en los relojes biométricos en los registros del personal influye en la protección de la información de las empresas de Ambato. **Variable independiente:** Protección de información				
CONCEPTO	**CATEGORÍA**	**INDICADORES**	**ÍTEMS**	**TÉCNICAS E INSTRUCCIONES**
Es defenderse de alguien o algo para evitarle un daño en la información en las bases de datos a través de métodos de seguridad.	Usuario Información Base de datos Seguridad	Tipo de Usuario Huellas Datos SGBD Tipo de seguridad	¿Con que tipo de usuarios cuenta las empresas? ¿Los datos que arroja el sistema biométrico le ayuda a usted en su labor diaria? ¿Qué tipo de información maneja el reloj biométrico? ¿Qué tipo de seguridad cuenta en los relojes biométricos?	Encuesta con cuestionario al personal encargado d

Tabla 3.2. Operacionalización de las variables

Fuente: Investigador

3.6. Recolección de análisis de la información

Los métodos de investigación aplicadas son las siguientes:

SECUNDARIA	PRIMARIA
Se recolecta la información en empresas que poseen relojes biométricos. Se analizará las posibles vulnerabilidades existentes en los sistema biométricos Las fuentes de información son: bibliotecas, archivos, internet.	Se recolecta directamente a través del contacto directo entre el sujeto investigador y el objeto de estudio, es decir, con la realidad.

Tabla 3.3. Métodos de investigación

Fuente: Investigador

Las técnicas de investigación aplicadas son las siguientes:

SECUNDARIA	PRIMARIA
El análisis de documentos (lectura científica)	La encuesta

Tabla 3.4. Técnicas de investigación

Fuente: Investigador

Recolección de la información

PREGUNTAS	EXPLICACIÓN
¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis
¿A qué personas o sujeto?	La población se tomara a los empleados de las empresas de Ambato.
¿Sobre qué aspectos?	**VI:** Vulnerabilidades del reloj biométrico. **VD:** Protección de la información.
¿Quién?	Geovanny Fernando Fonseca Velasco
¿Cuándo?	De acuerdo al cronograma

¿Lugar de recolección de la información?	En determinadas empresas de Ambato.
¿Cuántas veces?	Una sola vez
¿Qué técnica de recolección?	Encuestas
¿Con qué?	Cuestionario
¿En qué situación?	Situación normal y cotidiana

Tabla 3.5. Recolección de la información

Fuente: Investigador

3.7. Procesamiento y análisis de información

Revisión y codificación de la información

Categorización y tabulación de la información

Tabulación manual
Tabulación computarizada

Análisis de los datos

La presentación de los datos se hará a través de los gráficos, cuadros para analizar e interpretarlos

Interpretación de los resultados

Describir los resultados
Estudiar cada uno de los resultados por separado
Redactar una síntesis general de los resultados.

CAPÍTULO IV

Análisis e interpretación de resultados

4.1. Análisis de los resultados.

En este capítulo se expondrán los resultados de la aplicación de la metodología llevada a cabo para obtener información y de esta manera las vulnerabilidades de los relojes biométricos en los registros del personal para la protección de la información en determinadas empresas de Ambato.

Los resultados obtenidos se obtuvieron mediante encuestas al personal de recursos humanos de 5 empresas con un total de 14 encuestas realizadas sobre los relojes biométricos las mismas que se detallan a continuación con su respectivo análisis e interpretación.

Pregunta N° 1: ¿El sistema biométrico ha sufrido ataques en el funcionamiento interno?

N°	ITEMS	FRECUENCIA	%
1	Si	2	14%
2	No	12	86%
		14	

Tabla 4.6. Frecuencias de la pregunta 1

Fuente: Investigador

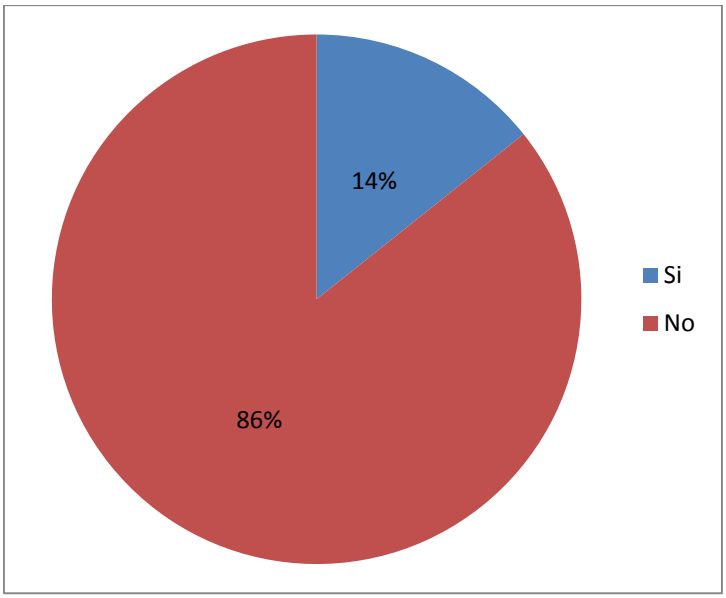


Figura 4.17. Pastel de porcentajes de la pregunta 1

Fuente: Investigador

Análisis

En la pregunta 1 correspondiente que si el sistema biométrico ha sufrido ataques en el funcionamiento interno tenemos los siguientes resultados: el 14% de las personas si han tenido ataques y el 86% no han tenido ataques biométricos.

Interpretación

Esta pregunta nos ayudará a determinar si han tenido algún tipo de ataques en el funcionamiento del sistema biométrico.

Pregunta N° 2: ¿Qué tipo de suplantaciones conoce usted?

N°	ITEMS	FRE.	%
1	HUELLAS FALSAS	9	64%
2	INFILTRACIÓN DE LA INFORMACIÓN	4	29%
3	OTROS	1	7%
		14	

Tabla 4.7. Frecuencias de la pregunta 2

Fuente: Investigador

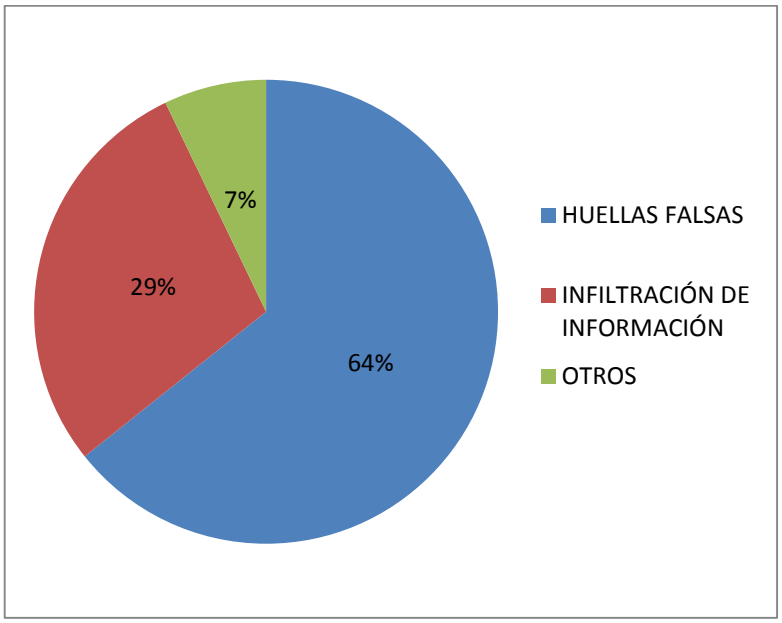


Figura 4.18. Pastel de porcentajes de la pregunta 2

Fuente: Investigador

Análisis

En la pregunta 2 correspondientes a tipos de suplantaciones que conoce tenemos los siguientes resultados: el 64% son de Huellas Falsas, el 29% son las infiltraciones de la información y el 7% son otros.

Interpretación

Esta pregunta nos ayudará a determinar si conocen algún mecanismo de como vulnerar el sistema biométrico a través de suplantación de huella o infiltración de información errónea.

Pregunta N° 3: ¿Qué tipo de relojes cuentan en la empresa?

N°	ITEMS	FRE	%
1	LECTOR DE HUELLAS DACTILARES	14	100%
2	LECTRO DE TARJETAS DE PROXIMIDAD	0	0%
3	LECTOR DE LA PALMA DE LA MANO	0	0%
4	TARJETEROS	0	0%
5	OTROS	0	0%
		14	

Tabla 4.8. Frecuencias de la pregunta 3

Fuente: Investigador

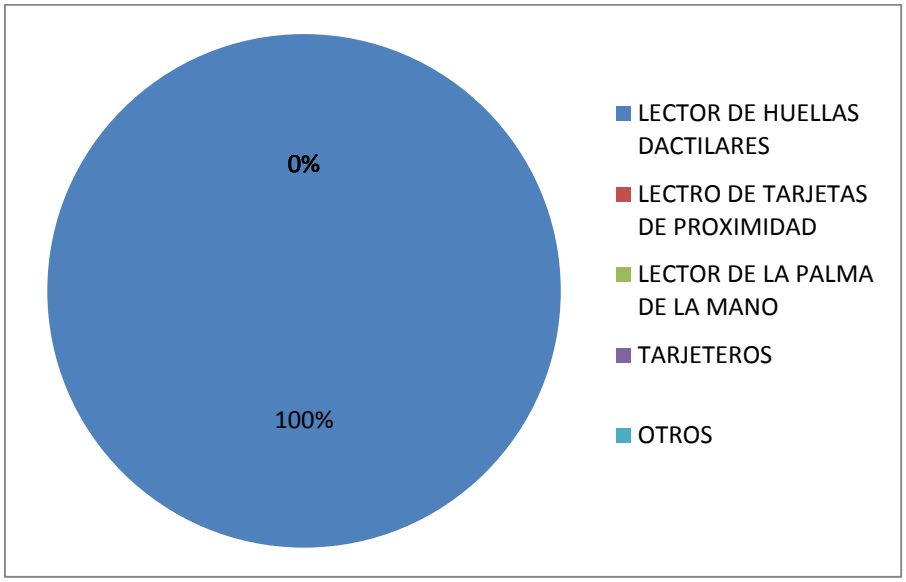


Figura 4.19. Pastel de porcentajes de la pregunta 3

Fuente: Investigador

Análisis

En la pregunta 3 correspondiente a los tipos de relojes cuentan en la empresa tenemos los siguientes resultados: el 93% de las empresas tienen relojes de lector de huellas dactilares y el 1% tiene el Hand Punch.

Interpretación

Esta pregunta nos ayudará a determinar qué tipo de reloj es el más usado para el control de asistencia y poder realizar algún tipo de estudio.

Pregunta N° 4: ¿Con respecto a la tecnología que tipo de usuarios cuentan su empresa?

N°	ITEMS	FRE.	%
1	EXPERTO	6	43%
2	PRINCIPIANTE	7	50%
3	INEXPERTO	1	7%
		14	

Tabla 4.9. Frecuencias de la pregunta 4

Fuente: Investigador

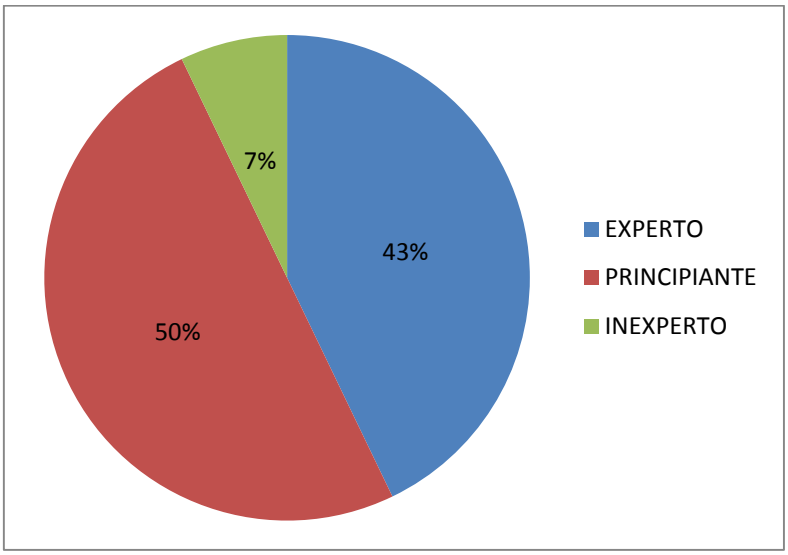


Figura 4.20. Pastel de porcentajes de la pregunta 4

Fuente: Investigador

Análisis

En la pregunta 4 con respecto a la tecnología que tipo de usuarios cuentan en las empresas tenemos los siguientes resultados: el 43% de las personas son expertos, el 50% son principiantes y el 7% son inexpertos.

Interpretación

Esta pregunta nos ayudará a determinar el tipo de usuario con el que cuenta en cada una de las instituciones.

Pregunta N° 5: ¿Los datos que arroja el sistema biométrico le ayuda a usted en su labor diaria?

N°	ITEMS	FRE.	%
1	SI	14	100%
2	NO	0	0%
		14	

Tabla 4.10. Frecuencias de la pregunta 5

Fuente: Investigador

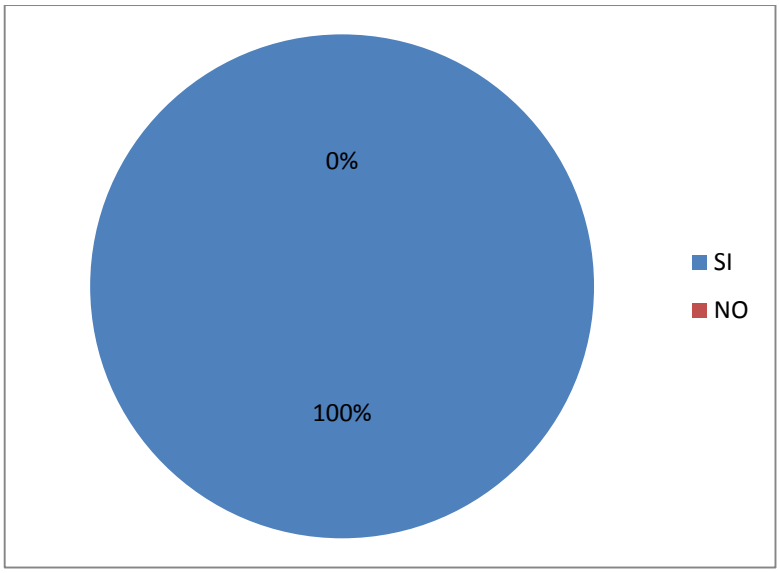


Figura 4.21. Pastel de porcentajes de la pregunta 5

Fuente: Investigador

Interpretación

En la pregunta 5 correspondiente a los datos que arroja el sistema biométrico le ayuda a usted en su labor diaria tenemos el siguiente resultado: el 100% de las personas están conformes con la información.

Análisis

Esta pregunta nos ayudará a conocer el grado de satisfacción que tiene los sistemas biométricos para el control del personal.

Pregunta N° 6: ¿Cómo se descarga la información del sistema biométrico?

N°	ITEMS	FRE.	%
1	FLASH MEMORY	1	7%
2	CABLE DE RED	12	86%
3	DIRECTAMENTE DEL RELOJ	1	7%
		14	

Tabla 4.11. Frecuencias de la pregunta 6

Fuente: Investigador

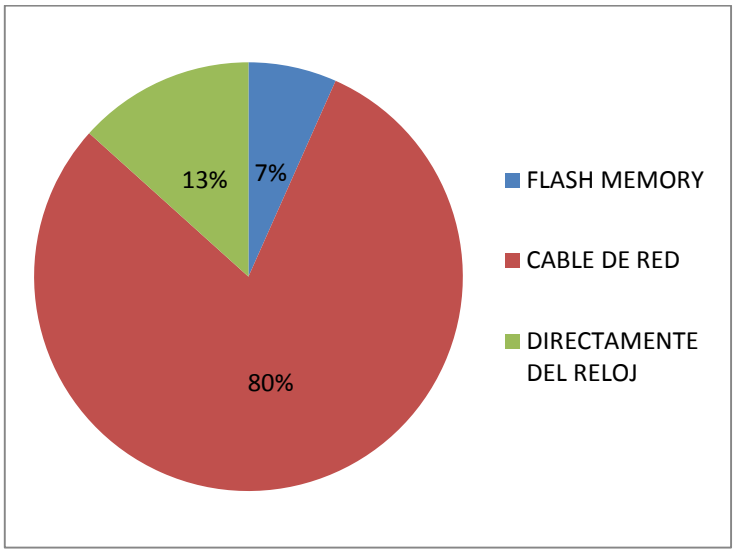


Figura 4.22. Pastel de porcentajes de la pregunta 6

Fuente: Investigador

Análisis

En la pregunta 6 correspondiente de cómo se descarga la información del sistema biométrico tenemos los siguientes resultados: el 80% se descargan a través del cable de la red, el 13 se descarga directamente del reloj biométrico y 7% mediante Flash Memory.

Interpretación

Esta pregunta nos ayudará a determinar el medio por el cual se descarga la información al software de control para realizar los reportes generales.

Pregunta N° 7: ¿Qué tipo de seguridad cuenta en los relojes biométricos?

N°	ITEMS	FRE.	%
1	CAMARAS	2	14%
2	GUARDIA DE SEGURIDAD	5	36%
3	NINGUNA	7	50%
4	OTROS	0	0%
		14	

Tabla 4.12. Frecuencias de la pregunta 7

Fuente: Investigador

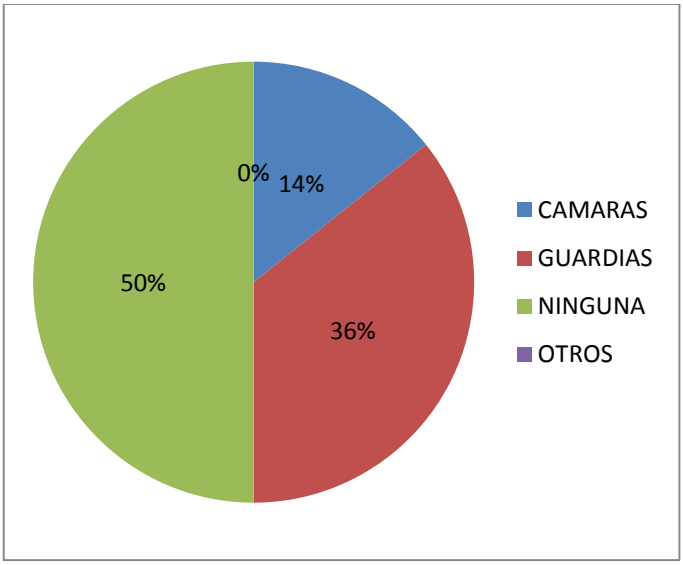


Figura 4.23. Pastel de porcentajes de la pregunta 7

Fuente: Investigador

Análisis

En la pregunta 7 correspondiente a qué tipo de seguridad cuenta en los relojes biométricos tenemos los siguientes resultados: el 14% utilizan cámaras de seguridad, el 36% tienen guardas y el 50% no cuentan con alguna seguridad.

Interpretación

Esta pregunta nos ayudará a conocer que tipo de seguridad cuentas para el control de los relojes biométricos

4.2. Interpretación

Se ha tomado en cuenta la pregunta **2** ¿Qué tipo de suplantaciones conoce usted? como pregunta discriminante de las encuestas aplicadas, ya que los resultados arrojados, dicen que un alto porcentaje conoce las suplantaciones de las huellas dactilares por lo cual podían ser fácilmente víctimas del fraude o alteración de la información.

La pregunta 3 ¿Qué tipo de relojes cuentan en la empresa? como pregunta discriminante de las encuestas aplicadas, ya que los resultados arrojados, dicen que un alto porcentaje poseen relojes biométricos de lector de huellas dactilares por lo cual podrían ser víctima de una vulneración de la información o falsificación de registros mediante huellas falsas.

Y por último se ha tomado en cuenta la pregunta 7 ¿Qué tipo de seguridad cuenta en los relojes biométricos? como pregunta discriminante de la encuesta aplicada, ya que los resultados arrojados, dicen que un alto porcentaje no cuentan con algún tipo de seguridad violentando la información.

CAPÍTULO V

Conclusiones y recomendaciones

Conclusiones

- De las encuestas realizadas en determinadas empresas tienen conocimiento de suplantaciones de las huellas dactilares por lo que están propensos a que algún empleado pueda realizar marcaciones con las mismas.

- Las empresas disponen de personal que administra el reloj biométrico y en la mayoría no dispone de controles de seguridad; la misma que nos ayudará a proteger la información y el dispositivo biométrico.

- Los resultados de las encuestas determinan que los empleados o usuarios muestran desconfianza en los sistemas biométricos por la falta de seguridad a los dispositivos.

- Se puede concluir que las personas que utilizan los sistemas biométricos como los jefes de talento humano y administradores tienen gran interés de utilizar los dispositivos biométricos porque les facilitan en sus labores diarias como controlar a sus empleados.

Recomendaciones

- Los Sistemas Biométricos se encuentran en auge por lo que se recomienda dar charlas motivadas de los sistemas biométricos para un mejor conocimiento.

- Se recomienda mejorar el conocimiento de los sistemas biométricos en cuestión de las seguridades de los sistemas biométricos.

- Proteger los registros o marcaciones en los relojes biométricos mediante políticas de seguridad de los dispositivos.

- Se recomienda realizar un análisis de las vulnerabilidades de sistemas biométricos para proteger la información de las personas que registran en las determinadas empresas de la ciudad de Ambato.

- Elaborar procedimientos de utilización e instalación de los relojes biométricos los mismos que nos ayudaran a mejorar la utilización y rendimiento de los dispositivos.

- Generar una propuesta de diseño de un manual de buenas prácticas de los sistemas biométricos para definir y organizar las funciones que debe cumplir tanto el dispositivo como el usuario final.

CAPÍTULO VI

Propuesta

6.1. Datos Informativos

La investigación realizada permitió detectar la necesidad de analizar las vulnerabilidades posibles de los relojes biométricos en determinadas empresas de Ambato, para establecer una propuesta de manuales.

- **Título:** Diseño de un manual de buenas prácticas de los sistemas biométricos
- **Institución ejecutoria:** Empresa ATIEMPOFFICE CIA. LTDA
- **Director de tesis:** Ing. Rene Terán
- **Beneficiario:** ATIEMPOFFICE CIA. LTDA
- **Ubicación:** Empresa Atiempoffice Cia. Ltda,
- **Tiempo estimado para la ejecución**
  - **Fecha de inicio:** enero 2012.
  - **Fecha de finalización:** diciembre 2012.
- **Equipo técnico responsable:**
  - **Investigador:** Geovanny Fonseca
  - **Tutor:** Ing. Rene Terán
  - **Costos:** El costo de la investigación incide por los $

6.2. Antecedentes de la propuesta

El presente estudio se realizó con base a la situación actual de las empresas anteriormente indicadas, las mismas que disponen de sistemas biométricos y administradores del sistema

encargados de control del personal, siendo los registros o marcaciones en el reloj biométrico la información más importante para controlar a los empleados, se tomó en cuenta en el análisis de las vulnerabilidades de los relojes biométricos con el propósito de salvaguardar y contar con esta información en el mayor tiempo posible.

Por tal motivo creemos que es beneficiosa para los jefes de talento humano y administradores plantear la propuesta que permita el diseño de un manual de configuración para los relojes biométricos y utilización adecuada del software que lo administra.

6.3. Justificación

El proyecto desde el punto de vista técnico es realizable, ya que está a la disposición en el mercado los relojes biométricos de la marca **BIOSYSTEM**, como también del software de control de personal ATTENDACE MANAGEMENT que permitirá el análisis de las posibles vulnerabilidades de los Relojes Biométricos como también en el manejo de los registros del personal.

Durante muchos años, la unicidad de las huellas dactilares ha sido de mucha ayuda y las autoridades de seguridad como de control pueden dar cuenta de ello. Gracias a las huellas digitales muchos criminales han podido ser identificados, para su posterior juicio y condena si se lo requiere. Por otra parte, las huellas digitales también son útiles para diferentes organismos como el Registro Civil, Bancos, entre otros, donde se deba tener en cuenta la seguridad y autentificación de la identidad de una persona, para evitar una suplantación, por ejemplo.

Con el pasar de los años, los robos de identidad y las suplantaciones se han hecho muy comunes, es así que muchas entidades han sido víctimas de hacker y cracker que toman la identidad de otra persona para beneficiarse de alguna manera y principalmente en lo económico. Para reducir las posibles falsificaciones de identidad, la tecnología biométrica ha venido aportando mejores soluciones y hoy es posible contar con mecanismos

electrónicos, que permiten validar la identidad de una persona en fracciones de segundo sin descartar que toda tecnología está expuesta a vulnerabilidades.

En el pasado, un análisis de huellas digitales podía tomar mucho tiempo, pero hoy la tecnología ofrece lectores de huellas que hacen un análisis de dactiloscopia en segundos. Así, este tipo de lectores permite saber si una persona es quien dice ser, lo cual es algo ideal en muchos contextos. Por ejemplo, si una persona va a un banco y piensa retirar una gran cantidad de dinero, a ésta no solo se le exigiría su tarjeta y su documento de identidad, sino también un rápido escaneo de su huella digital. Con esta estrategia cualquier robo de identidad o suplantación sería detectado de inmediato y el banco y el titular de una cuenta no serían estafados.

Un análisis de huellas, de este tipo, también es de mucha ayuda en instituciones de salud. En Estados Unidos, los fraudes al seguro médico dejaban pérdidas millonarias cada año, pero esto parece haber llegado a su fin, gracias al uso de lectores electrónicos de huellas digitales. Con estos lectores, una persona que desee acceder a un servicio de salud debe mostrar su carnet y poner su dedo en una pequeña ventana, la cual analiza la huella y determina si dicha persona puede acceder a dicho servicio.

En la actualidad, las huellas digitales van más allá de la resolución de homicidios y permiten evitar otras prácticas delictivas que no dejan de ser problemáticas, como la suplantación y el robo de identidad. Todo esto es posible como consecuencia de los recientes desarrollos, en el campo de la biometría de huellas digitales.

Las soluciones de identificación biométricas, son una de las mejores opciones para la automatización y control de acceso del personal de las empresas los mismos que disponen de un alto rendimiento y de fácil uso.

Al analizar las vulnerabilidades de los relojes biométricos en determinadas empresas de Ambato, es importante hallar mecanismos de seguridad para los sistemas biométricos para garantizar la información.

Para la realización del presente estudio de análisis de las vulnerabilidades se tomará en cuenta el reloj biométrico marca **BIOSYSTEM**.

6.4. Objetivos de la propuesta

6.4.1. Objetivos generales

Diseñar un manual de buenas prácticas de los sistemas biométricos para definir y organizar las funciones que debe cumplir tanto el dispositivo como el usuario final.

6.4.2. Objetivos específicos

- Determinar las vulnerabilidades de los relojes biométricos con las posibles herramientas seleccionadas.

- Determinar la estructura del manual de buenas prácticas de los sistemas biométricos.

- Desarrollar un manual de buenas prácticas de los sistemas biométricos.

6.5. Análisis de factibilidad

- **Político.-** Para la empresa ATIEMPOFFICE CIA. LTDA. Se toma como estrategia imprescindible la creación de una guía de seguridades para prevenir la alteración de la información. La empresa tiene como política brindar el asesoramiento a todos sus clientes para la utilización segura de los sistemas biométricos.

- **Socio cultural.-** La puesta en marcha del proyecto ayudará a mejorar la seguridad de los registros de acceso del personal de cada una de la empresas que poseen los sistemas biométricos, de esta manera de evitará la sociedad se verá afectada positivamente en razón de que se evitará el malestar en el personal de la empresa y el fraude informáticos de las empresas.

- **Tecnológico.-** El proyecto tiene como fin ayudar a mejorar los conocimientos de protección de los registros de los sistemas biométricos mediante el uso de las mejores prácticas y tecnologías de control de acceso.

- **Equilibrio de genero.-** El proyecto está desarrollado para que lo puedan aplicar tanto hombres como mujeres sin distinción de género.

- **Ambiental.-** El proyecto a desarrollar no atenta al medio ambiente puesto que es una guía de seguridades para el manejo de los sistemas biométricos.

- **Económico – financiero.-** ATIEMPOFFICE CIA. LTDA. Cuenta con los recursos económicos para financiar el proyecto como también para la realización de capacitaciones a los socios acerca de fraudes informáticos.

- **Legal.-** El proyecto se sujeta a las leyes y reglamentos que rige en el estado ecuatoriano y dentro de las normas establecidas en la Universidad Técnica de Ambato.

6.6. Fundamentación teórica

Manuales

Los manuales constituyen una de las herramientas con que cuentan las organizaciones para facilitar el desarrollo de sus funciones administrativas y operativas.

Son fundamentalmente, un instrumento de comunicación. Si bien existen diferentes tipos de manuales, que satisfacen distintos tipos de necesidades, puede clasificarse a los manuales como un cuerpo sistemático que contiene la descripción de las actividades que deben ser desarrolladas por los miembros de una organización y los procedimientos a través de los cuales esas actividades son cumplidas.

A continuación se dan algunas definiciones sobre lo que es un manual,

Según Duhalt Kraus Miguel A., [11]Un manual es:
"Un documento que contiene, en una forma ordenada y sistemática, información y/o instrucciones sobre historia, organización, política y procedimientos de una empresa, que se considera necesarios para la mejor ejecución del trabajo".

Para Terry G.R. [11], un manual es:
"Un registro inscrito de información e instrumentos que conciernen al empleado y pueden ser utilizados para orientar los esfuerzos de un empleado en una empresa".

Ventajas del uso de Manuales

1. La gestión administrativa y la toma de decisiones no quedan adheridas a improvisaciones o criterios personales del funcionario actuante en cada momento; Sino que son guiadas por normas.

2. Mantienen la homogeneidad en cuanto a la ejecución de la gestión administrativa y evitan la formulación de la excusa del desconocimiento de las normas vigentes.

3. Sirven para ayudar a que la organización se aproxime al cumplimiento de las condiciones que configuran un sistema.

4. Facilitan el control por parte de los supervisores de las tareas delegadas al existir un instrumento que define con precisión cuáles son los actos delegados.

5. Son elementos informativos para entrenar o capacitar al personal que se inicia en funciones a las que hasta ese momento no había accedido

6. Ubican la participación de cada Componente de la organización en el lugar que le corresponde, a los efectos del cumplimiento de los objetivos empresariales.

7. Constituyen un elemento que posibilita la evaluación objetiva de la actuación de cada empleado a través del cotejo entre su asignación de responsabilidades según el manual, y la forma en que las mismas se desarrollan.

Clasificación de manuales

Se presentan seis tipos de manuales de aplicación en las organizaciones empresarias:

- Manual de Organización.
- Manual de Políticas.
- Manual de procedimientos y normas.
- Manual del especialista.
- Manual del empleado.
- Manual de Propósito múltiple.

El manual de **organización** describe la organización formal, mencionado, para cada puesto de trabajo, los objetivos del mismo, funciones, autoridad y responsabilidad.
El manual de políticas contiene los principios básicos que regirán el accionar de los ejecutivos en la toma de decisiones

El manual de **procedimientos y normas** describe en detalle las operaciones que integran los procedimientos administrativos en el orden secuencial de su ejecución y las normas a cumplir por los miembros de la organización compatibles con dichos procedimientos.

El manual para **especialistas** contiene normas o indicaciones referidas exclusivamente a determinado tipo de actividades u oficios. Se busca con este manual orientar y uniformar la actuación de los empleados que cumplen iguales funciones.

El manual del **empleado** contiene aquella información que resulta de interés para los empleados que se incorporan a una empresa sobre temas que hacen a su relación con la misma, y que se les entrega en el momento de la incorporación. Dichos temas se refieren a objetivos de la empresa, actividades que desarrolla, planes de incentivación y programación de carrera de empleados, derechos y obligaciones, etc.

El manual de **propósitos** múltiples reemplaza total o parcialmente a los mencionados anteriormente, en aquellos casos en los que la dimensión de la empresa o el volumen de actividades no justifique su confección y mantenimiento.

Partes Componentes de un Manual

Los elementos que más interesan dentro de los integrantes de un manual son aquellos que serán objeto de consulta y que se encontrarán ubicados en lo que se denomina "cuerpo Principal": funciones, normas, instrucciones, procedimientos, lineamientos, etc. Dependiendo estos temas del tipo de manual de que se trate.

En primer lugar comenzará el texto con una sección denominada "contenido", donde se enunciarán las partes o secciones integrantes del manual.

Esta sección será seguida de un "índice" en el que, al igual que todo texto, se indicará el número de página en que se localiza cada título y subtítulo. Es un índice numérico, cuyo ordenamiento respeta la secuencia con que se presentan los temas en el manual. Pero también puede existir un índice temático, en el que los temas se presentan ordenados alfabéticamente

para facilitar su localización por este medio. Por lo general, el índice temático se ubica como última sección del manual.

La tercera sección será la "introducción" en la que se explicará el propósito del manual y se incluirán aquellos comentarios que sirvan para proponer al lector y clarificar contenidos en los capítulos siguientes.

La cuarta sección contendrá la "instrucciones para el uso del manual". Esto es, explicará de qué manera se logra ubicar un tema en el cuerpo principal a efectos de una consulta, o bien en qué forma se actualizarán las piezas del manual, dada la necesidad de revisiones y reemplazos de normas y medidas que pierden vigencia o surgen nuevas necesidades a cubrir.

La quinta sección es el "cuerpo principal"; es la parte más importante y la verdadera razón del manual.

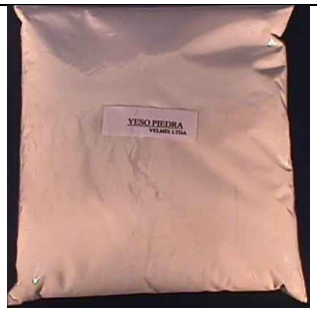
6.7. Análisis de vulnerabilidades en los relojes biométricos

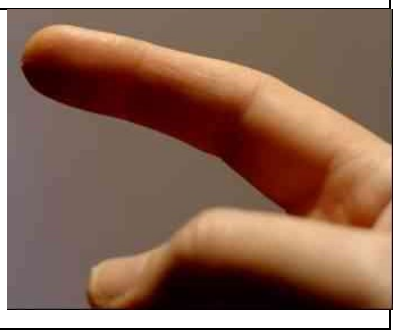
6.7.1. Suplantación de la huella dactilar.

Pasos para realizar la suplantación de una huella dactilar

Para las diferentes pruebas de suplantación de huellas se utilizara los siguientes materiales

Para realizar el molde:

MATERIAL	CANTIDAD	IMAGEN
Yeso de piedra odontológica	100gr	

Un recipiente de plástico	1	
Agua	50cc	
Vaso dosificador	1 de 20ml	
Huella dactilar a duplicar	1	

Espátula odontológica	1	

Tabla 6.13. Lista de materiales

Fuente: Investigador

Realización del molde

- Verter agua en el recipiente de plástico y después poco a poco evitando la aglomeración para que no se incorpore burbujas se va espolvoreando el yeso sobre el agua hasta que esté al mismo nivel del agua.

- Se espátula más o menos 1 minuto hasta que se quede homogénea y suave quedando así la masa de yeso.

- Se vibra la mezcla hasta que no broten más burbujas de aire a la superficie

- Verter rápidamente la mezcla en el molde.

- Introducir el dedo en el recipiente y dejar secar.

Figura 6.24. Creación del molde de una huella

Fuente: Investigador

- En 20 minutos retirar el dedo despacio.

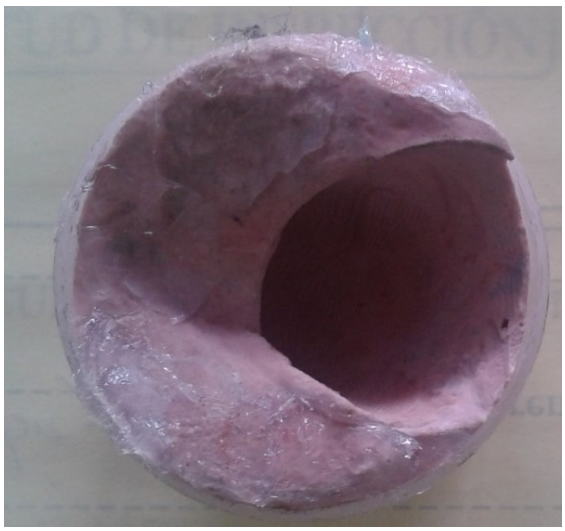


Figura 6.25. Molde de yeso

Fuente: Investigador

Relleno con silicona

Para el siguiente experimento se utilizara silicona para realizar una huella falsa blanda

Materiales

MATERIAL	CANTIDAD	IMAGEN

Silicona	1	
Molde	1	
Paleta	1	

Tabla 6.14. Lista de materiales

Fuente: Investigador

Pasos para realizar el llenado de la silicona

- Rellenar el molde con la pasta de silicona.

Figura 6.26. Relleno de silicona

Fuente: Investigador

- Colocar la paleta en el silicón para que se quede como un mango para sujetar
- Dejar secar hasta que esté rígido.

Figura 6.27. Huella duplicada

Fuente: Investigador

- Retirar la silicona de molde.

Figura 6.28: Huella duplicada

Fuente: Investigador

CREACIÓN DEL MOLDE CON PRODUCTOS ODONTOLÓGICOS

Lista de materiales que se utiliza para realizar el molde

MATERIAL	CANTIDAD	IMAGEN
Pasta liviana	1	

Pasta de condensación o pasta base	1	
Catalizador	1	
Medidor	1	
Un vidrio y una espátula	1	

Tabla 6.15. Lista de materiales

Fuente: Investigador

- Mezclar la Pasta de condensación o pasta base con la pasta catalizador hasta formar una masa de aspecto blando luego colocar la huella hasta que se seque.

Figura 6.29. Primera base

Fuente: Investigador

- Colocar la pasta liviana con el catalizador y mezclar sobre el vidrio para que no se seque rápidamente.

Figura 6.30. Pasta liviana

Fuente: Investigador

- Colocar la maza en el molde realizado anteriormente en toda en la zona.

Figura 6.31. Segundo molde

Fuente: Investigador

- Colocar nuevamente la huella dactilar y dejar que se seque en el molde anterior un lapso de 15 a 20 minutos hasta que se seque; luego retirar el dedo cuando este seco.

Figura 6.32. Molde con pasta odontológica

Fuente: Investigador

Relleno con yeso de piedra.

Para el siguiente experimento se utilizara yeso de piedra dura para realizar una huella falsa rígida.

Materiales

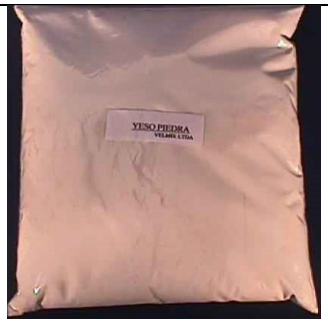
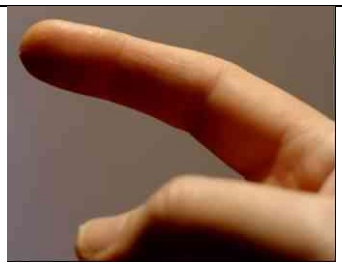
MATERIAL	CANTIDAD	IMAGEN
Yeso de piedra odontológica	100gr	
Un recipiente de plástico	1	
Agua	50cc	
Vaso dosificador	1 de 20ml	
Huella dactilar a duplicar	1	

Tabla 6.16. Lista de materiales

Fuente: Investigador

Pasos a realizar

- Verter agua en el recipiente de plástico y después poco a poco evitando la aglomeración para que no se incorpore burbujas se va espolvoreando el yeso sobre el agua hasta que esté al mismo nivel del agua.

- Se espátula más o menos 1 minuto hasta que se quede homogénea y suave quedando así la masa de yeso.

- Se vibra la mezcla hasta que no broten más burbujas de aire a la superficie

- Verter rápidamente la mezcla al molde.

- Introducir la paleta en la mezcla para que se quede como mango.

- Dejar 20 minutos o hasta que esté bien seco.

Verificación del funcionamiento de las huellas falsas.

Luego de los diferentes análisis se pudo observar que las huellas en material rígido no son reconocidas por los lectores de los relojes biométricos mientras que las huellas de material blando los reconocen con facilidad.

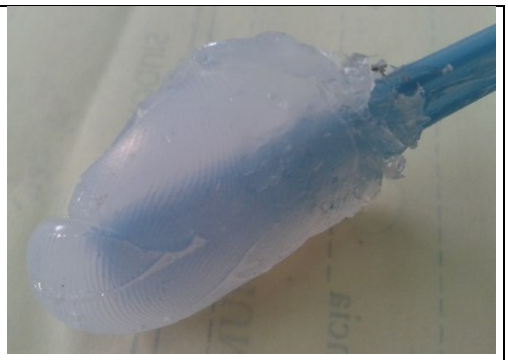
	
Huella rigida	**Huella blanda**

Tabla 6.17. Tipo de suplantaciones

Fuente: Investigador

Medidas preventivas para la controlar la autentificación con huellas falsas.

Como se pudo demostrar una de las vulnerables más evidentes es la falsificación de las huellas dactilares de los empleados o usuarios que utilizan el reloj biométrico es la falsificación de las huellas dactilares por lo que una alternativa para minimizar estos actos es incluir una cámara de seguridad que vigile los registros en el reloj para disponer de un mayor control en su utilización.

La ventaja de disponer de una cámara de video es guardar los sucesos como también controlar en un determinado momento el tiempo en el que se demora para el reconocimiento de una huella falsa, que toma aproximadamente 10 segundos y normalmente el reconocimiento toma entre 3 a 5 segundos.

Una desventaja al disponer una cámara de video es el incremento del costo considerando que no todas las personas se prestan para hacer una falsificación o ser un infiltrado con respecto a las marcaciones.

6.7.2. Borrado de información del reloj biométrico.

En el reloj biométrico se guardan todos los registros en una memoria interna en donde se pueden guardar 5000 registros considerando además el número de empleados y el horario de trabajo.

Esta información puede ser manipulada por medio de las propiedades del dispositivo en el software ATTENDANCE MANAGEMENT siendo muy fácil para borrar o administrar la información del reloj, la cual puede ser vista como una debilidad.

Requerimiento para borrar los registros del reloj biométrico:

- 1 Reloj biométrico para realizar el ataque

- Tener instalado el programa de Software ATTENDANCE MANAGEMENT en una computadora

- Saber la dirección IP del reloj biométrico y tener conectividad en la red.

Desde la barra de tareas de Windows seleccione el comando Inicio, luego desde el Todos los Programas seleccione el ítem Control del Personal y ATTENDANCE MANAGEMENT una vez hechas las selecciones se abrirá la aplicación del control del personal.

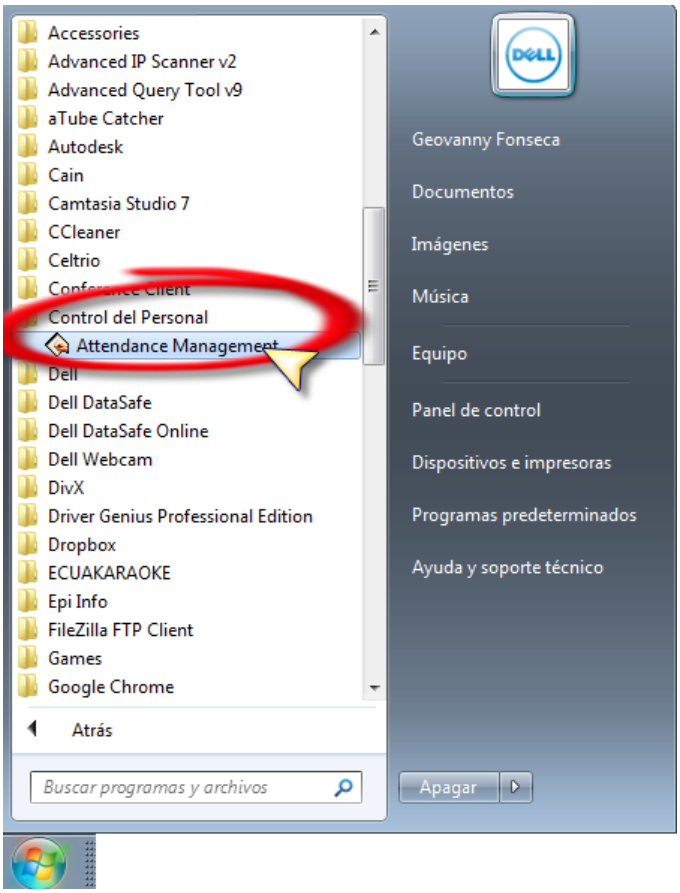


Figura 6.33. Pantalla de ingreso al programa

Fuente: Investigador

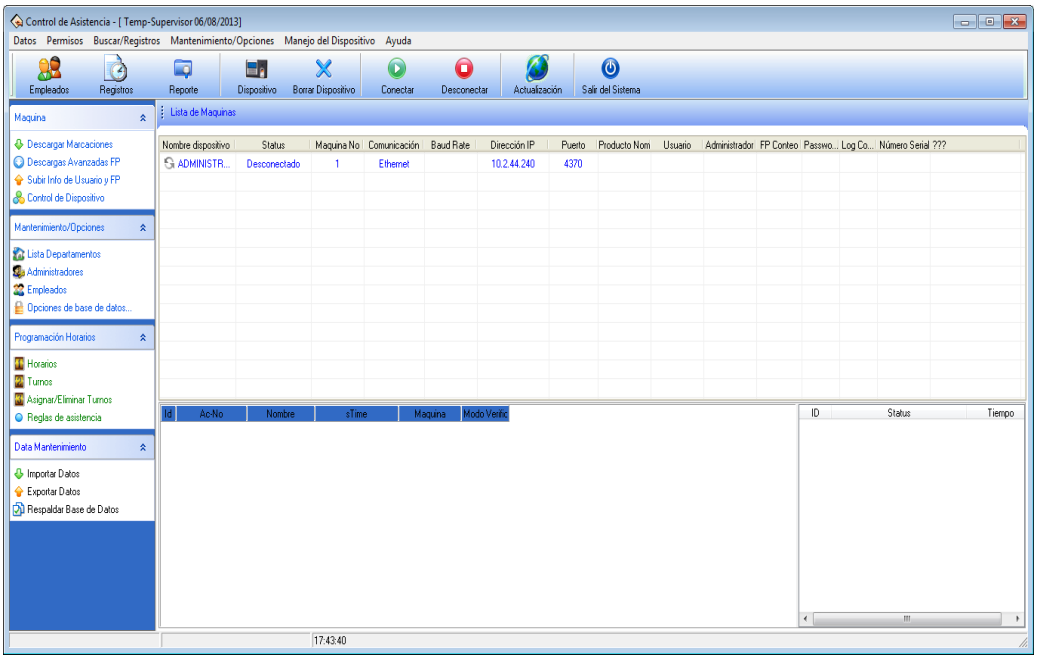


Figura 6.34. Pantalla del software

Fuente: Investigador

Una vez ingresado al programa Attendance Management damos clic en Dispositivo para ingresar a la configuración donde pondremos la dirección IP del reloj biométrico.

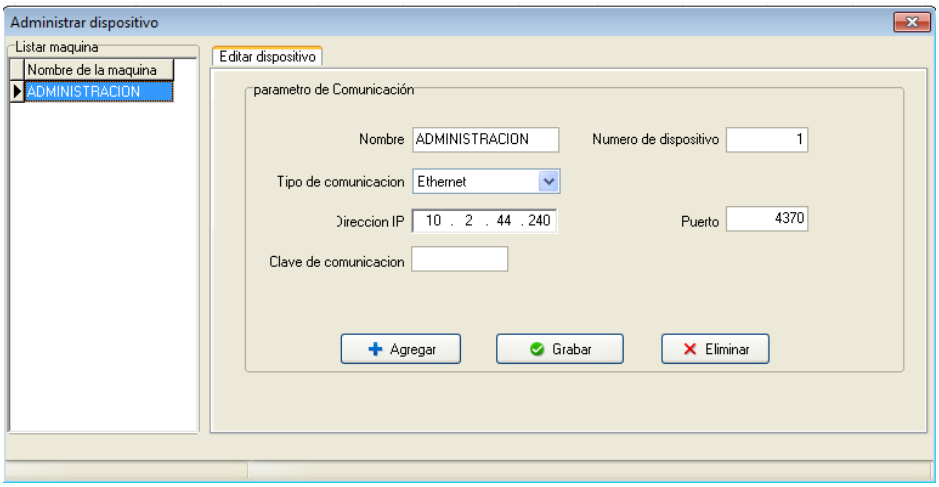


Figura 6.35. Pantalla de cambio de IP

Fuente: Investigador

Luego de haber configurado la dirección IP nos salimos de esa pantalla y nos conectamos al reloj biométrico seleccionando al dispositivo y dando clic en conectar.

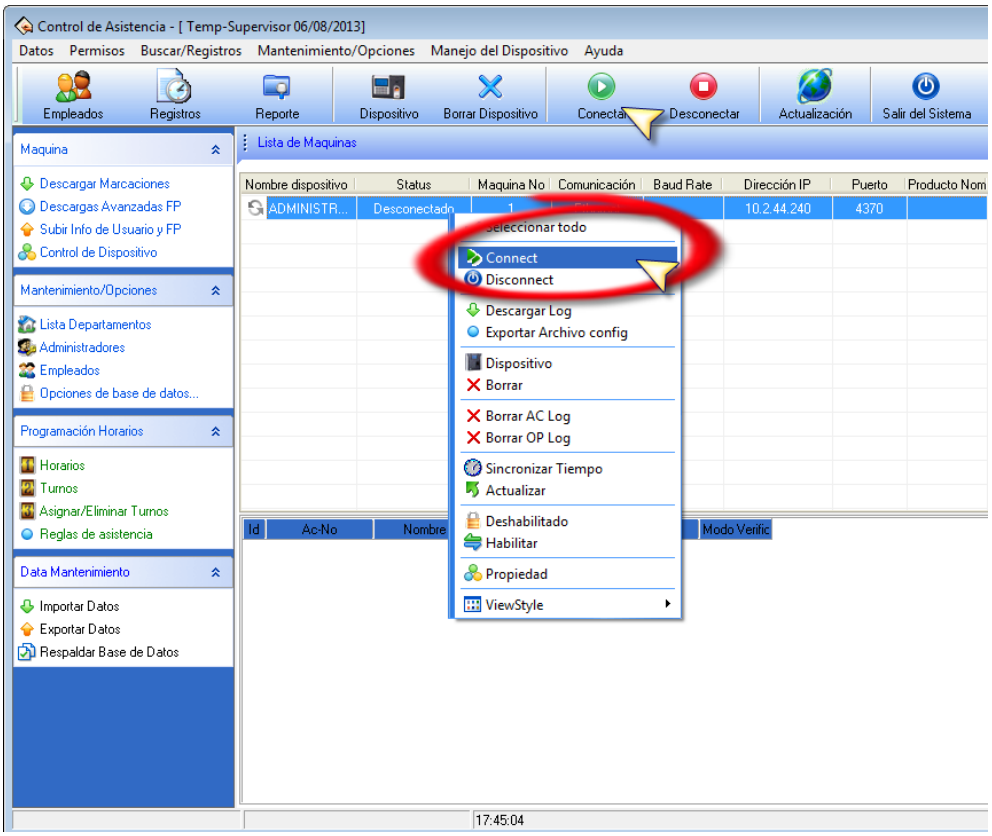


Figura 6.36. Conectar a un dispositivo

Fuente: Investigador

Una vez dado clic en conectar verificamos que esté conectado con el reloj biométrico el sistema del control del personal.

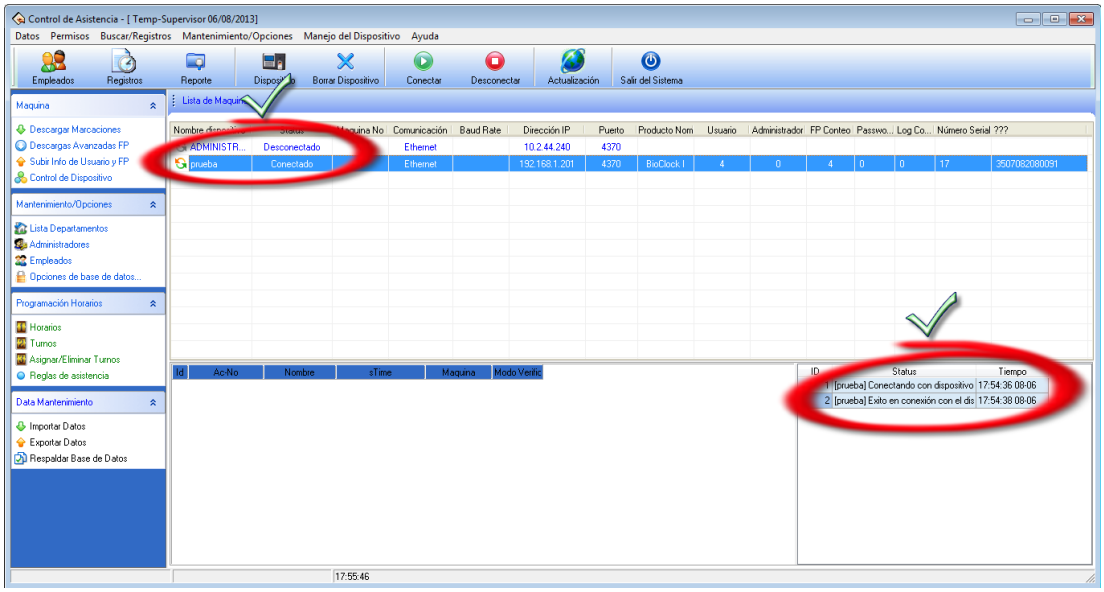


Figura 6.37. Conectado el dispositivo

Fuente: Investigador

Una vez que estemos conectados con el dispositivo o el reloj biométrico, damos clic derecho en el reloj y seleccionamos propiedades.

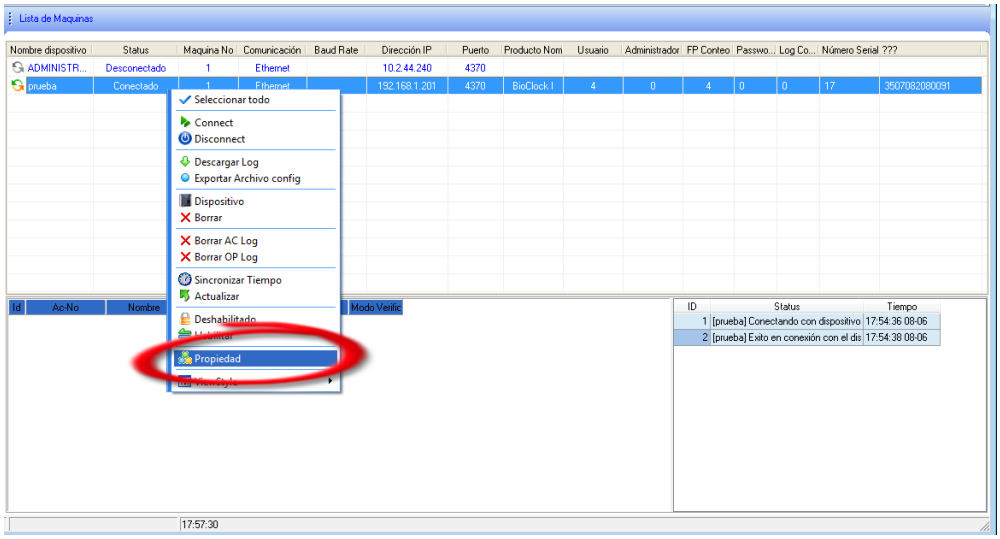
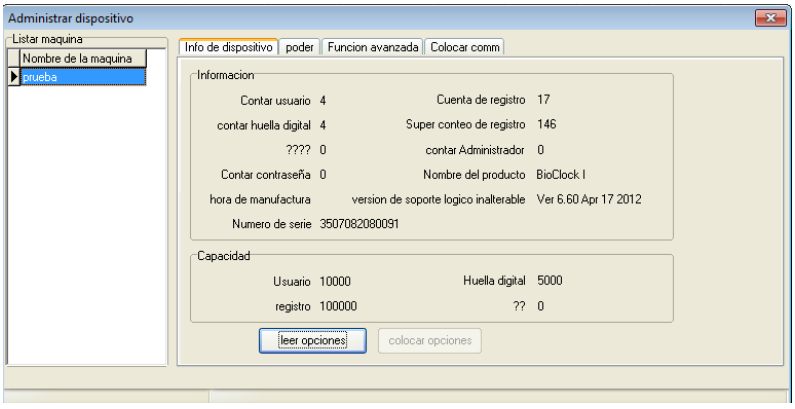


Figura 6.38: Propiedades del dispositivo

Fuente: Investigador

Nos desplegara la ventana de Administración del Dispositivo



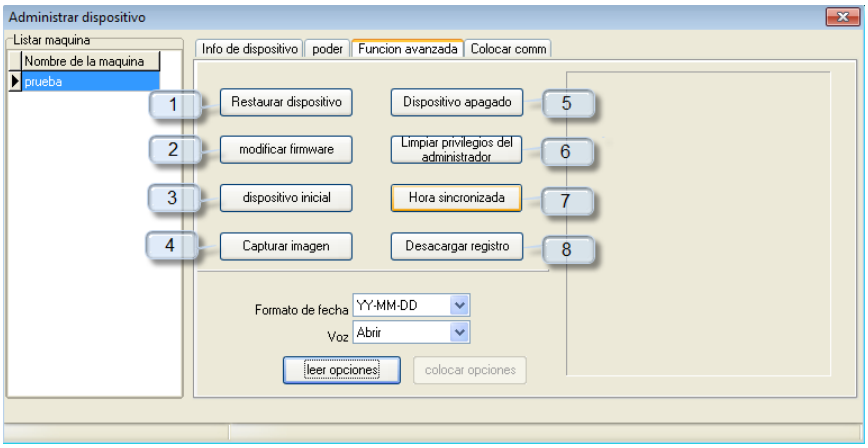


Figura 6.39. Pantalla de propiedades del dispositivo

Fuente: Investigador

Con esta pantalla nosotros podemos realizar cambios de información en el reloj biométrico como es:

1. **Restaurar el dispositivo.-** En esta opción nos permite restaurar el dispositivo a modo de fábrica borrando toda la información del reloj biométrico en lo que respecta a usuarios, huellas dactilares registradas y marcaciones realizadas además las configuraciones realizadas.

2. **Modificar firmware.-** Con esta opción podemos alterar o cambiar el firmware de configuración del dispositivo biométrico.

3. **Dispositivo inicial.-** En esta opción de Dispositivo Inicial nos permite borrar toda la información del reloj biométrico en lo que respecta a usuarios, huellas dactilares registradas y marcaciones realizadas.

4. **Capturar imagen.-** Dependiendo del tipo de reloj biométrico esta opción puede capturar una imagen desde el dispositivo al computador.

5. **Dispositivo apagado.-** En esta opción el software da una orden de apagado al reloj biométrico.

6. **Limpiar privilegios de administradores.-** Antes de dar clic en limpiar privilegios del administrador revisamos el reloj biométrico lo que está bloqueado y solo el administrador del dispositivo puede acceder a la información.

Figura 6.40. Pantalla del reloj biométrico bloqueada

Fuente: Investigador

Una vez revisada que verificamos que se encuentra bloqueado damos clic en Limpiar Privilegios del administrador

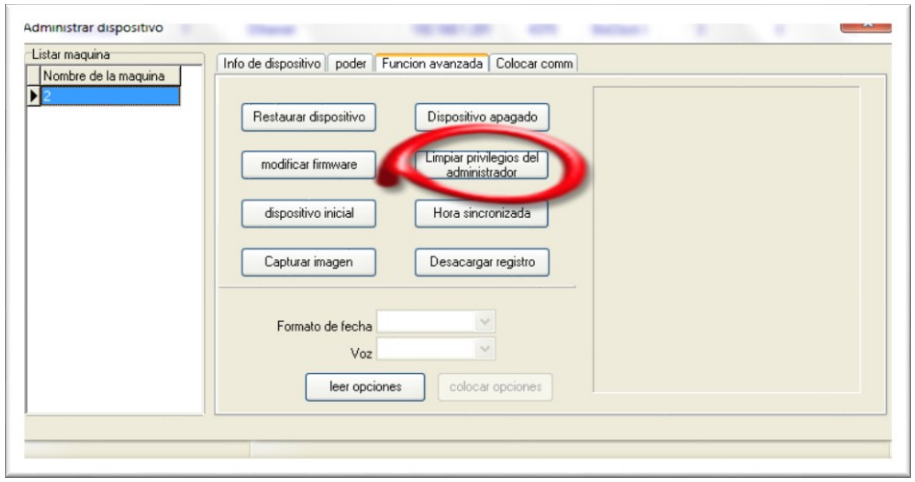


Figura 6.41. Limpiar privilegios

Fuente: Investigador

En esta pantalla clic en limpiar Privilegios del administrador en la cual nosotros le borramos todos los administradores que tiene en el reloj biométrico y así poder acceder a la información y poder manipular sin autorización del administrador.

Figura 6.42. Reloj biométrico sin acceso del administrador.

Fuente: Investigador

Podemos acceder al menú de reloj biométrico sin autenticación de un administrador y poder cambiar la fecha/ hora, borrar usuarios, borrar marcaciones, borrar los usuarios, cambiar la dirección IP, cambiar las configuraciones internas del reloj biométrico

7. **Hora sincronizada.-** En esta opción se sincroniza la fecha y hora del reloj biométrico con la hora del sistema de Windows; si acaso la hora de Windows no se encuentra la hora igualada el reloj biométrico se configura con esa hora.

8. **Descargar registros.-** Se puede enviar una orden para descargar la información de los registros al sistema que lo administra la asistencia del personal.

6.7.3. Alteración de información en la base de datos del software de control del personal.

Cuando se instala el sistema ATTENDANCE MANAGEMENT la referencia de instalación es en la ruta: "**C:\Program Files (x86)\Att2008"** por defecto; en esta carpeta se crea la base de datos que es utilizada en el software de control para guardar los registros, usuarios y configuración internar del sistema.

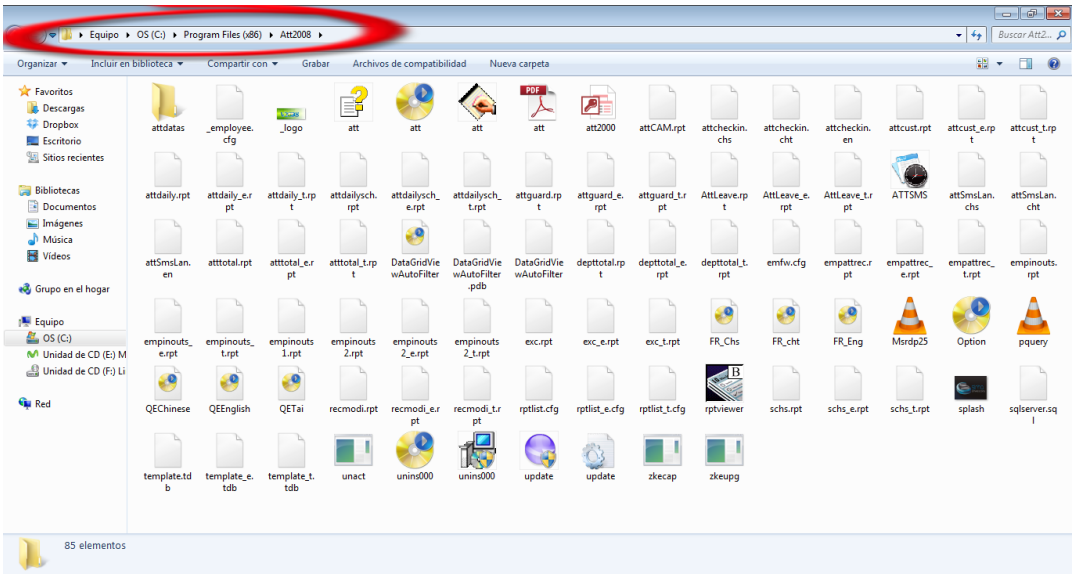
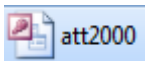


Figura 6.43. Directorio de instalación del sistema Atendance Manager

Fuente: Investigador

La base de datos que utiliza este software se encuentra implementado en Microsoft Access  y el nombre de la base de datos es 

para que sea reconocida por el software

Alteración de datos en la base de datos

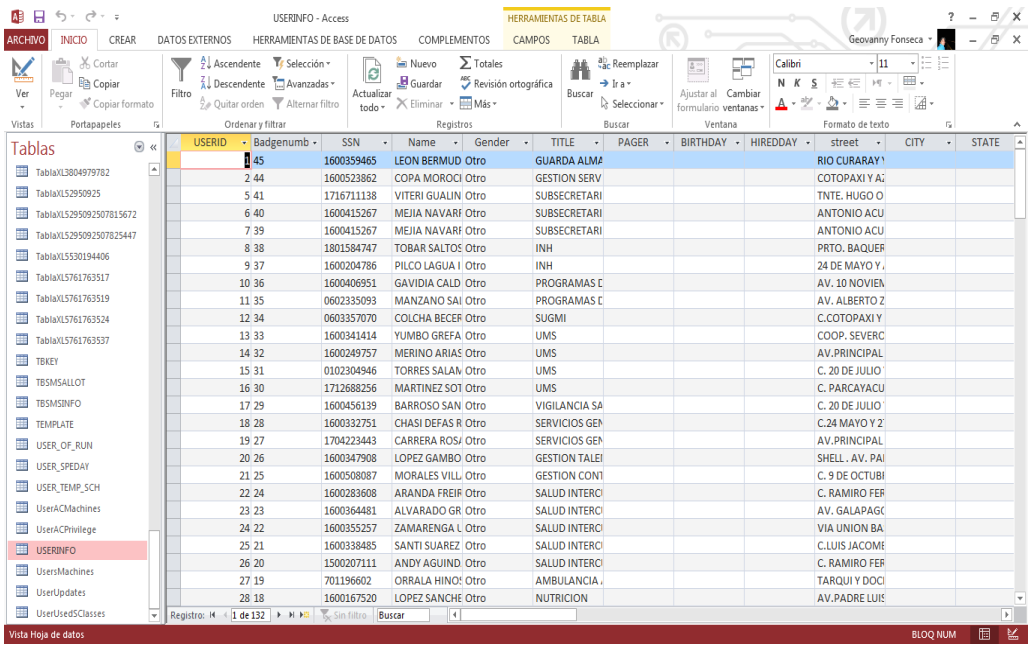


Figura 6.44. Pantalla de la base de datos

Fuente: Investigador

Las tablas de configuración del sistema son:

ATTPARAM.

En esta tabla encontramos toda la configuración del sistema de control de asistencia, la misma que se puede alterar el programa causando des configuración al sistema.

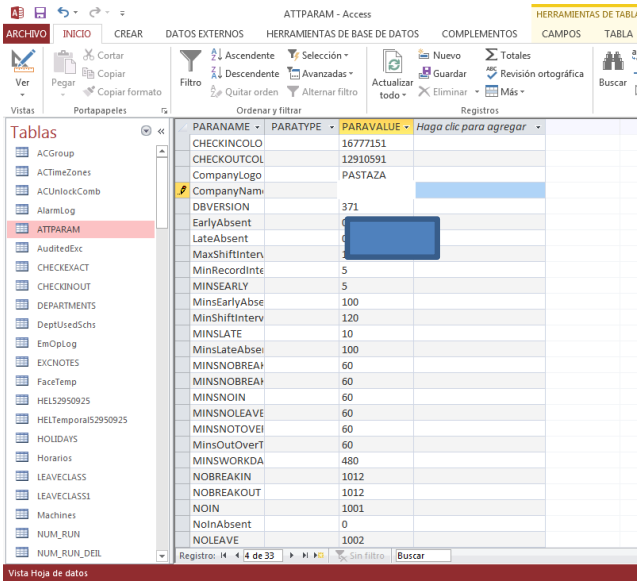


Figura 6.45. Tabla ATTPARAM

Fuente: Investigador

En la figura siguiente podemos observar las configuraciones las mismas que están en la tabla ATTPARAM

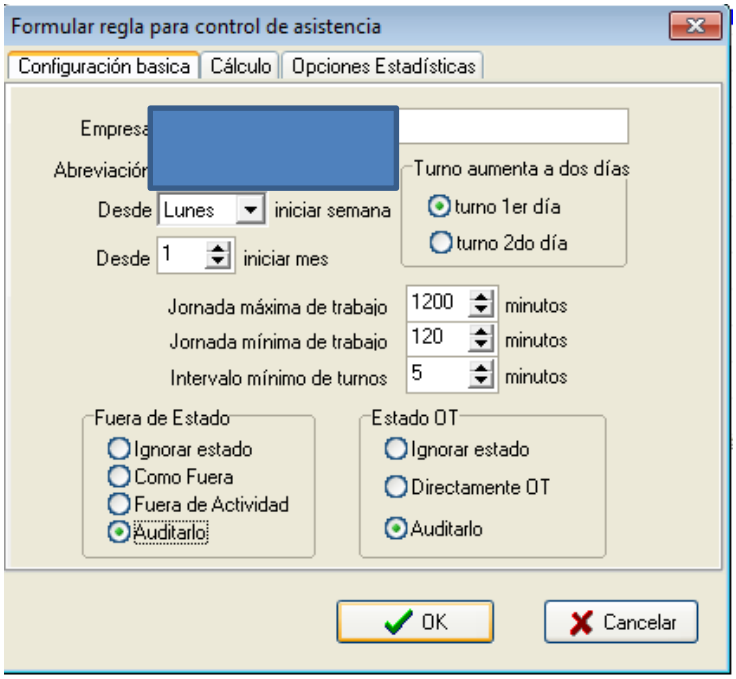
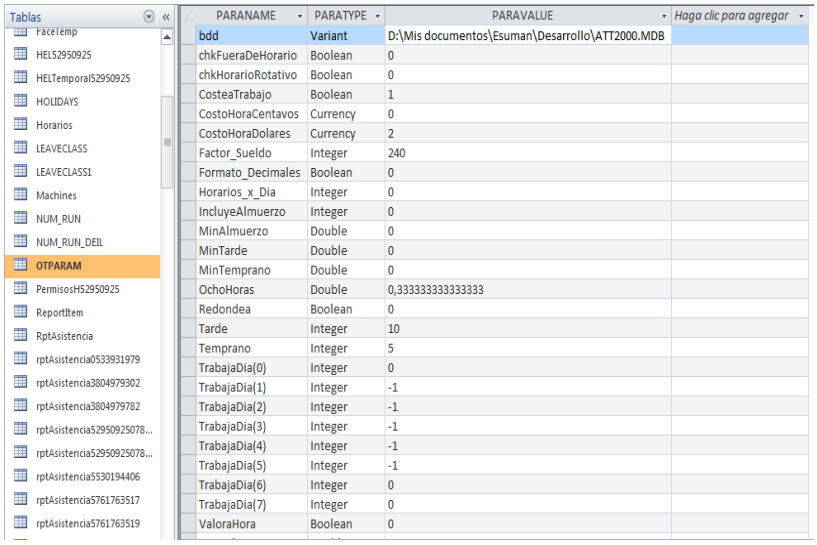


Figura 6.46. Muestra en el software

Fuente: Investigador

OTPARAM.- En esta tabla podemos alterar las reglas para generar reportes de asistencias como son el tiempo de almuerzo, horas extras y asistencias de cada usuario.



PARANAME	PARATYPE	PARAVALUE	Haga clic para agregar
bdd	Variant	D:\Mis documentos\Esuman\Desarrollo\ATT2000.MDB	
chkFueraDeHorario	Boolean	0	
chkHorarioRotativo	Boolean	0	
CosteaTrabajo	Boolean	1	
CostoHoraCentavos	Currency	0	
CostoHoraDolares	Currency	2	
Factor_Sueldo	Integer	240	
Formato_Decimales	Boolean	0	
Horarios_x_Dia	Integer	0	
IncluyeAlmuerzo	Integer	0	
MinAlmuerzo	Double	0	
MinTarde	Double	0	
MinTemprano	Double	0	
OchoHoras	Double	0,333333333333333	
Redondea	Boolean	0	
Tarde	Integer	10	
Temprano	Integer	5	
TrabajaDia(0)	Integer	0	
TrabajaDia(1)	Integer	-1	
TrabajaDia(2)	Integer	-1	
TrabajaDia(3)	Integer	-1	
TrabajaDia(4)	Integer	-1	
TrabajaDia(5)	Integer	-1	
TrabajaDia(6)	Integer	0	
TrabajaDia(7)	Integer	0	
ValoraHora	Boolean	0	

Figura 6.47. OTPARAM

Fuente: Investigador

En la figura siguiente podemos observar las configuraciones de los cálculos de horas extras y consideraciones en la hora de entrada y de salida las mismas que están en la tabla OTPARAM

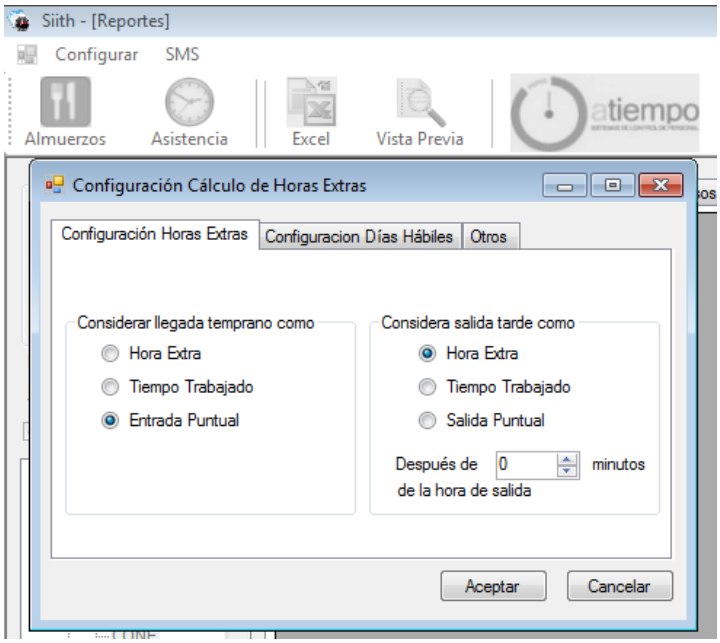


Figura 6.48. Muestra en el sistema donde afecta los cambios realizados

Fuente: Investigador

MACHINES

En esta tabla se encuentran el listado de todos los relojes biométricos que están configurados con el sistema con su dirección IP y Puerto que sean configurados.

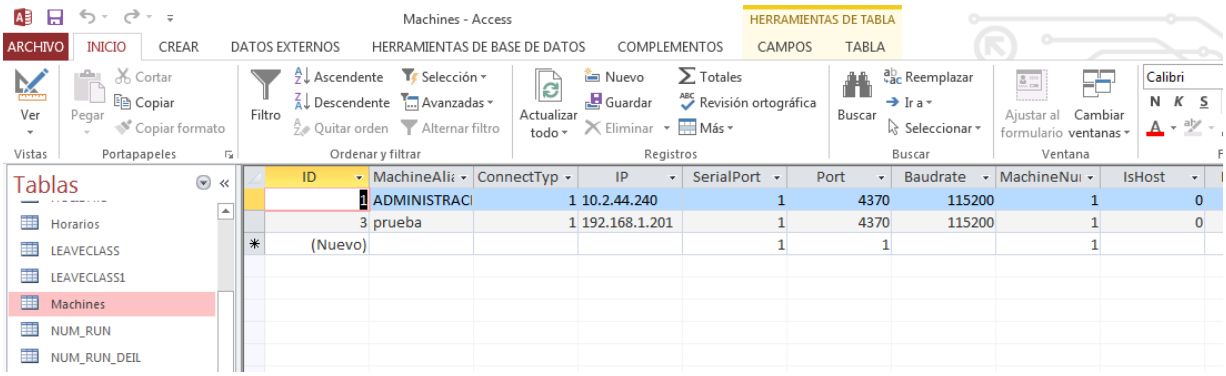


Figura 6.49. Machines

Fuente: Investigador

En la figura siguiente podemos observar los relojes que se han añadido o registrado en el sistema de control de asistencia las mismas que se pueden utilizar para descargarse la información las mismas que están en la tabla Machines.

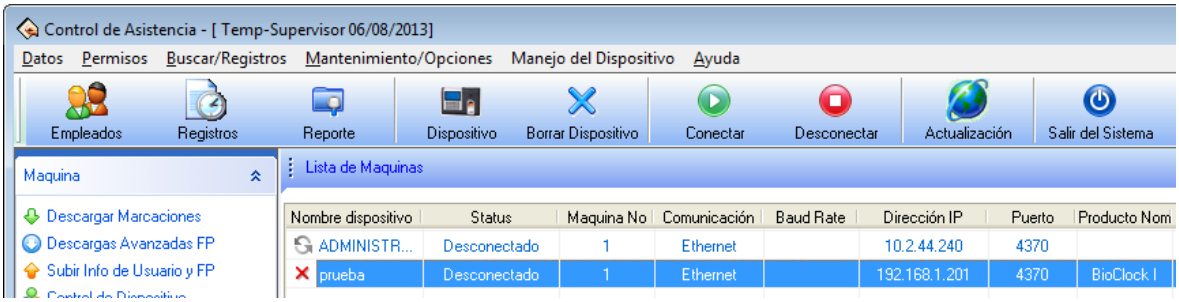


Figura 6.50. Informacion que se puede verificar en el sistema.

Fuente: Investigador

HOLIDAYS

En esta tabla se encuentran el listado de los días festivos que se han ingresado mediante el software de control para que en esos días el sistema no arroje días ausentes a todo el personal que registra en su organización.

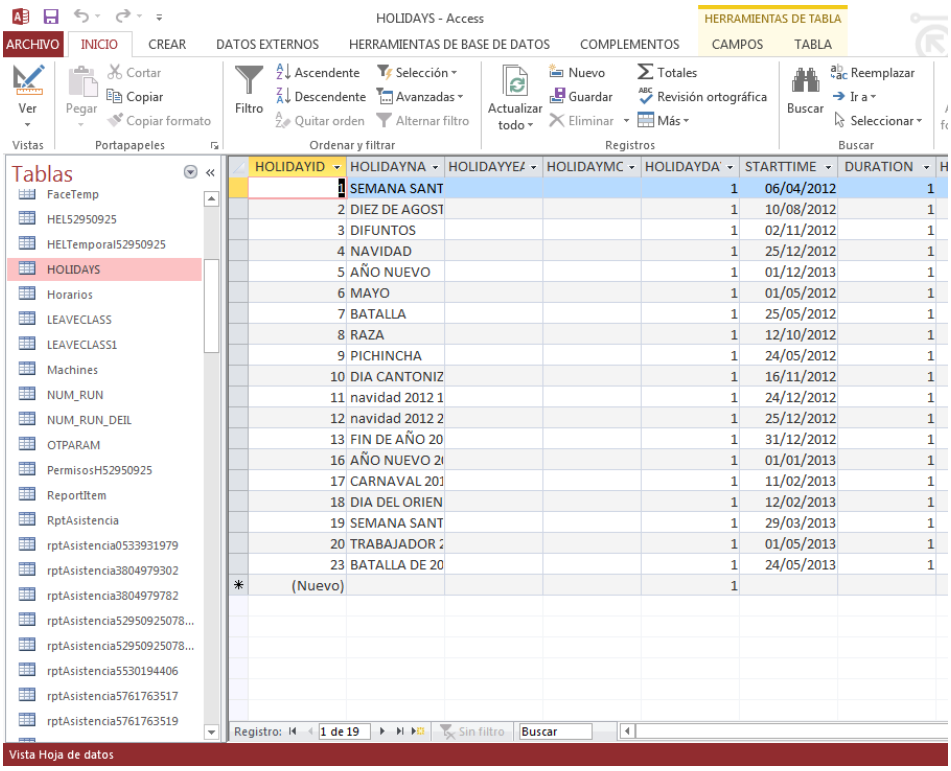


Figura 6.51. HOLIDAYS

Fuente: Investigador

En la figura siguiente podemos observar los ingresos de las fechas de los días feriados registrados en el sistema de control de asistencia las mismas que están en la tabla Holidays.

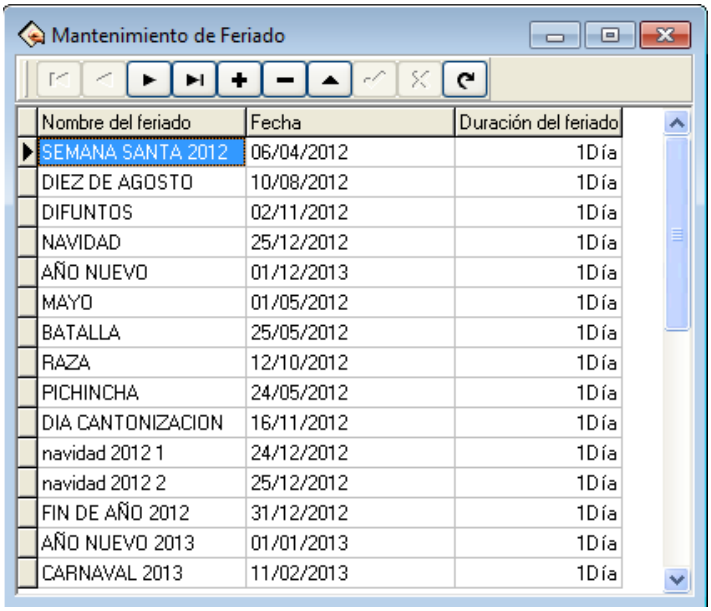


Figura 6.52. Muestra en el sistema la información que se puede manipular

Fuente: Investigador

SCHCLASS

En esta tabla se encuentran el listado de los horarios que se han ingresado mediante el software de control.

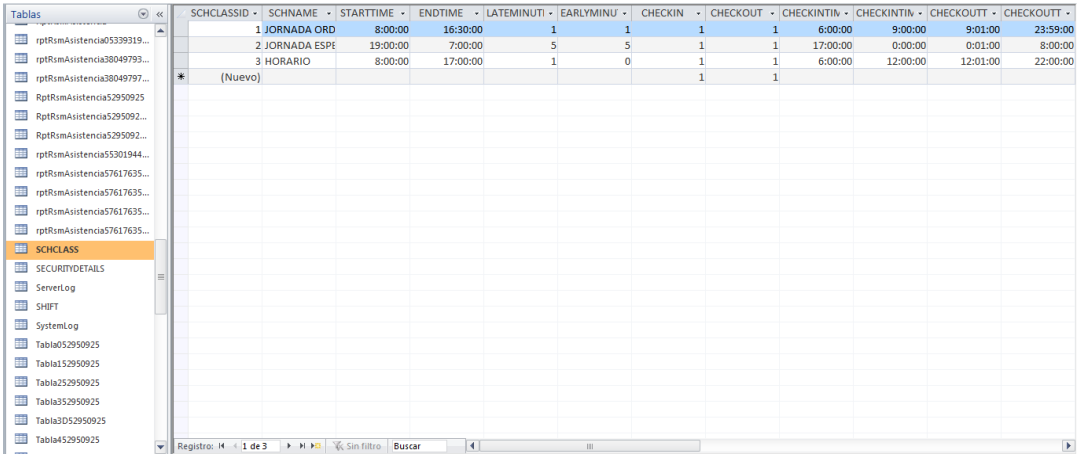


Figura 6.53. SCHCLASS

Fuente: Investigador

En la figura siguiente podemos observar los horarios o turnos que ingresamos por usuario o grupos en el sistema de control de asistencia las mismas que están en la tabla SCHCLASS.

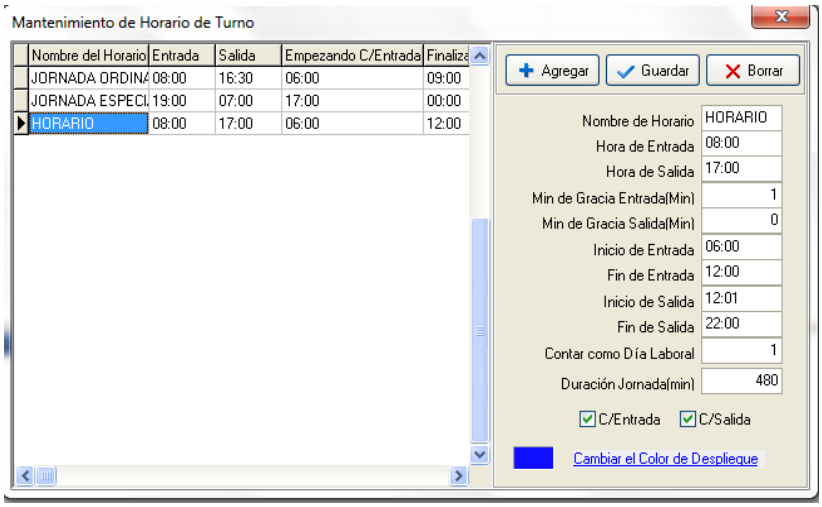
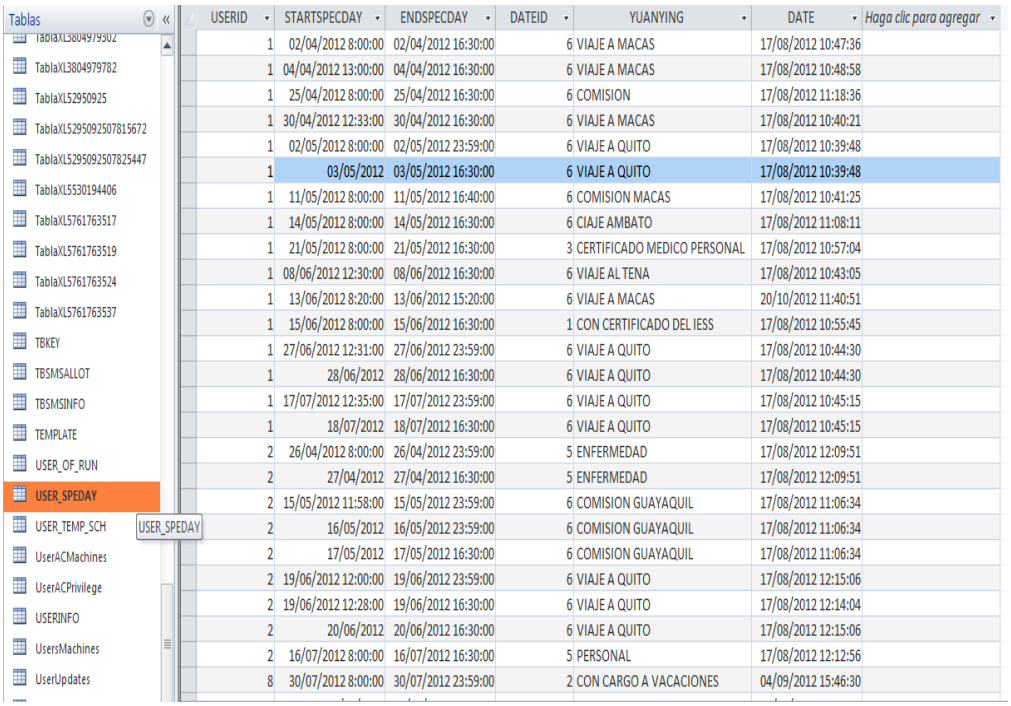


Figura 6.54. Muestra en el sistema

Fuente: Investigador

USER_SPEDAY

En esta tabla se encuentran el listado de los permisos que se dan a cada usuario que registra en el reloj biométrico.



USERID	STARTSPECDAY	ENDSPECDAY	DATEID	YUANYING	DATE	Haga clic para agregar
1	02/04/2012 8:00:00	02/04/2012 16:30:00	6	VIAJE A MACAS	17/08/2012 10:47:36	
1	04/04/2012 13:00:00	04/04/2012 16:30:00	6	VIAJE A MACAS	17/08/2012 10:48:58	
1	25/04/2012 8:00:00	25/04/2012 16:30:00	6	COMISION	17/08/2012 11:18:36	
1	30/04/2012 12:33:00	30/04/2012 16:30:00	6	VIAJE A MACAS	17/08/2012 10:40:21	
1	02/05/2012 8:00:00	02/05/2012 23:59:00	6	VIAJE A QUITO	17/08/2012 10:39:48	
1	03/05/2012	03/05/2012 16:30:00	6	VIAJE A QUITO	17/08/2012 10:39:48	
1	11/05/2012 8:00:00	11/05/2012 16:40:00	6	COMISION MACAS	17/08/2012 10:41:25	
1	14/05/2012 8:00:00	14/05/2012 16:30:00	6	CIAJE AMBATO	17/08/2012 11:08:11	
1	21/05/2012 8:00:00	21/05/2012 16:30:00	3	CERTIFICADO MEDICO PERSONAL	17/08/2012 10:57:04	
1	08/06/2012 12:30:00	08/06/2012 16:30:00	6	VIAJE AL TENA	17/08/2012 10:43:05	
1	13/06/2012 8:20:00	13/06/2012 15:20:00	6	VIAJE A MACAS	20/10/2012 11:40:51	
1	15/06/2012 8:00:00	15/06/2012 16:30:00	1	CON CERTIFICADO DEL IESS	17/08/2012 10:55:45	
1	27/06/2012 12:31:00	27/06/2012 23:59:00	6	VIAJE A QUITO	17/08/2012 10:44:30	
1	28/06/2012	28/06/2012 16:30:00	6	VIAJE A QUITO	17/08/2012 10:44:30	
1	17/07/2012 12:35:00	17/07/2012 23:59:00	6	VIAJE A QUITO	17/08/2012 10:45:15	
1	18/07/2012	18/07/2012 16:30:00	6	VIAJE A QUITO	17/08/2012 10:45:15	
2	26/04/2012 8:00:00	26/04/2012 23:59:00	5	ENFERMEDAD	17/08/2012 12:09:51	
2	27/04/2012	27/04/2012 16:30:00	5	ENFERMEDAD	17/08/2012 12:09:51	
2	15/05/2012 11:58:00	15/05/2012 23:59:00	6	COMISION GUAYAQUIL	17/08/2012 11:06:34	
2	16/05/2012	16/05/2012 23:59:00	6	COMISION GUAYAQUIL	17/08/2012 11:06:34	
2	17/05/2012	17/05/2012 16:30:00	6	COMISION GUAYAQUIL	17/08/2012 11:06:34	
2	19/06/2012 12:00:00	19/06/2012 23:59:00	6	VIAJE A QUITO	17/08/2012 12:15:06	
2	19/06/2012 12:28:00	19/06/2012 16:30:00	6	VIAJE A QUITO	17/08/2012 12:14:04	
2	20/06/2012	20/06/2012 16:30:00	6	VIAJE A QUITO	17/08/2012 12:15:06	
2	16/07/2012 8:00:00	16/07/2012 16:30:00	5	PERSONAL	17/08/2012 12:12:56	
8	30/07/2012 8:00:00	30/07/2012 23:59:00	2	CON CARGO A VACACIONES	04/09/2012 15:46:30	

Figura 6.55. USER_SPEDAY

Fuente: Investigador

En la figura siguiente podemos observar la forma de como ingresar los permisos a cada usuario que están registrados en el sistema de control de asistencia las mismas que están en la tabla USER_SPEDAY.

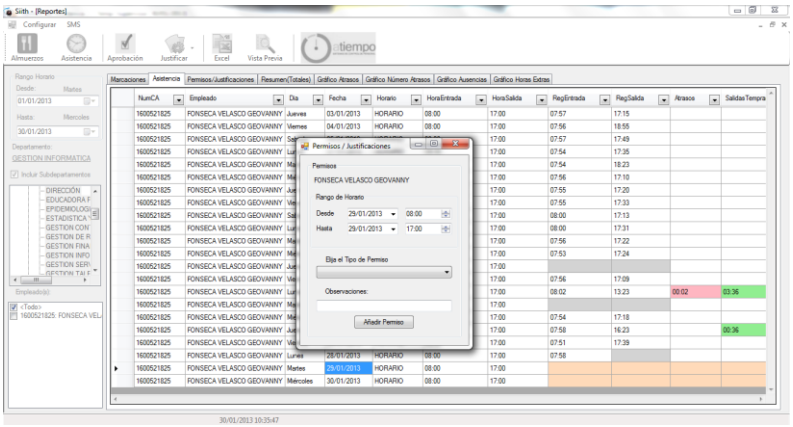


Figura 6.56. Muestra en el sistema

Fuente: Investigador

ATTCHECKIN.EN

En este archivo plano se encuentran todas las etiquetas del sistema de control de asistencia.

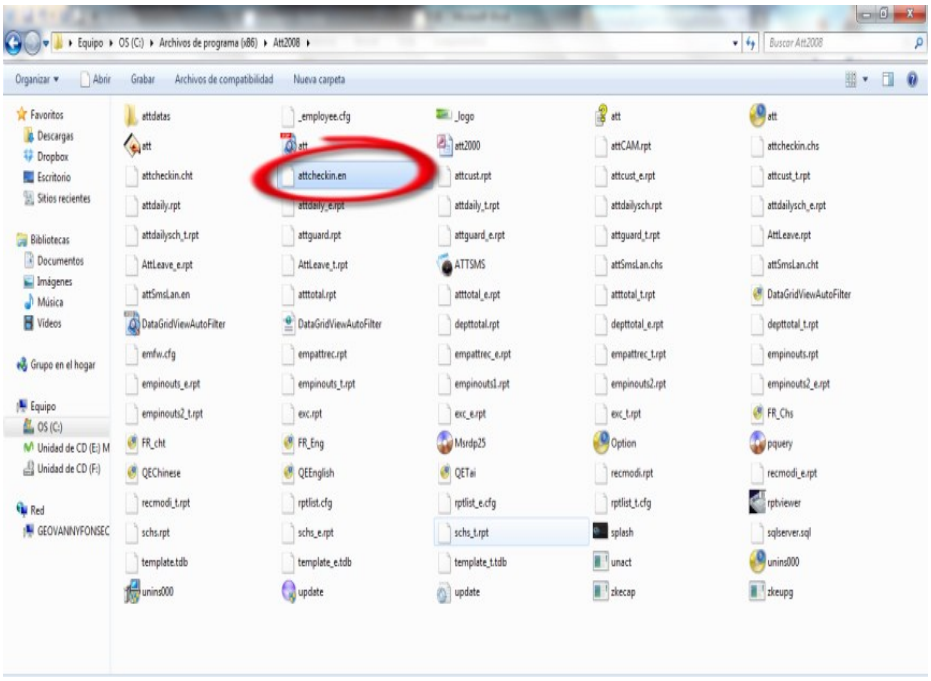


Figura 6.57. ATTCHECKIN.EN

Fuente: Investigador

En la figura siguiente podemos observar la etiqueta que podemos cambiar para efecto de ejemplo en el sistema de control del personal utilizamos el OverTime.

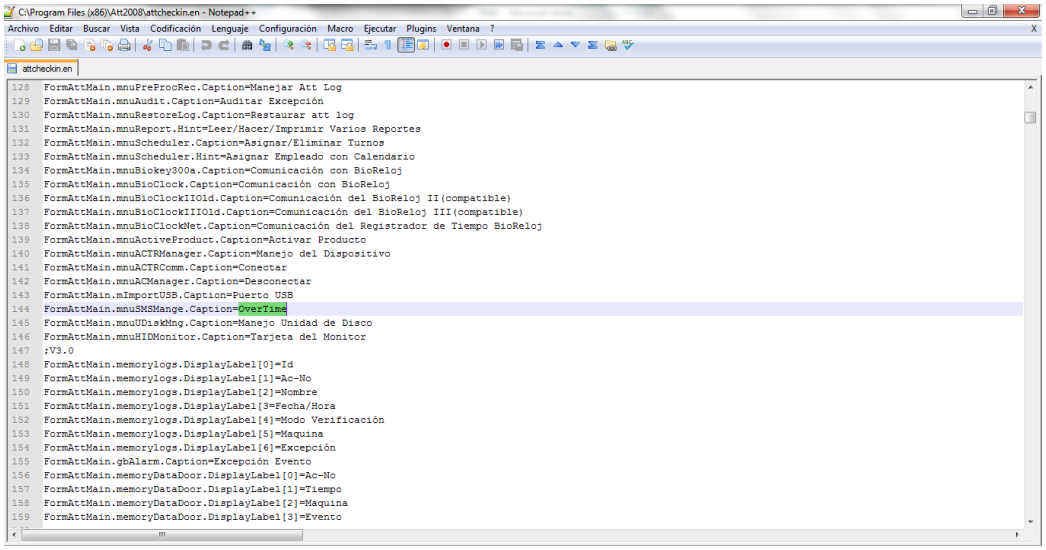


Figura 6.58. Vista del ATTCHECKIN.EN

Fuente: Investigador

En la figura siguiente podemos observar el nombre de la etiqueta que muestra en el archivo plano la misma que está ubicada en la carpeta de instalación sin ninguna restricción.

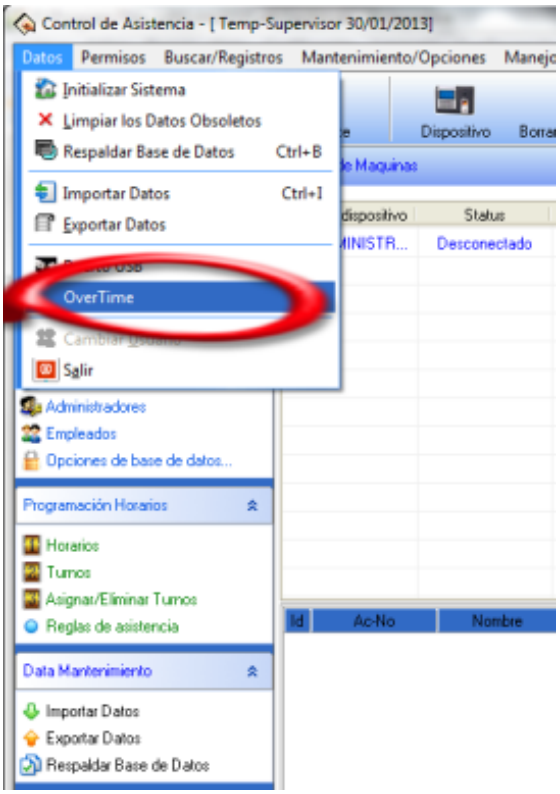


Figura 6.59. Muestra en el sistema

Fuente: Investigador

6.7.4. MANUAL BÁSICO DE CONFiguraCIONES

RELOJ BIOMÉTRICO

El reloj biométrico es un sistema independiente que registra los eventos de entrada y salida de los empleados de una empresa a través de su huella digital o de un password, quedando en él almacenada la hora y el tipo de marcación realizada, esta información es descargada y analizada por el software de control para la generación de los diferentes reportes.

La capacidad de almacenamiento de huellas es de 5000 y de marcaciones es de 100000. Es una buena opción para cualquier tipo de empresa que requiera llevar un registro del control de asistencia del personal.

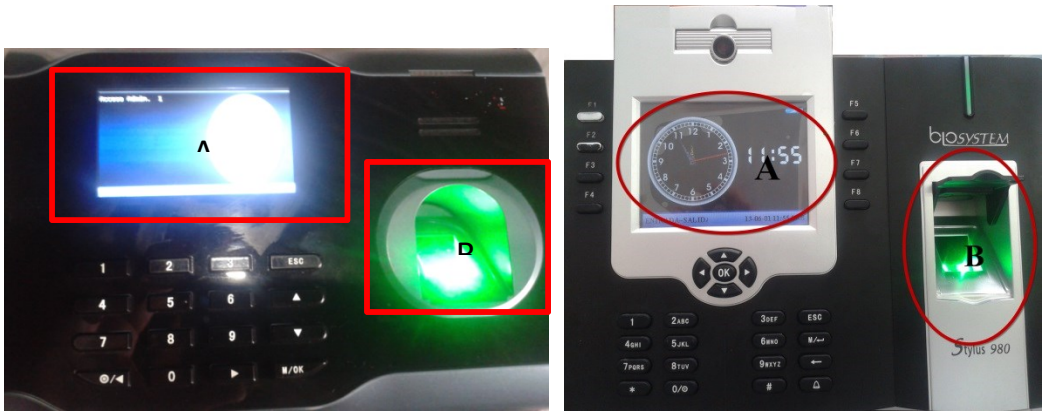


Figura 6.60. Reloj biométrico

Fuente: Investigador

DESCRIPCIÓN DEL EQUIPO

- **PANTALLA**

  Posee una pantalla full color ver figura 53 parte A

- **LECTOR ÓPTICO**

  Lector óptico en la cual podemos registrar las huellas dactilares y la tarjeta de proximidad ver Figura 6.58 parte B.

TECLAS DE FUNCIONES

Figura 6.61. Teclado

Fuente: Investigador

M/Ok: Nos permite ingresar al menú principal.

▼: Permite el desplazamiento a través del menú hacia abajo.

▲: Permite el desplazamiento a través del menú hacia arriba.

O/◄: Permite el desplazamiento a través del menú hacia arriba y tecla de encendido; controla el encendido y apagado del dispositivo, basta con mantenerla oprimida durante unos segundos.

►: Permite el desplazamiento a través del menú hacia la derecha.

ESC: En los submenús se usa para cancelar una operación en curso.

1-9: Teclas que tiene la numeración mostrada en cada tecla.

a) LED´S INDICADORES

Verde: Muestra esta luz cuando el reloj reconoce la huella dactilar o no está registrada.

Rojo: Muestra esta luz cuando el reloj no reconoce la huella dactilar o no está registrada.

b) PARLANTE

Nos indica mediante voz las accione realizadas las mismas que pueden ser:

- Acceso correcto
- Clave incorrecta
- Acceso denegado
- Código no valido
- Intente de nuevo por favor
- Reintroduzca el código
- Huella duplicada
- Ya ha sido registrado

Figura 6.62. Parlantes posteriores

Fuente: Investigador

c) BOTÓN DE RESETEO

Al pulsar este botón el equipo se reinicia este botón se utiliza cuando el equipo se encuentre bloqueado.

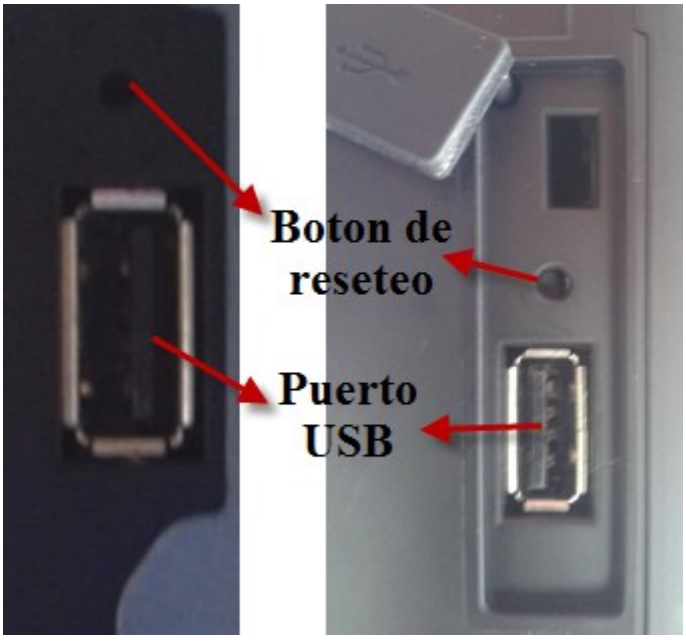


Figura 6.63. Puertos USB y Boton de reseteo

Fuente: Investigador

d) PUERTO USB

Mediante este puerto figura 6 podemos descargar la información del sistema biométrico.

e) TARJETA DE RED

Mediante este puerto podemos comunicarnos a través de la red LAN con la computadora y el reloj biométrico.

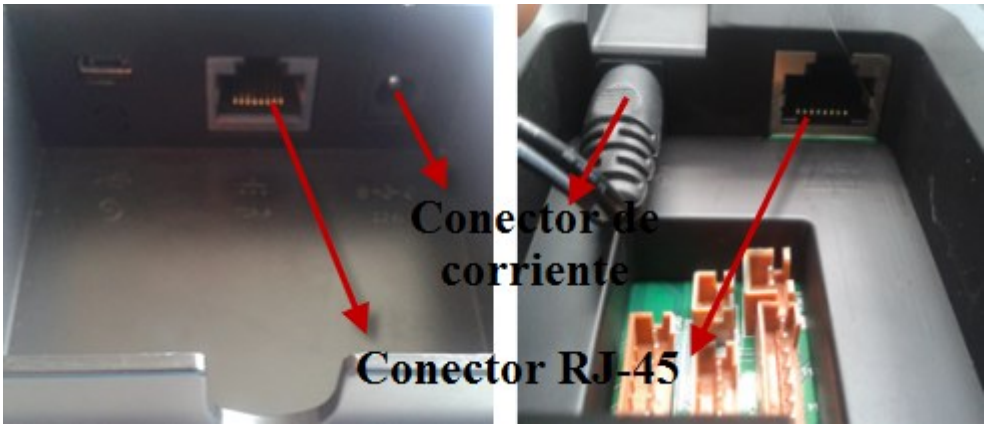


Figura 6.64. Puertos

Fuente: Investigador

- **CONECTOR RJ-45**

  Conector figura 57 por donde conectamos el cable de red a un

- **CONECTOR DE CORRIENTE**

  Conector figura 57 por donde conectamos la batería mini ups o directamente el cable de poder del dispositivo.

f) BATERÍA DE MINI UPS

Batería de respaldo con una duración de 4 ahora que nos mantendrá prendido el reloj biométrico.

Figura 6.65. Bateria de respaldo o UPS

Fuente: Investigador

g) ADAPTADOR DE LUZ 5V

Figura 6.**66.** Adaptador de luz

Fuente: Investigador

h) SOPORTE

Este soporte nos ayuda a sujetar al reloj biométrico contra la pared.

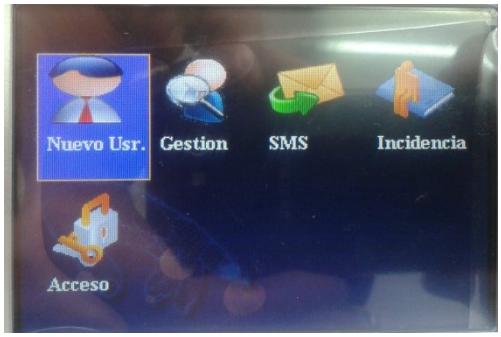
Figura 6.67. Soporte del dispositivo biométrico

Fuente: Investigador

CONCEPTOS BÁSICOS

1. GRABAR UN USUARIO

Para registrar un usuario nuevo ingresamos al menú principal con la tecla **M/Ok** posteriormente asignamos la opción de **Usuarios** y **Nuevo Usuario** como nos indica las siguiente figura.



Modelo 1 **Modelo 2**

Figura 6.68. Pantalla principal

Fuente: Investigador

En la siguiente pantalla ingresamos la siguiente información:

- Número de identificación del usuario.

- Registro de la o las huellas dactilares la mismas que se pueden registrar hasta 10 verificando que tengamos una buena calidad de reconocimiento.

Modelo 1 **Modelo 2**

Figura 6.69. Registro de huellas dactilares

Fuente: Investigador

- Asignarle una contraseña o password,

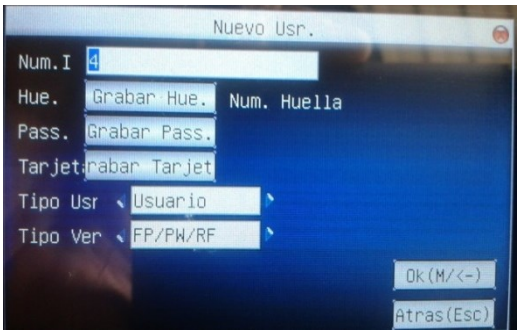
- Registrar una tarjetas de proximidad que haya sido asignada al usuario

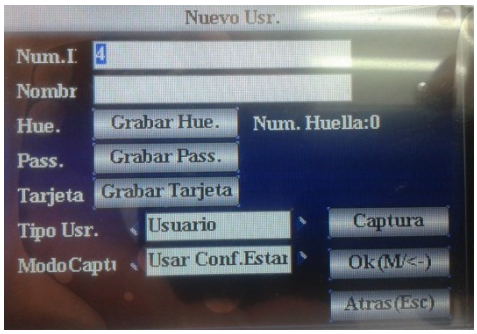
Modelo 1 **Modelo 2**

Figura 6.70. Registro de tarjetas de proximidad

Fuente: Investigador

- Identificar el perfil de usuario





Modelo 1 **Modelo 2**

Figura 6.71. Pantalla de ingreso a un nuevo usuario

Fuente: Investigador

- **Perfiles de usuarios**
  - **Usuario:** Son usuarios que pueden registrar la marcación mediante huella, contraseña, tarjeta de proximidad.

  - **Subadministrador:** Son usuarios que pueden registrar la marcación mediante huella, contraseña, tarjeta de proximidad, agregar nuevos usuario y ver los registros de los usuario registrados.

- **Administrador:** Son usuarios que pueden registrar la marcación mediante huella, contraseña, tarjeta de proximidad y acceder a todo el menú principal.

1.1. IDENTIFICAR UN USUARIO EN EL SISTEMA BIOMÉTRICO

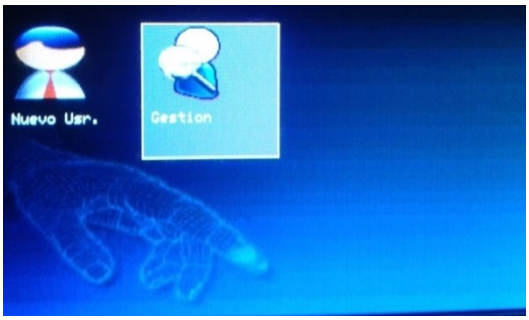
- Si el usuario ha sido grabado por medio de su huella digital basta con ubicar el dedo registrado con anterioridad sobre el sensor óptico.
- Si la persona se grabó con un password inicialmente deberá digitar su ID y luego presionar OK, seguidamente deberá digitar su contraseña o password confirmándolo con la tecla OK.
- Si la persona ha sido grabada por medio de tarjeta de proximidad basta con ubicar la tarjeta sobre el sensor óptico.
- Si la persona se grabó con la huella, un password o tarjeta de proximidad, podrá igualmente realizar su verificación con cualquiera de los tres como se describió anteriormente.
- En caso que el sistema biométrico no reconozca algún tipo de identificación anteriormente mencionada nos indicara mediante luz roja los que intentemos de nuevo caso contrario nos indicará que ya hemos registrado

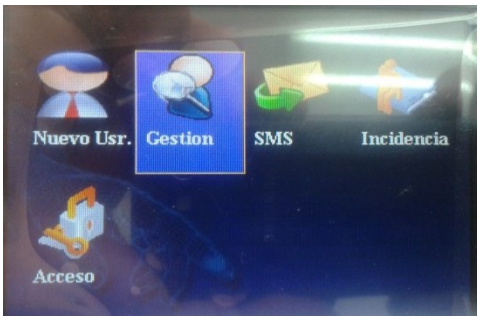
Figura 6.72. Colores de los LEEDS

Fuente: Investigador

1.2. BORRAR UN USUARIO DEL SISTEMA BIOMÉTRICO

Para borrar a una persona grabada en el sistema ingresamos al menú principal y gestión de usuarios donde se encuentra el listado de todos los usuarios registrados



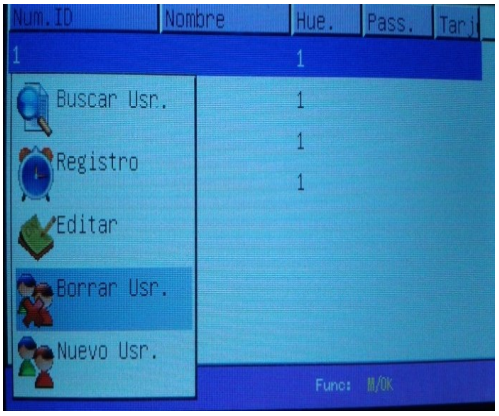


Modelo 1 **Modelo 2**

Figura 6.73. Opcion de gestión de usuarios

Fuente: Investigador

Se deberá digitar el ID que corresponde a la persona que se desea borrar del sistema seguida de la tecla OK. Aparecerán en pantalla un submenú donde seleccionamos borrar usuario

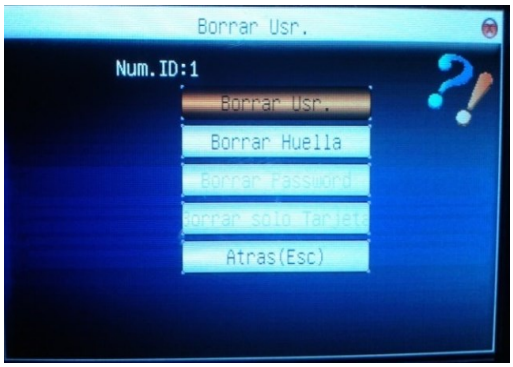


Modelo 1 **Modelo 2**

Figura 6.74. Borrar un usuario

Fuente: Investigador

Una vez ingresado a la pantalla de borrar usuario nos desplegara un listado de que es lo que queremos borrar ya sea al todo el usuario o solo las huellas, la contraseña, la tarjera de proximidad.



Modelo 1 **Modelo 2**

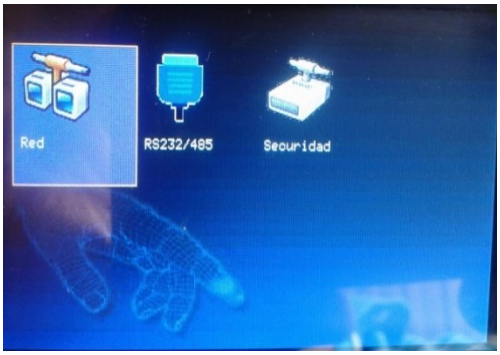
Figura 6.75. Opciones de borrado

Fuente: Investigador

Nota: Es posible borrar la información (Huella, password o tarjeta de proximidad) de la persona sin necesidad de borrarla del sistema.

2. COMUNICACIÓN

Para ingresar una dirección IP en el reloj biométrico ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la opción de **Comunicación** y **Red** como nos indica las siguiente figura.

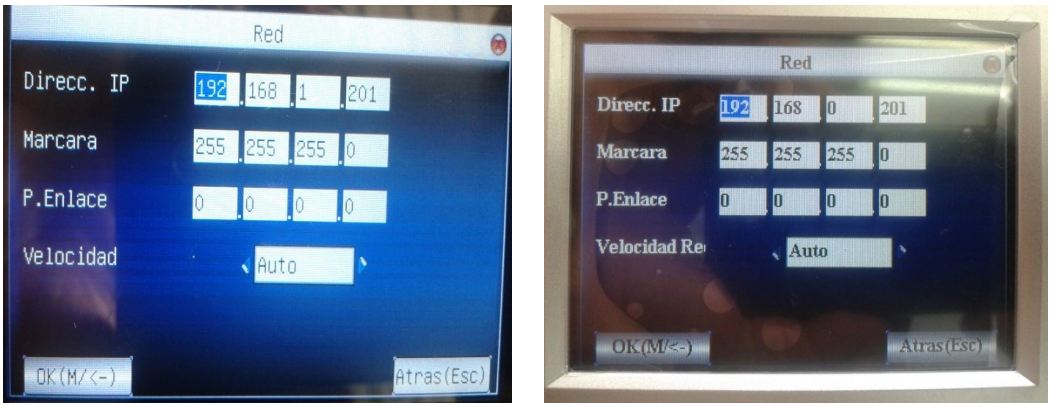


Modelo 1 **Modelo 2**

Figura 6.76. Pantalla de comunicaciones

Fuente: Investigador

El terminal puede transmitir y recibir información de un computador, pero para que esta comunicación se pueda establecer primero se deben configurar la dirección IP, la dirección IP por defecto es la dirección 192.168.0.201 la misma que puede ser cambiada de acuerdo a sus requerimientos.



Modelo 1 **Modelo 2**

Figura 6.77. Opciones del direccionamiento IP

Fuente: Investigador

Las opciones de Dirección IP, Mascara y Puerta de Enlace pueden ser configuradas con solo ubicar el cursor frente a cada una y por medio de las teclas de desplazamiento hacer la selección que se desea seguida con las teclas de números digitar seguidamente la tecla OK para guardar los cambios realizados.

La velocidad de la red la dejamos en auto, pero puede seleccionar entre las siguientes opciones 100M, AUTO, 10M según sus requerimientos.

Nota: Siempre que haga cambios en los parámetros de comunicaciones, es necesario apagar y encender el reloj nuevamente.

3. CONFiguraCIÓN DEL SISTEMA

El sistema cuenta básicamente con ocho áreas que pueden ser configuradas, las cuales son las opciones del sistema, datos, actualización, teclado, display, reseteo, timbres y alimentación.

Modelo 1 **Modelo 2**

Figura 6.78. Configuracion del sistema

Fuente: Investigador

Para tener acceso a estas áreas primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la opción de Sistema como nos indica las siguiente figura.

3.1. SISTEMA

En esta ventana podemos configurar:

- **Comparación 1:1 o 1:N.-** La cual nos permite seleccionar el nivel de seguridad para la comparación uno a uno o de uno a varios.
- **El formato de la fecha.**- la cual podemos identificar en que formato queremos que nos aparezca la fecha ya sea YY-MM-DD, YY/MM/DD, YY.MM.DD, MM-DD-YY, MM/DD/YY, MM.DD.YY, DD-MM-YY,DD/MM/YY, DD.MM.YY o YYYYMMDD
- **Teclas Beep.-** Activar o desactivar el sonido al aplastar cada tecla
- **Voz.-** Activar o desactivar las indicaciones por voz.
- **Ajuste de volumen.-** Ajustar el volumen de los sonidos.
- **Versión de algoritmo.-** Es la versión del algoritmo con la que el dispositivo reconoce las huellas, password o tarjeta de proximidad
- **Tiempo mínimo.-** Es el tiempo en la que el usuario no puede a volver a hacer un registro.

Modelo 1 **Modelo 2**

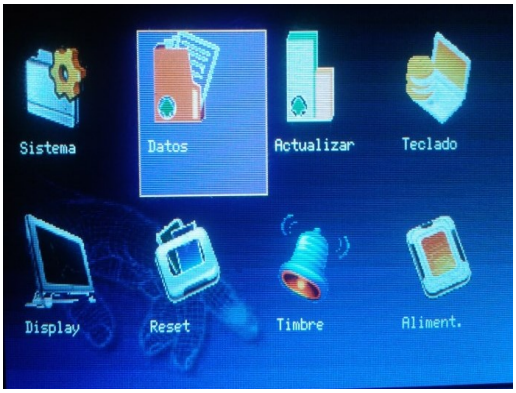
Figura 6.79. Opción del sistema

Fuente: Investigador

Nota: Para grabar los cambios realizados aplastamos la tecla Ok y siempre que hagamos cambios en los parámetros, es necesario apagar y encender el reloj nuevamente.

3.2. DATOS

Para tener acceso a la opción de Datos primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Datos como nos indica las siguiente figura.



Modelo 1 **Modelo 2**

Figura 6.80. Opción datos

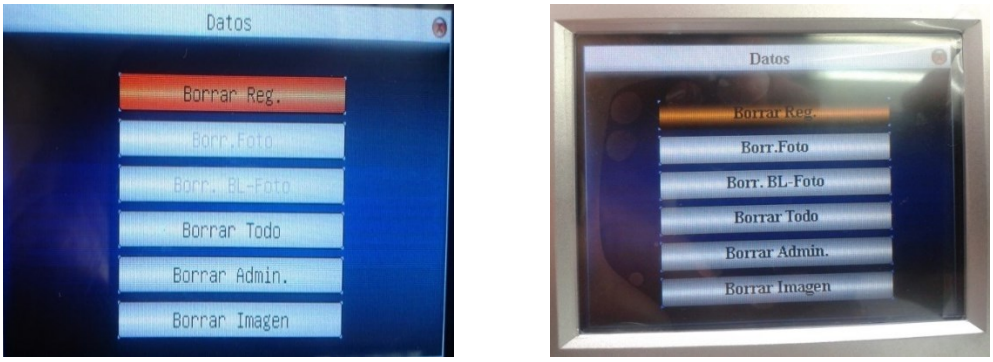
Fuente: Investigador

- **Borrar Registros.-** Borra todos los registros o marcaciones almacenados en el sistema biométrico.

- **Borrar Todos.-** Borra todos los usuarios registrados en el sistema biométrico.

- **Borrar Administrador.-** Borra todos los privilegios de administrador de los usuarios que poseen.

- **Borrar Imagen.-** Borra las imágenes que aparecen en la pantalla principal del reloj biométrico.



Modelo 1 **Modelo 2**

Figura 6.81. Tipo de borrados de la información

Fuente: Investigador

3.3. ACTUALIZACIÓN

Para tener acceso a la opción de Teclado primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Teclado como nos indica las siguiente figura.

Modelo 1 **Modelo 2**

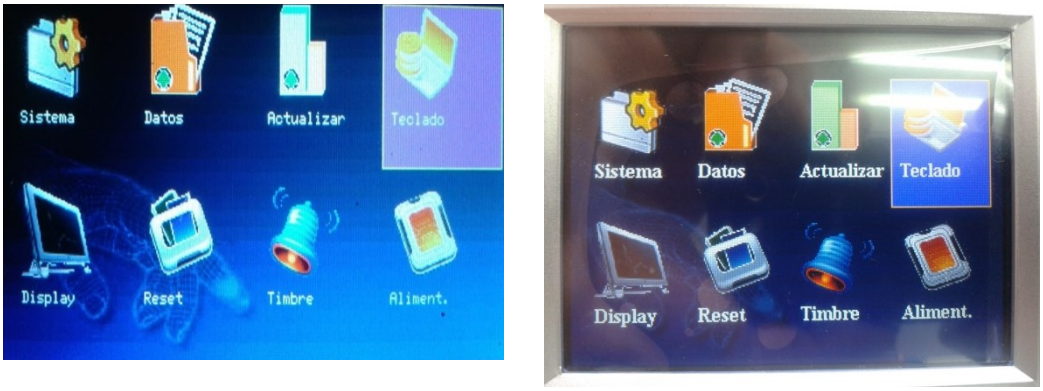
Figura 6.82. Opción de actualización

Fuente: Investigador

En esta sección nos permite hacer la actualización del firmware del sistema biométrico mediante un flash memory, uso exclusivo para personal técnico.

3.4. TECLADO

Para tener acceso a la opción de Teclado primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Teclado como nos indica las siguiente figura.

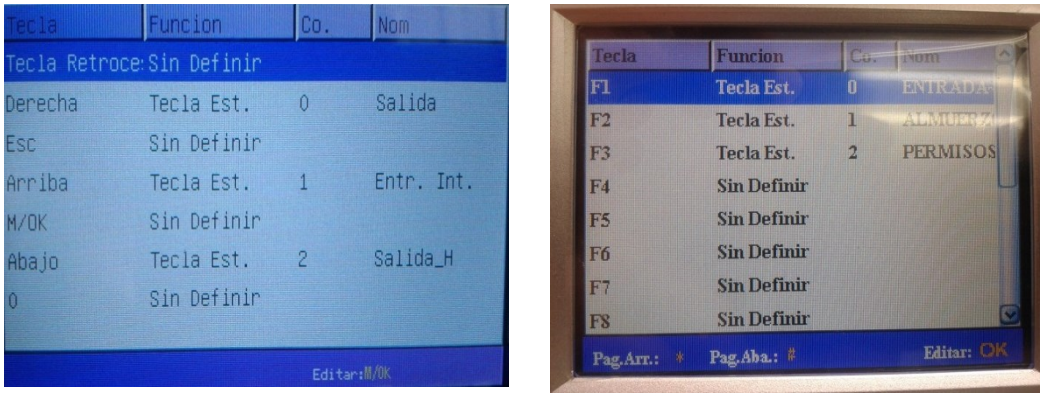


Modelo 1 **Modelo 2**

Figura 6.83. Opción de teclado

Fuente: Investigador

Dentro de esta pantalla podemos configurar las teclas de función cuando son presionadas fuera del menú.



Modelo 1 **Modelo 2**

Figura 6.84. Opciones de las teclas de función

Fuente: Investigador

3.5. DISPLAY

Para tener acceso a la opción de Teclado primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Teclado como nos indica las siguiente figura.

Modelo 1 **Modelo 2**

Figura 6.85. Opción del displey

Fuente: Investigador

- Sección donde nos permite determinar el número de intentos en lo que respecta a marcación con huella o mediante contraseña.

- Nos permite escoger un modelo de reloj entre dos opciones la misma que se muestra en la pantalla principal.

- Nos permite configurar el retardo de la imagen que se muestra en la pantalla principal del sistema biométrico.

Modelo 1 **Modelo 2**

Figura 6.86. Opciones de la configuración del displey

Fuente: Investigador

3.6. RESET

Para tener acceso a esta opción ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Reset como nos indica las siguiente figura.

Modelo 1 **Modelo 2**

Figura 6.87. Opción de reseteo

Fuente: Investigador

Con esta opción nos permite resetear todo la configuración a modo de fábrica, resetear la configuración del teclado, resetear los toques de sirena.

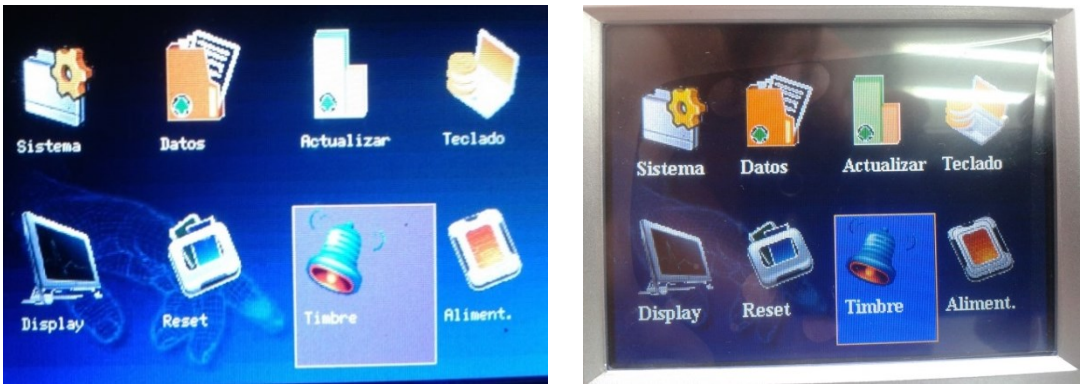
Modelo 1 **Modelo 2**

Figura 6.88. Tipo de reseteos

Fuente: Investigador

3.7. TIMBRE

Para tener acceso a esta opción primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Timbre como nos indica las siguiente figura.

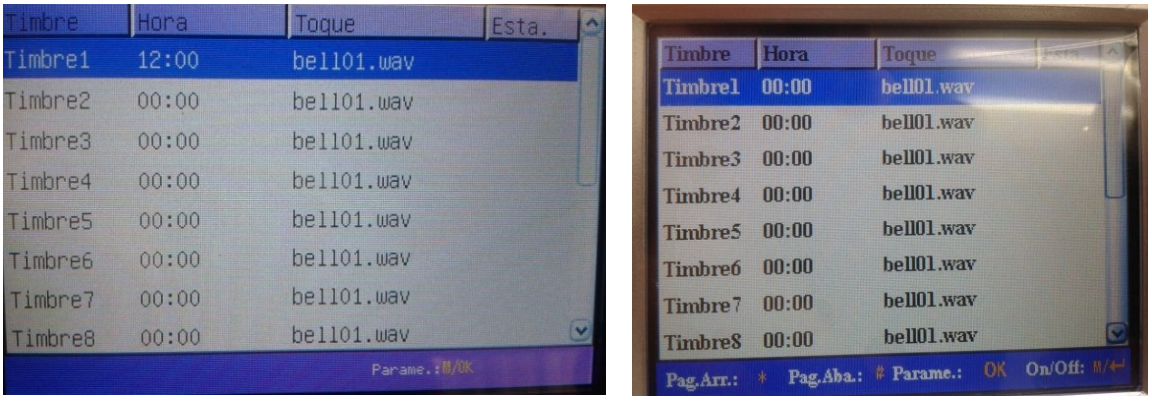


Modelo 1 **Modelo 2**

Figura 6.89. Opción de timbres

Fuente: Investigador

En esta sección nos permitirá programar una alarma, tono, volumen y número de veces que sonará.



Modelo 1 **Modelo 2**

Figura 6.90. Configuración de timbres

Fuente: Investigador

3.8. ALIMENTACIÓN

Para tener acceso a esta opción primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos la Sistema y Alimentación como nos indica las siguiente figura.

Modelo 1 **Modelo 2**

Figura 6.91. Opción de alimentación

Fuente: Investigador

- En esta sección nos permite determinar el tiempo de duración que el equipo se ponga en modo de reposo.

- Determinar si se presenta la imagen de huella, ver el nivel, ver huella y el nivel, o no ver nada.

- Activar o desactivar la tecla del apagado.

- Cambiar el idioma del dispositivo entre inglés y español.

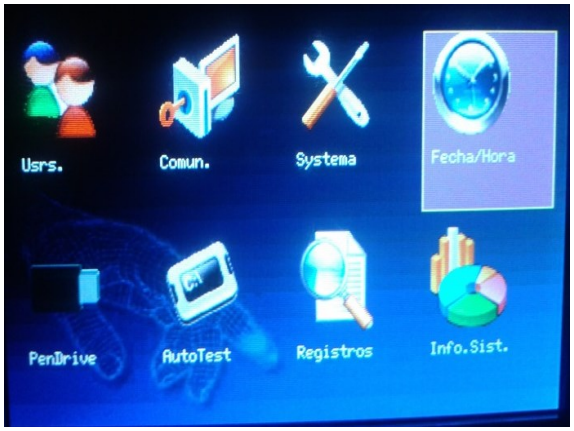
Modelo 1 **Modelo 2**

Figura 6.92. Configuracion de la alimentación

Fuente: Investigador

4. FECHA Y HORA

Para tener acceso a esta opción, ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos a Fecha/Hora como nos indica las siguiente figura.



Modelo 1 **Modelo 2**

Figura 6.93. Opción de fecha y hora

Fuente: Investigador

Al acceder a esta opción, se tendrá la posibilidad de configurar la fecha, hora; Con esta función se podrá configurar la hora y fecha. Cabe anotar que el formato de la fecha puede ser configurado, pero el formato de la hora está establecido por defecto de fábrica a 24H. Las modificaciones se harán a través del teclado y utilizando las teclas de desplazamiento.

Modelo 1 **Modelo 2**

Figura 6.94. Configuración de la fecha y hora

Fuente: Investigador

5. PENDRIVE

Para tener acceso a la opción de Pendrive primero ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos a Pendrive como nos indica las siguiente figura.

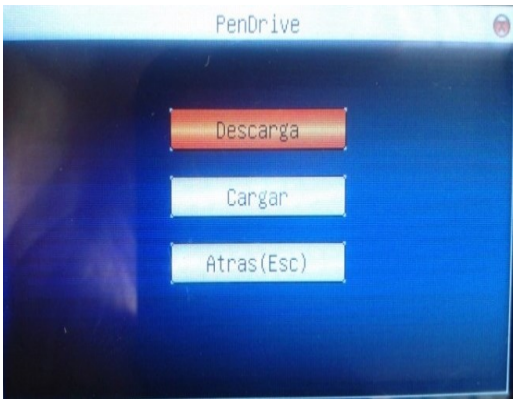
Modelo 1 **Modelo 2**

Figura 6.95. Opción de pendrive

Fuente: Investigador

Descargar.- Esta opción nos permite descargar todos los registros y todos los usuarios registrados.

Cargar.- Con esta opción nos permite subir los usuarios y cargar imágenes con el siguiente formato ad_#.jpg



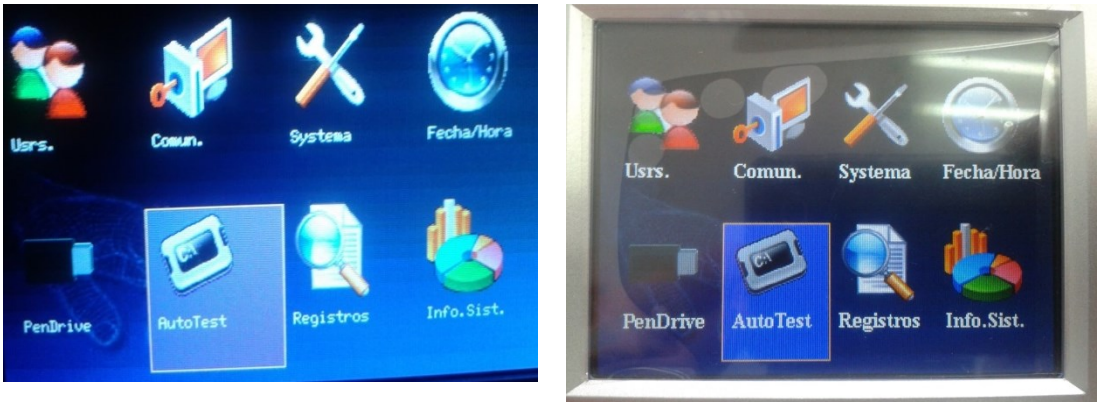
Modelo 1 **Modelo 2**

Figura 6.96. Opciones de pendrive

Fuente: Investigador

6. AUTOTEST

Para tener acceso a esta opción ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos a Autotest como nos indica las siguiente figura.



Modelo 1 **Modelo 2**

Figura 6.97. Opción de autotest

Fuente: Investigador

Esta opción permite ejecutarle diferentes tipos de pruebas al dispositivo, de tal forma que cuando esté operando mal, sea más fácil y rápido la detección de la falla. Dentro de los diferentes test con que cuenta el sistema encontramos:

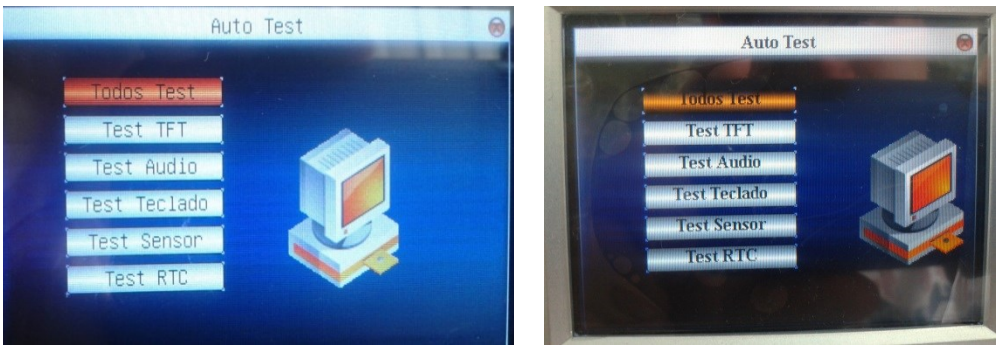
- **Test Todo.** Este realiza la revisión de todo el sistema, es decir, agrupa todo lo test de chequeo en uno solo. Para ejecutarlo basta con ubicar el cursor frente a esta opción y presionar la tecla OK.

- **Test TFT.-** Prueba el funcionamiento del LCD. En pantalla aparecerá una gama de colores.

- **Test Audio.** Confirma que cada una de las indicaciones por voz esté funcionando de manera correcta.

- **Test Teclado.-** Comprueba la correcta operación de cada tecla. Presione una a una las teclas y en pantalla deberá aparecer que tecla está presionando.

- **Test Sensor.-** Chequea el funcionamiento del sensor óptico o prisma.
- **Test RTC.-** Realiza el respectivo chequeo del reloj.



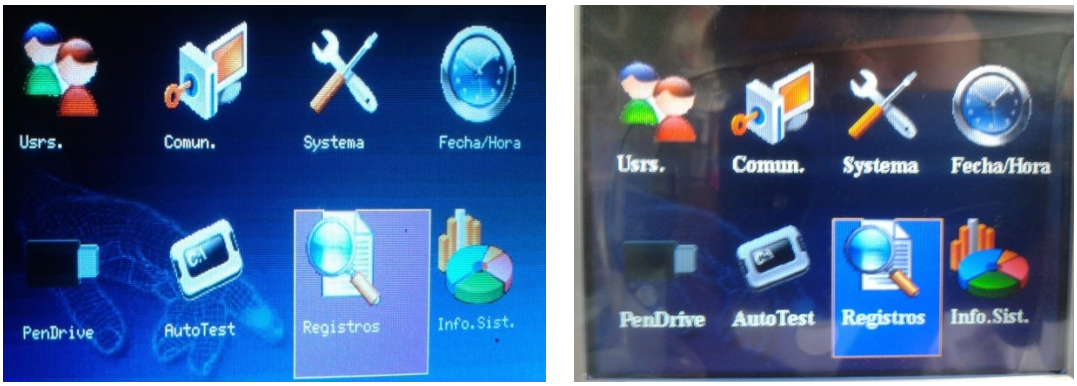
Modelo 1 **Modelo 2**

Figura 6.98. Tipos de autotest

Fuente: Investigador

7. REGISTROS

Para tener acceso a esta opción ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos a Autotest como nos indica las siguiente figura.



Modelo 1 **Modelo 2**

Figura 6.99. Opción de registros

Fuente: Investigador

Cuando ingresamos en esta pantalla ingresamos el código de un usuario registrado, determinamos las fechas de consulta y aplastamos OK la cual nos mostrará el listado de los registros realizados.

8. INFORMACIÓN DEL SISTEMA BIOMÉTRICO

Para tener acceso a esta opción ingresamos al menú principal con la tecla **M/Ok,** posteriormente asignamos a información del sistema como nos indica las siguiente figura.

Modelo 1 **Modelo 2**

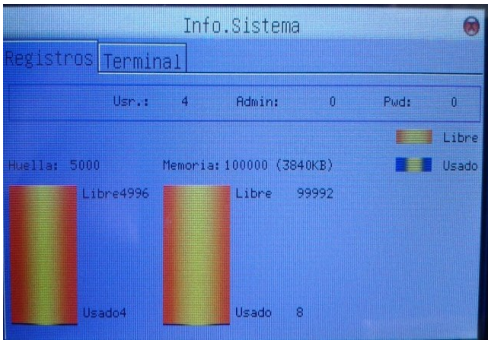
Figura 6.100. Opción de información del sistema

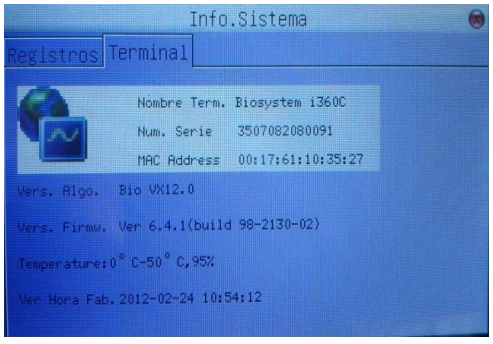
Fuente: Investigador

- En una pestaña de esta sección nos muestra un resumen de los usuarios registrados, administradores, además de una gráfica de la capacidad de la memoria.

- En la otra pestaña no muestra la información complementaria del sistema biométrico.

Modelo 1





Modelo 2

Figura 6.101. Información del sistema

Fuente: Investigador

SOFTWARE DE CONTROL

En esta parte del manual explicaremos cómo normalizar los parámetros necesarios para que el sistema entregue los resultados de acceso, esto quiere decir que existen unos parámetros mínimos para que el sistema funcione como Software de acceso, es bueno destacar que los accesos directos del software corresponden al ícono en el escritorio como se ve a continuación:

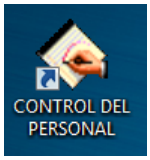


Figura 6.**102** Icono del software biométrico

Fuente: Investigador

DESCRIPCIÓN DEL SOFTWARE DE CONTROL

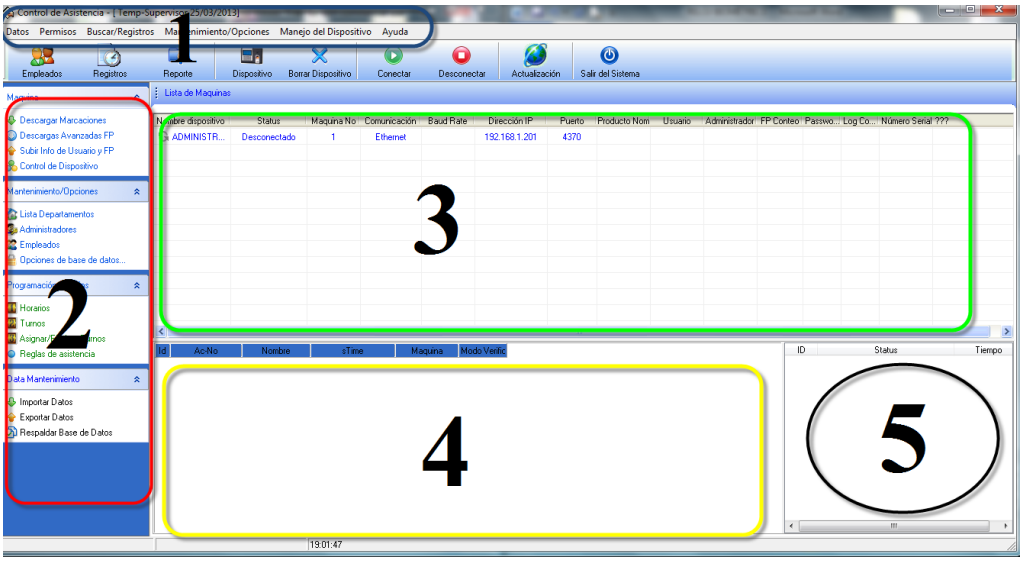


Figura 6.103. Pantalla del software biométrico

Fuente: Investigador

El software de sistema biométrico se divide en 5 partes la cuales son:

1. Barra de menú
2. Barra de accesos directos
3. Lista de dispositivos
4. Listado de un reporte de marcaciones
5. Ventana de sucesos del dispositivo biométrico

CONCEPTOS BÁSICOS

1. INGRESO AL SISTEMA DE ATTENDACE MANAGER O CONTROL DE ASISTENCIA

Para ingresar al sistema del reloj biométrico tenemos que dar clic en inicio – Todos los Programas – Control del Personal y Attendance Management

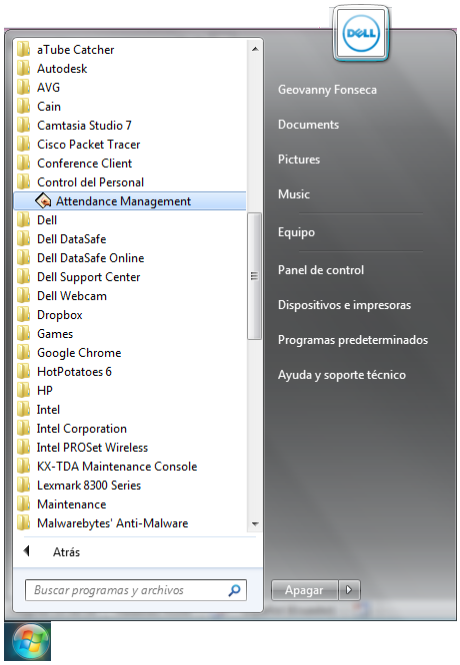


Figura 6.104. Ingreso al sistema ATTENDANCE MANAGEMENT

Fuente: Investigador

2. CONFiguraCIÓN DE LA BASE DE DATOS

Para ingresar a la ventana de configuración de la base de datos ingresamos al software y damos en **Mantenimiento/Opciones** y posteriormente damos clic en **Opción De La Base De Datos** nos muestra la siguiente figura.

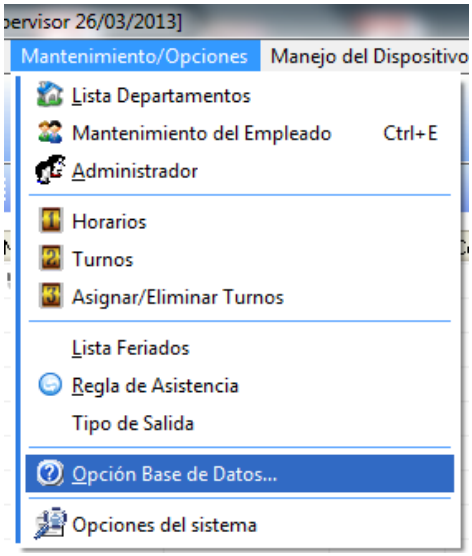


Figura 6.105. Opción de la base de datos

Fuente: Investigador

En la siguiente ventana de propiedades de vínculo de datos lo primero que tenemos que hacer es digitar o buscar la ruta de la base de datos y comprobar la conexión.

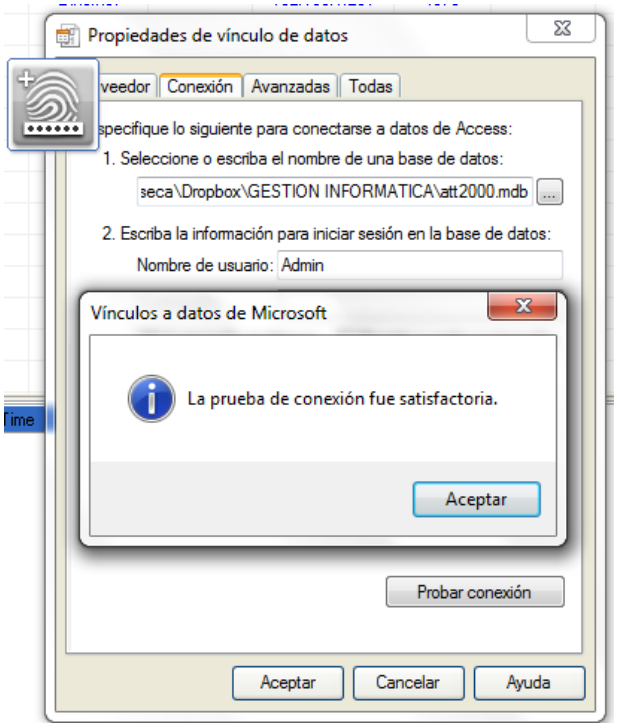


Figura 6.106. Configuración de la base de datos

Fuente: Investigador

Nota: Una vez que se ha comprobado la conexión con la base de datos debemos cerrar y abrir nuevamente el sistema de control del personal.

3. CONFiguraCIÓN DE DISPOSITIVOS BIOMÉTRICOS

Para ingresar a la ventana de configuración de dispositivos biométricos ingresamos al software y damos en **Dispositivos** como nos muestra la siguiente figura.

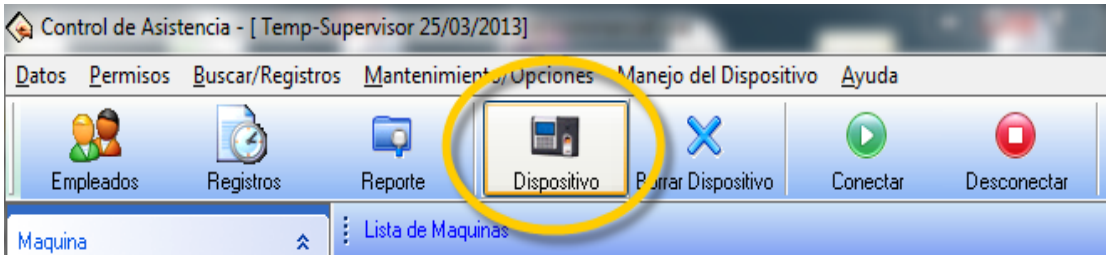


Figura 6.107. Dispositivos

Fuente: Investigador

Una vez ingresado a la ventana de administración de dispositivos aquí podemos agregar, modificar y eliminar los dispositivos existentes.

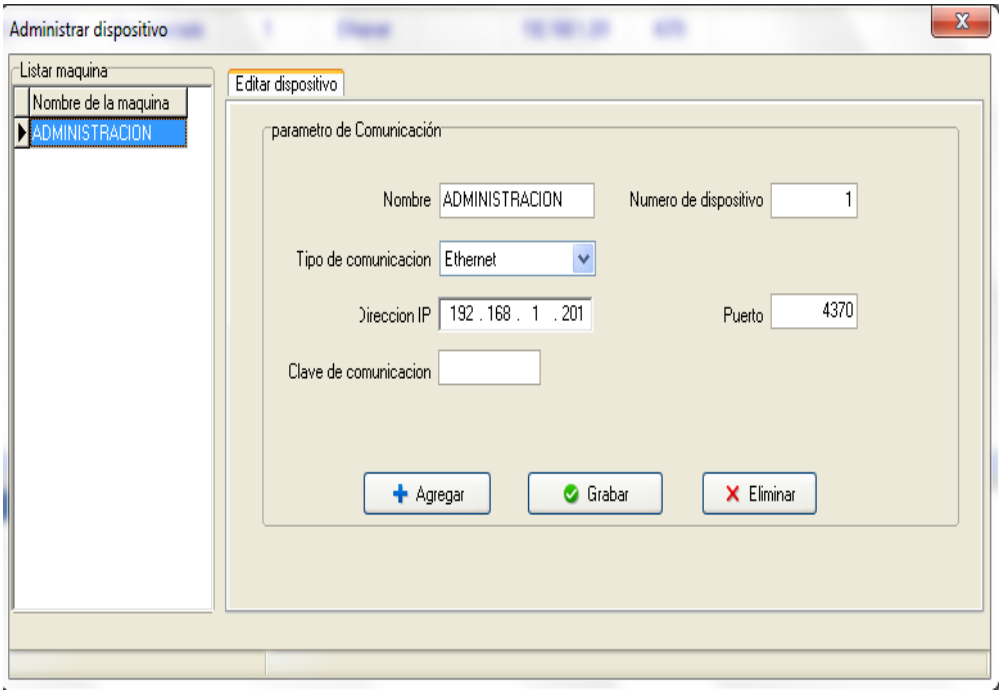


Figura 6.108. Administración de dispositivos

Fuente: Investigador

En esta Ventana se le indicará al sistema que el Reloj que está agregando posee una Comunicación Ethernet, se le debe asignar la IP y el puerto de comunicación que siempre y para todos los equipos es 4370 la cual no debe ser cambiada al final se le coloca un nombre.

4. MANEJO DE EMPLEADOS

Para ingresar a la ventana de manejo de la información de empleados ingresamos al software y damos en la barra de menú en la opción de **Mantenimiento/Opciones** y posteriormente damos clic en **Mantenimiento del empleado** como nos muestra la siguiente figura.

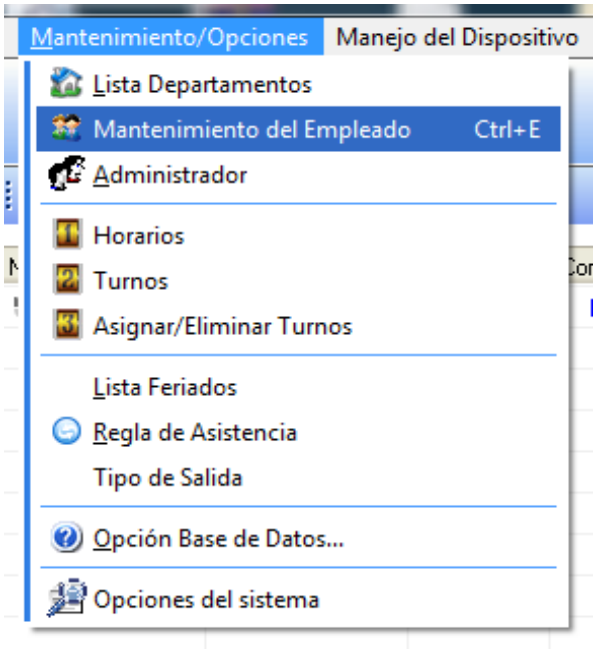


Figura 6.109. Mantenimiento de empleados

Fuente: Investigador

Una vez ingresado a la ventana de Empleados se puede crear y eliminar usuarios, registrado en el reloj biométrico, asignar un usuario a un departamento o sub-departamentos según sean los requerimientos. La información de cada empleado se ingresa llenando los campos que se encuentran en la parte inferior de la siguiente figura.

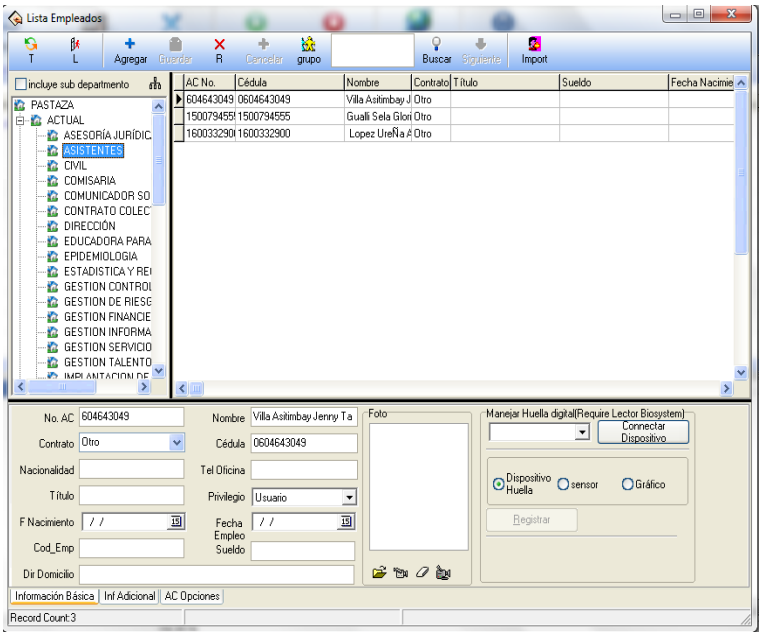


Figura 6.110. Ventana de empleados

Fuente: Investigador

NOTA: El campo No. AC debe ser igual que el número de identificación con la que se registró en el reloj biométrico.

Funcionamiento de los botones de la ventana

Agregar un nuevo usuario o empleado

Eliminar un usuario o empleado.

Asignar un empleado a un departamento o sub-departamento.

Despedir temporalmente a un usuario o empleado

Buscar a un empleado de todo el listado general

5. CREACIÓN DE DEPARTAMENTOS

Para ingresar a la ventana de creación de departamentos ingresamos al software y damos en la barra de menú en la opción de **Mantenimiento/Opciones** y posteriormente damos clic en **Lista Departamentos** como nos muestra la siguiente figura.

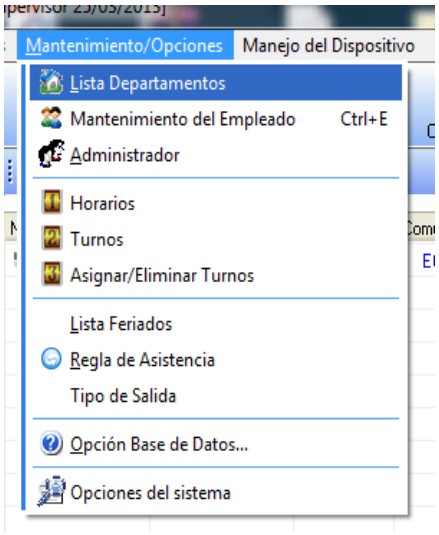


Figura 6.111. Creación de departamentos

Fuente: Investigador

Una vez ingresado a la ventana de departamentos se puede crear varios departamentos y sub-departamentos según sean los requerimientos de la organización u empresa y así poder clasificar a los empleados por departamentos o por áreas de trabajo según correspondan.

- Para agregar un nuevo sub-departamento damos clic en **agregar** y digitamos el nombre del mismo.
- Para eliminar un sub-departamento no correspondiente seleccionamos y damos clic en **Borrar**.

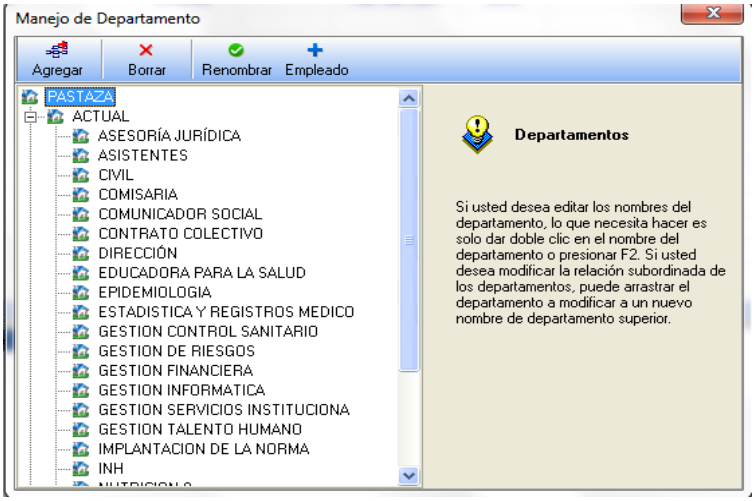


Figura 6.112. Manejo de departamentos

Fuente: Investigador

6. CREACIÓN DE HORARIOS

Para ingresar a la ventana de creación de Horarios ingresamos al software y damos en la barra de menú en la opción de **Mantenimiento/Opciones** y posteriormente damos clic en **Horarios** como nos muestra la siguiente figura la misma que corresponde al periodo de tiempo entre el registro de ingreso y registro de salida.

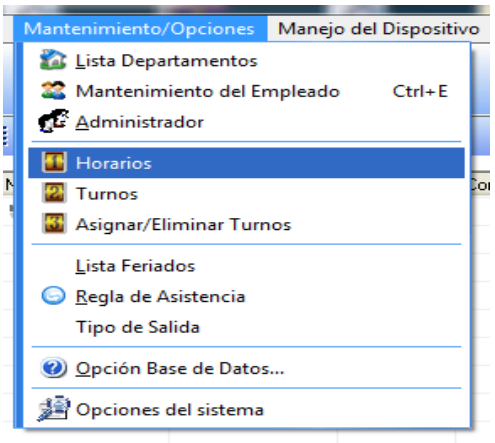


Figura 6.113. Horarios

Fuente: Investigador

Una vez ingresado a la ventana de Horarios se puede crear varios horarios según sean los requerimientos de la organización u empresa.

- Para agregar un nuevo Horario en el botón **Agregar** e ingresamos la información mostrada en la parte derecha de la siguiente imagen.
- Para eliminar seleccionamos el Horario no deseado y damos clic en **Borrar**.

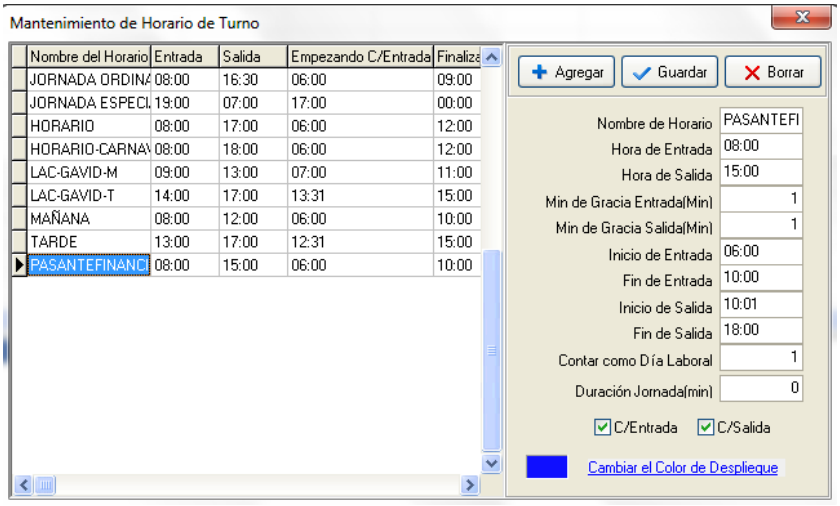


Figura 6.114: ADMINISTRACIÓN DE HORARIOS

Fuente: Investigador

En la pantalla de Horarios cada campo representa lo siguiente:

- **Nombre de Horario:** Es el nombre que se asigna al horario.

- **Hora de Entrada:** Es la hora en la que debe iniciar la jornada de trabajo.

- **Hora de Salida:** Es la hora en la que debe finalizar la jornada de trabajo.

- **Min de Gracia Entrada (Min):** Es el tiempo (en minutos) transcurrido a partir de la hora de entrada que tiene el empleado para llegar tarde sin que se registre como atraso.

- **Min de Gracia Salida (Min):** Es el tiempo (en minutos) antes de la hora de salida que tiene el empleado para salir sin que se registre como salida temprano.

- **Inicio de Entrada y Fin de Entrada:** Es el intervalo de tiempo en donde el empleado puede marcar para que sea reconocida la **Hora de Entrada**.

- **Inicio de Salida y Fin de Salida:** Es el intervalo de tiempo en donde el empleado puede marcar para que sea reconocida la **Hora de Salida.**

- **Contar como Día Laboral:** En este campo nosotros asignamos como queremos que sea el Horario si:

    - El horario es una sola jornada se asigna el valor número 1

    - El horario es media jornada se asigna el valor número 0,5.

7. CREACIÓN DE TURNOS

Para ingresar a la ventana de creación de turnos ingresamos al software y damos en la barra de menú en la opción de **Mantenimiento/Opciones** y posteriormente damos clic en **Turnos** como nos muestra la siguiente figura la misma que corresponde al de que día a que día se le asigna un horario.

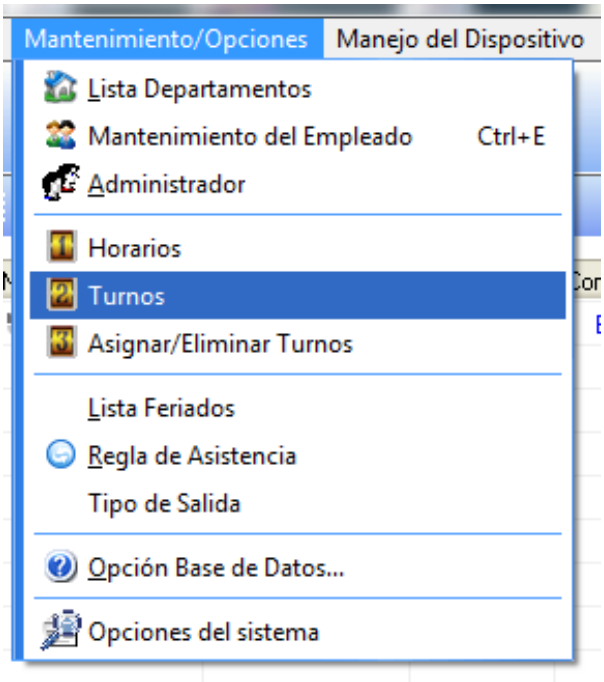


Figura 6.115. Turnos

Fuente: Investigador

Una vez en la ventana de manejo de turno damos click en Añadir para crear un nuevo turno y le asignamos un nombre, en la columna fecha de inicio ingresamos la fecha desde la cual va a estar en vigencia este turno, luego damos click en Añadir hora para asignar un horario a este turno y nos aparece la siguiente ventana En la cual seleccionamos el o los horarios dependiendo el número de jornadas que tenga en el día y en el cuadro de la derecha seleccionamos los días laborables.

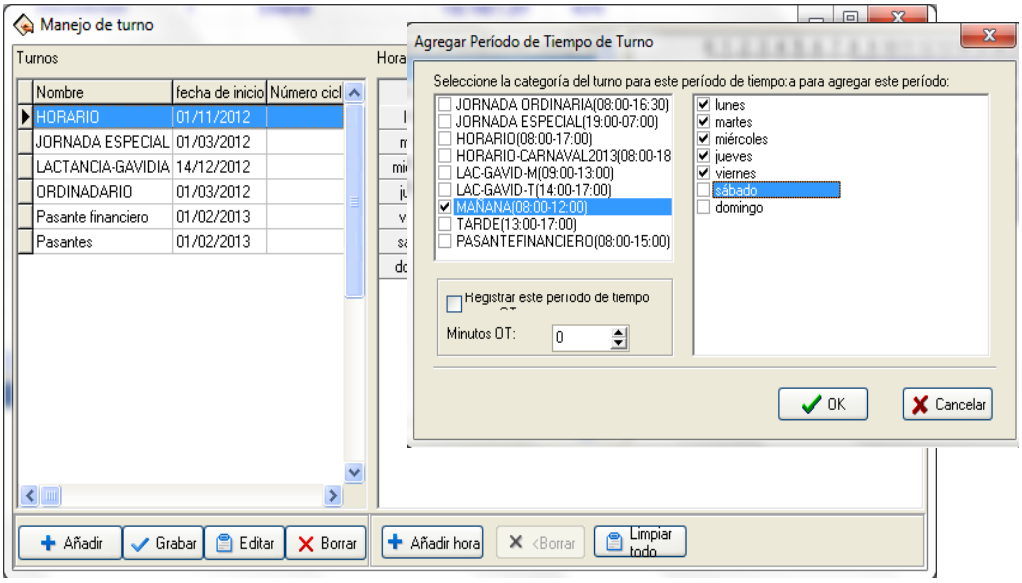


Figura 6.116. CREACIÓN DE TURNOS

Fuente: Investigador

8. ASIGNACIÓN DE TURNO U HORARIOS

Para ingresar a la ventana de asignaciones de turnos ingresamos al software y damos en la barra de menú en la opción de **Mantenimiento/Opciones** y posteriormente damos clic en **Asignar/Eliminar Turnos** como nos muestra la siguiente figura la misma que corresponde un empleado en que turno va a timbrar dependiendo al horario de trabajo.

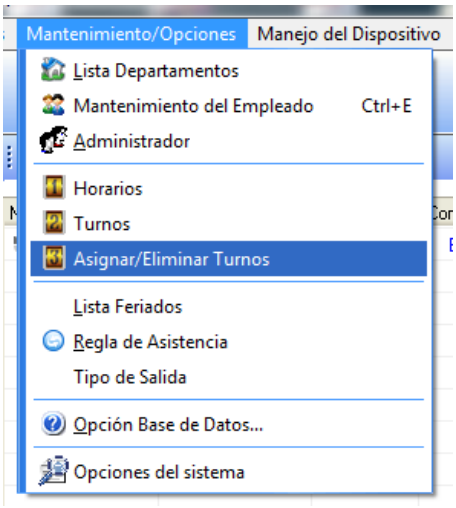


Figura 6.117: Turnos

Fuente: Investigador

Para asignar un turno seleccionamos al o los empleados y damos click en Asignar Turnos, y obtenemos la siguiente ventana.

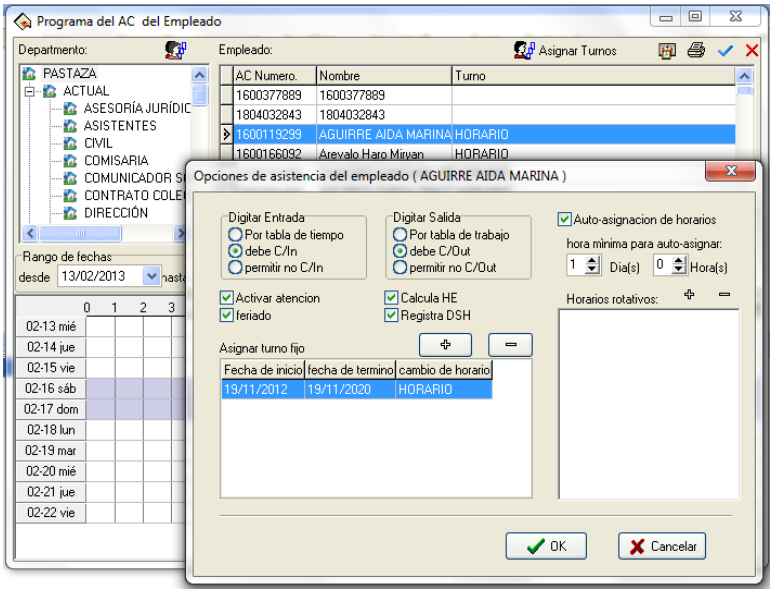


Figura 6.118. Asignación de turnos

Fuente: Investigador

En el cuadro de la izquierda ingresamos los turnos fijos y en el cuadro de la izquierda para los turnos rotativos.

- Para agregar un turno damos click en el signo +
- Seleccionamos el turno que pertenece a este empleado o usuario.
- En la parte inferior el Rango del horario desde cuando hasta cuándo va a estar en vigencia este turno.

9. REPORTES

Para ingresar a la ventana de Reportes ingresamos al software y damos en la barra de menú en la opción de **Datos** y posteriormente damos clic en **OverTime** como nos muestra la siguiente figura.

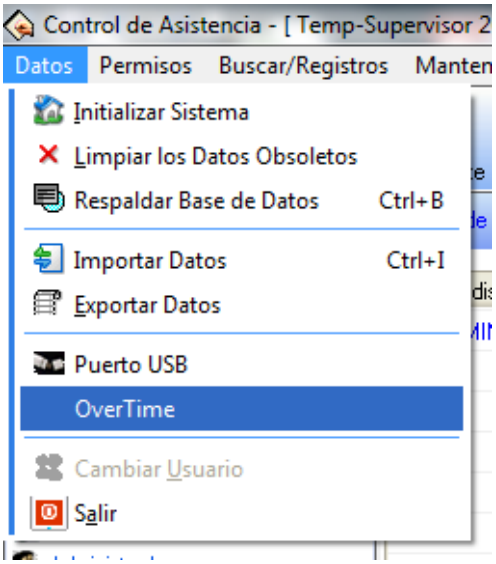


Figura 6.119. Menú Overtime para acceder a sacar reportes

Fuente: Investigador

En la siguiente ventana podemos sacar 5 tipos de reportes los mismos que son necesarios para el control de asistencia de un empleado como son: Reporte de marcaciones, Reporte de asistencia diaria, Reportes de permisos, Reportes de resúmenes generales, Reportes gráficos.

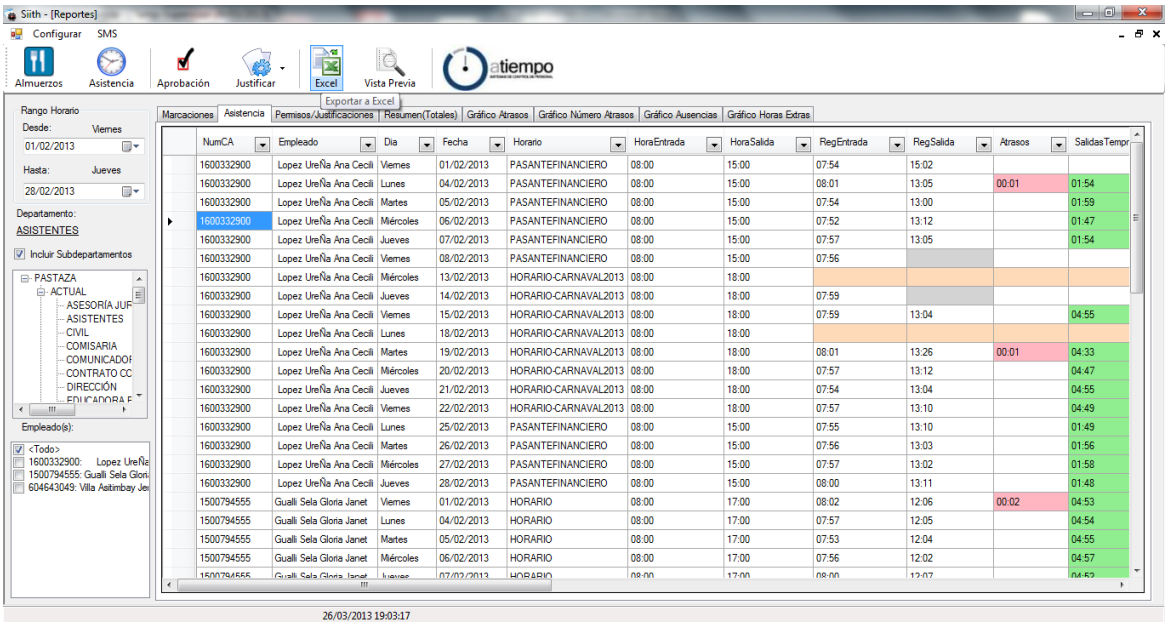


Figura 6.120. Reportes generado

Fuente: Investigador

10. Respaldos

Para sacar respaldados del sistema de control del personal debemos ingresar al software y damos clic en la barra de menú en la opción de **Datos** y posteriormente damos clic en **Respaldo Base de Datos** como nos muestra la siguiente figura y guardar en un lugar seguro.

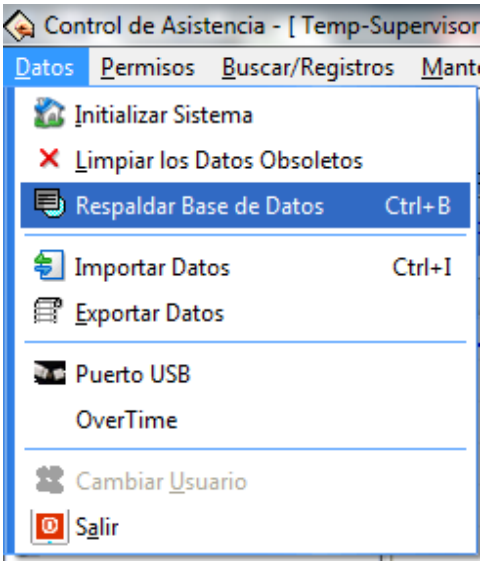


Figura 6.121. Respaldo

Fuente: Investigador

6.7.4.1. Conexiones Ethernet

Inicialmente configuramos la dirección IP del reloj, ingresando por Menú, Comunicaciones, Red he e ingresando la IP, modifique la dirección IP asegurándose de que sea una IP válida y esté disponible en la red.

Formas de conectar en una red

- Podemos conectar el reloj biométrico a través de un SWITCH o HUP a la computadora.

Figura 6.122. Conexión mediante un switch o hup

- Podemos conectar el reloj biométrico directamente a la computadora.

Figura 6.123. Conexión directa

Nota: Cuando conecte el reloj directamente a la tarjeta de red del computador por favor use un cable cruzado (Apéndice B), si por el contrario conecta a un Hub/Switch hágalo por medio de un patch cord.

Estos equipos biométricos vienen con su respectivo software de control de personal, el mismo que permite la creación de horarios, permisos, manejo de información de empleados, reportes.

6.7.4.2. Forma correcta de colocar la huella dactilar en el lector óptico

Ubique el dedo de manera firme y centrada sobre la superficie del lector óptico, sin girarlo hasta que reciba la indicación de que su huella ha sido leída correctamente mediante luz y mediante voz.

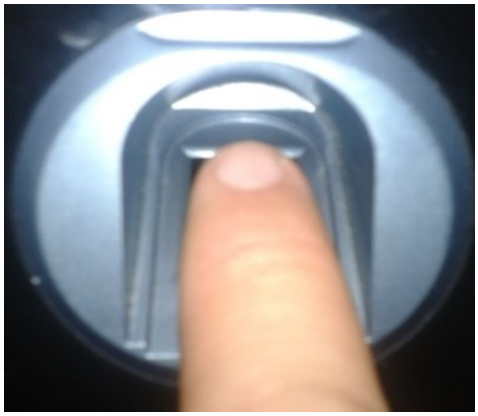


Figura 6.124. Forma correcta de marcar
Fuente: Investigador

No debe colocar el dedo de costado, inclinado, girado o de punta la huella dactilar. Como muestra la siguiente figura.

Figura 6.125. Forma incorrecta de marcar

Fuente: Investigador

6.7.4.3. PROCEDIMIENTOS DE UTILIZACIÓN DEL RELOJ BIOMÉTRICO Y DEL SOFTWARE

FORMATO DE PRESENTACIÓN DE LOS PROCEDIMIENTOS

Nombre del procedimiento

Cada procedimiento estará identificado con un nombre, el cual nos permite identificarlos con facilidad en el manual.

a) Objetivo

Define el propósito que tiene el procedimiento

b) intervienen

Son todas aquellas personas que se relacionan directamente con la ejecución del procedimiento descrito.

c) Descripción del procedimiento

Es la descripción detallada del procedimiento, que se presenta por partes. Dicha descripción se organiza de la siguiente manera: un encabezado del procedimiento, el cuadro o cuerpo del procedimiento conformado por tres columnas a saber: paso, descripción y responsable. A continuación se detallan estas partes:

Manual de procedimientos:	
Elaborado:	
Aprobado:	

PASO	**DESCRIPCIÓN**	**RESPONSABLE**

d) Diagrama

Se diagrama el proceso

e) Materiales

Se describe los materiales a utilizarse

PROCEDIMIENTOS

PROCEDIMIENTO # 1: VERIFICACIÓN DEL DISPOSITIVO BIOMÉTRICO

a) Objetivo

Describir los requisitos básicos para la Verificación del dispositivo biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Representantes de la empresa que adquiere el reloj biométrico.

c) Descripción del procedimiento

Manual de procedimientos:	Verificación del dispositivo biométrico
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

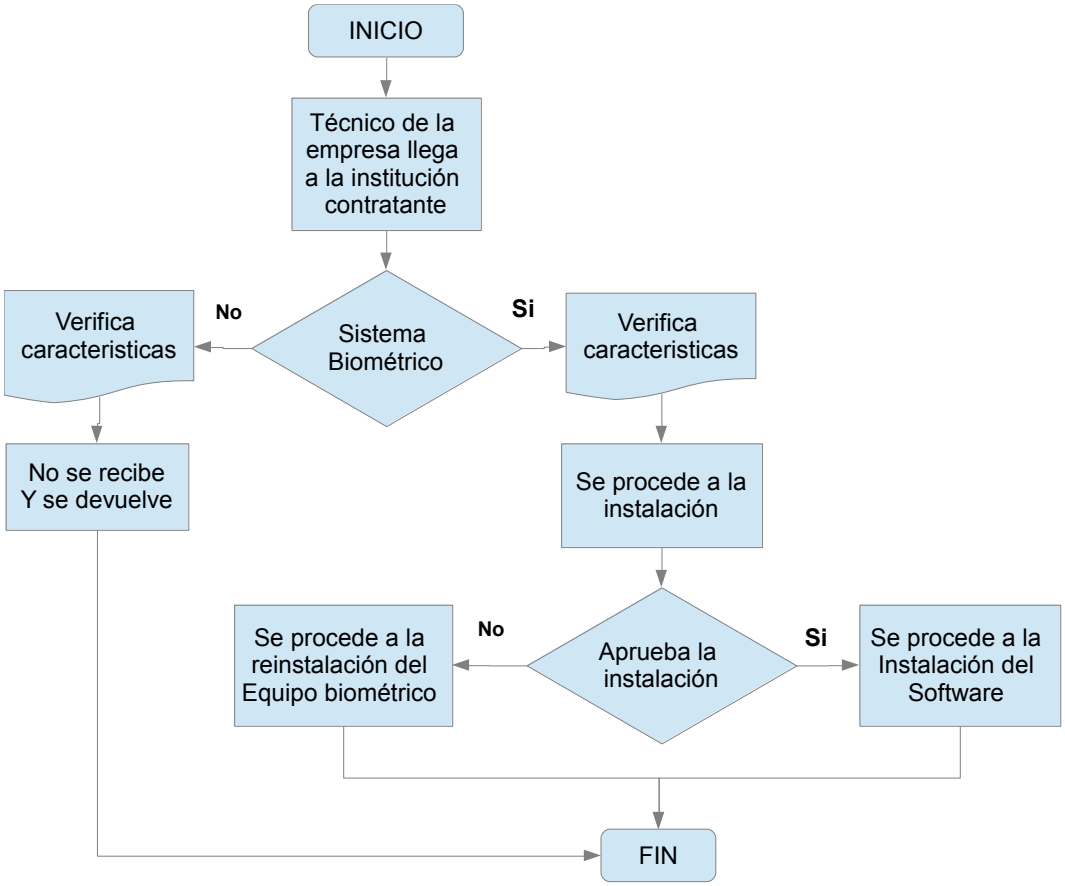
PASO	DESCRIPCIÓN	RESPONSABLE
1	Tener el equipamiento de instalación	Servicio técnico
2	Trasladarse al lugar de instalación del equipo biométrico	Servicio técnico
3	Comprobar y revisar características del Equipo Biométrico **Si:** Pasa al siguiente paso **No:** Pasa al último paso	Servicio técnico, Representantes de la empresa que adquiere el Reloj Biométrico.

4	Proceder a la instalación (P#2)	Servicio técnico
5	Aprobación de la instalación **Si:** Pasa al siguiente paso **No:** Pasa al paso anterior	Representantes de la empresa que adquiere el Reloj Biométrico
6	Entrega recepción del dispositivo	Soporte técnico

Tabla 6.18. Procedimiento 1

Fuente: Investigador

d) Diagrama



e) Materiales

Por parte de la empresa que compra el dispositivo biométrico debe poseer la proforma para realizar la verificación del dispositivo biométrico.

PROCEDIMIENTO # 2: INSTALACIÓN DEL RELOJ BIOMÉTRICO

a) Objetivo

Describir los requisitos básicos para la Instalación del reloj biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.

c) Descripción del procedimiento

Manual de procedimientos:	Instalación del reloj biométrico
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

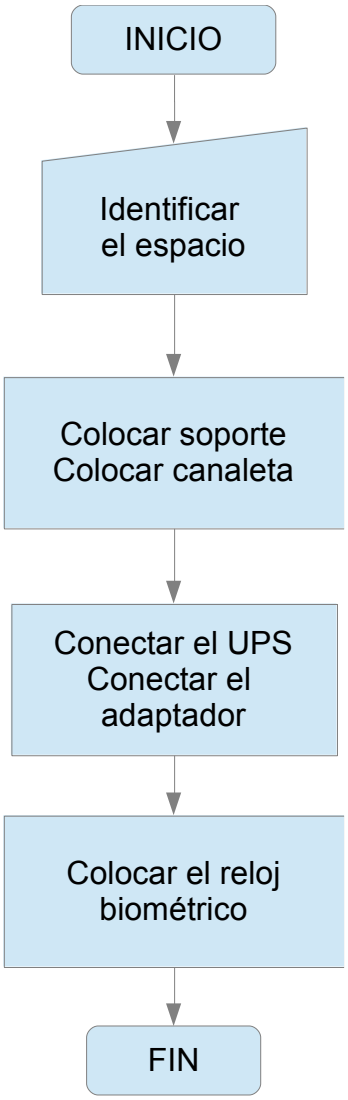
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Identificar el espacio en donde se va a instalar: - Toma de luz 120V, - Toma de punto de red RJ-45, - No este frente a la luz solar.	Servicio técnico
3	Colocar el soporte metálico del reloj biométrico a 1,20m. a nivel.	Servicio técnico
4	Colocar la canaleta desde el reloj hacia la toma eléctrica y punto de red.	Servicio técnico

5	Conectar el UPS, cable de red en el reloj biométrico.	Servicio técnico
6	Conectar el adaptador de luz en el UPS	Soporte técnico
7	Colocar el reloj biométrico en el soporte y ajustarlo con un tornillo.	Soporte técnico
8	Fin del proceso	

Tabla 6.19. Procedimiento 2

Fuente: Investigador

d) Diagrama



Materiales

Los materiales que se necesita para realizar en una instalación de un dispositivo biométrico se consideran:

- Taladro
- Metro
- Destornillador estrella pequeño
- Cinta doble faz
- Chaveta
- Canaleta
- Nivel
- Accesorios y el reloj biométrico

PROCEDIMIENTO # 3 INSTALACIÓN DEL SOFTWARE DE CONTROL

a) Objetivo

Describir los requisitos básicos para la Instalación del software de control.

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.

c) Descripción del procedimiento

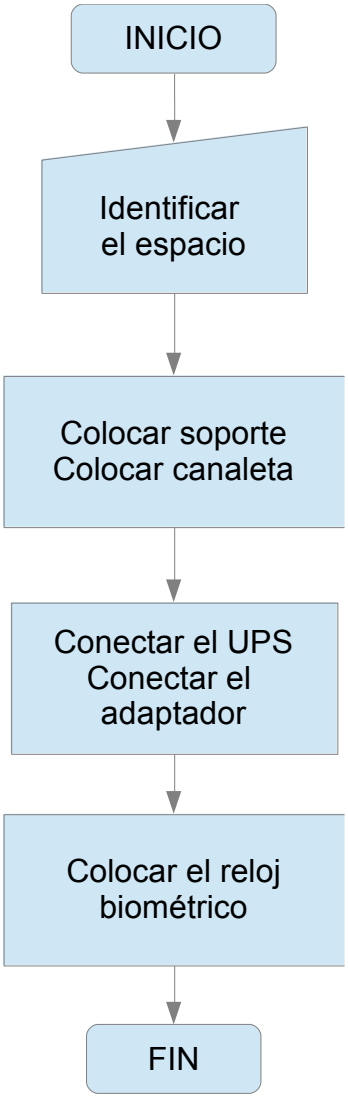
Manual de procedimientos:	Instalación del software de control
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Identificar la computadora en donde se va a instalar	Servicio técnico
3	Instalar el framework desde el cd	Servicio técnico
4	Instalar el cristal report desde el cd	Servicio técnico
5	Instalar el sistema ATTENDANCE MANAGEMENT desde el cd	Servicio técnico
6	Configurar la conexión de la base de datos en el ODBC	Soporte técnico
7	Fin del proceso	

Tabla 6.20. Procedimiento 3

Fuente: Investigador

d) Diagrama



e) Materiales

Cd de instalación del reloj biométrico

Computadora que esté conectado en la red

PROCEDIMIENTO # 4 CREACIÓN DE USUARIOS EN EL DISPOSITIVO BIOMÉTRICO

a) Objetivo

Describir los pasos básicos para crear la creación de usuarios en el dispositivo biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**CREACIÓN DE USUARIOS EN EL DISPOSITIVO BIOMÉTRICO**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

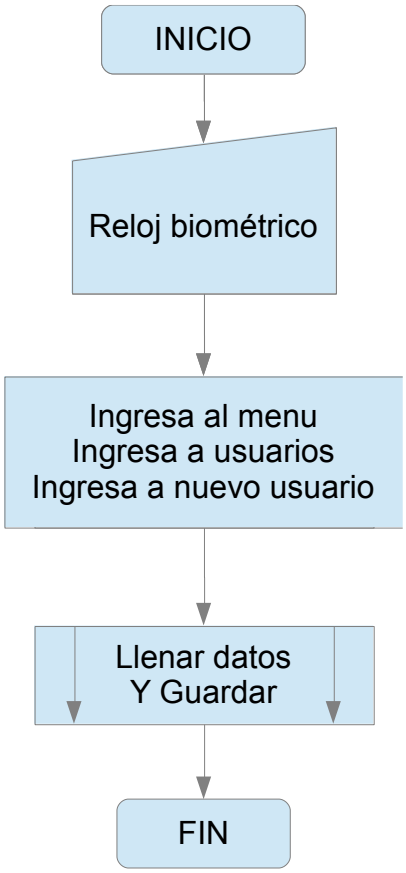
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Ingresar al menú con la tecla M/OK	Servicio técnico Administrador del reloj biométrico
3	Ingresar a la opción de usuario	Servicio técnico Administrador del reloj biométrico
4	Ingresar a Nuevo Usuario	Servicio técnico Administrador del reloj biométrico
5	Llenar los datos:	Servicio técnico

	• Número de identificación • Registrar la o las Huellas • Registrar la tarjeta de proximidad si lo poseen • Registrar una contraseña o password • Tipo de usuario o Usuario o Administrador o Super administrador • Modo de registro o Solo Huellas o Huellas y contraseña o Huellas y tarjeta de proximidad o Huellas, Contraseña y tarjeta de proximidad o Solo tarjeta o Solo Contraseña o password.	Administrador del reloj biométrico
6	Colocar Ok para guardar cambios	Soporte técnico Administrador del reloj biométrico
7	Salir con la tecla ESC	Servicio técnico Administrador del reloj biométrico
8	Comprobar el registro del usuario	Servicio técnico Administrador del reloj biométrico
9	Fin del proceso	

Tabla 6.21. Procedimiento 4

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

PROCEDIMIENTOS # 5 BORRADO DE UN USUARIO

a) Objetivo

Describir los pasos básicos para el Borrado de un usuario

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**BORRADO DE UN USUARIO**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

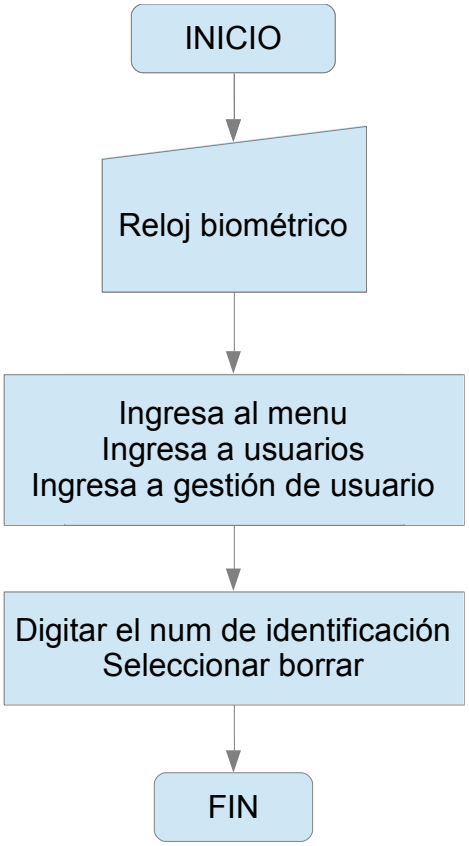
PASO	**DESCRIPCIÓN**	**RESPONSABLE**
1	Inicio del proceso	
2	Ingresar al menú con la tecla M/OK	Servicio técnico Administrador del reloj biométrico
3	Ingresar a la opción de usuario	Servicio técnico Administrador del reloj biométrico
4	Ingresar a Gestión de Usuario	Servicio técnico

		Administrador del reloj biométrico
5	Buscar el número de identificación a ser borrado	Servicio técnico Administrador del reloj biométrico
6	Aplastar M/OK para que se desplegué el sub menú	Servicio técnico Administrador del reloj biométrico
7	Seleccionar borrar usuario	Servicio técnico Administrador del reloj biométrico
8	Identificar y seleccionamos que opción necesitamos borrar: • **Password.-** Solo la contraseña • **Tarjeta de proximidad:** Solo la tarjeta • **Huellas:** Solo las huellas • **Usuario:** Todo las huellas, contraseña, y tarjeta de proximidad	Soporte técnico Administrador del reloj biométrico
9	Salir con la tecla ESC	Servicio técnico Administrador del reloj biométrico
10	Fin del proceso	

Tabla 6.22. Procedimiento 5

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

PROCEDIMIENTOS # 6 CONFIGURACIÓN DE LA IP

a) Objetivo

Describir los pasos básicos para la Configuración del direccionamiento IP

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**CONFIGURACIÓN DEL DIRECCIONAMIENTO IP**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

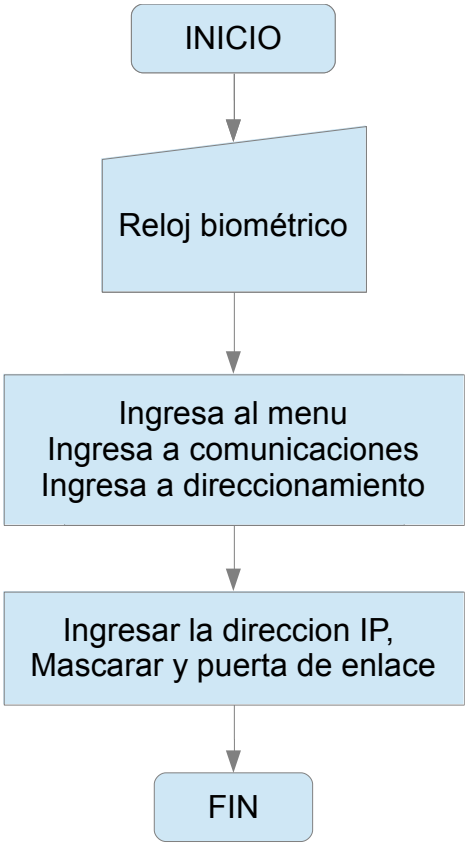
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Ingresar al menú con la tecla M/OK	Servicio técnico Administrador del reloj biométrico
3	Ingresar a la opción de comunicaciones	Servicio técnico Administrador del reloj biométrico
4	Ingresar a direccionamiento	Servicio técnico Administrador del reloj biométrico
5	Ingresar la dirección IP, mascara y puerta de enlace	Servicio técnico Administrador del reloj biométrico

6	Aplastar M/OK para guardar cambios	Servicio técnico Administrador del reloj biométrico
7	Salir con la tecla ESC	Servicio técnico Administrador del reloj biométrico
8	Fin del proceso	

Tabla 6.23. Procedimiento 6

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

PROCEDIMIENTOS # 7 BORRAR LOS REGISTROS DEL RELOJ BIOMÉTRICO

a) Objetivo

Describir los pasos básicos para el Borrado de los registros del reloj biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**BORRAR LOS REGISTROS DEL RELOJ BIOMÉTRICO**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

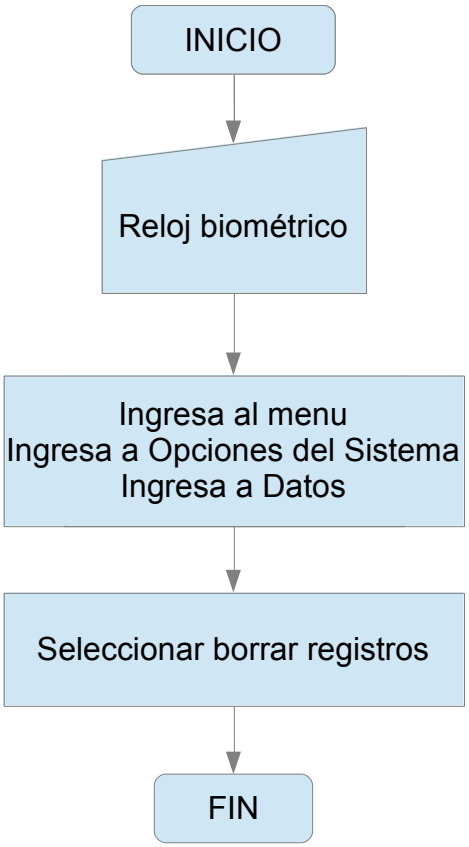
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Ingresar al menú con la tecla M/OK	Servicio técnico Administrador del reloj biométrico
3	Ingresar a la opción de Sistema	Servicio técnico Administrador del reloj biométrico
4	Ingresar a Datos	Servicio técnico Administrador del reloj biométrico
5	Seleccionar la opción de borrar registros	Servicio técnico

		Administrador del reloj biométrico
6	Aplastar M/OK para que surta efecto	Servicio técnico Administrador del reloj biométrico
7	Salir con la tecla ESC	Servicio técnico Administrador del reloj biométrico
8	Fin del proceso	

Tabla 6.24. Procedimiento 7

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

PROCEDIMIENTOS # 8 CONFIGURACIÓN DE LA FECHA Y HORA

a) Objetivo

Describir los pasos básicos para el Borrado de los registros del reloj biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**CONFIGURACIÓN DE LA FECHA Y HORA**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Ingresar al menú con la tecla M/OK	Servicio técnico Administrador del reloj biométrico
3	Ingresar a la opción de Fecha y Hora	Servicio técnico Administrador del reloj biométrico
4	Ingresar la Fecha, Hora.	Servicio técnico Administrador del reloj biométrico
5	Aplastar M/OK para guardar cambios	Servicio técnico Administrador del reloj biométrico

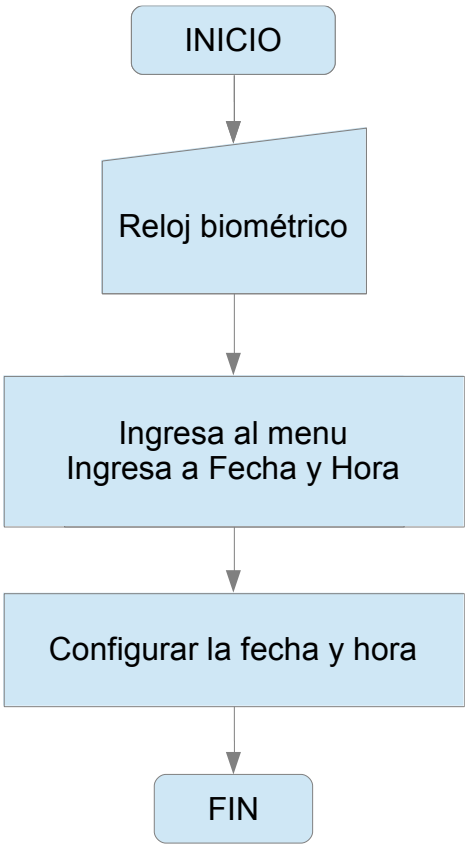
6	Salir con la tecla ESC	Servicio técnico Administrador del reloj biométrico
7	Fin del proceso	

Tabla 6.25. Procedimiento 8

Fuente: Investigador

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

PROCEDIMIENTOS # 9 CONFIGURACIÓN DEL SOFTWARE DE CONTROL

a) Objetivo

Describir los pasos básicos para el Borrado de los registros del reloj biométrico

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**CONFIGURACIÓN DEL SOFTWARE DE CONTROL**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

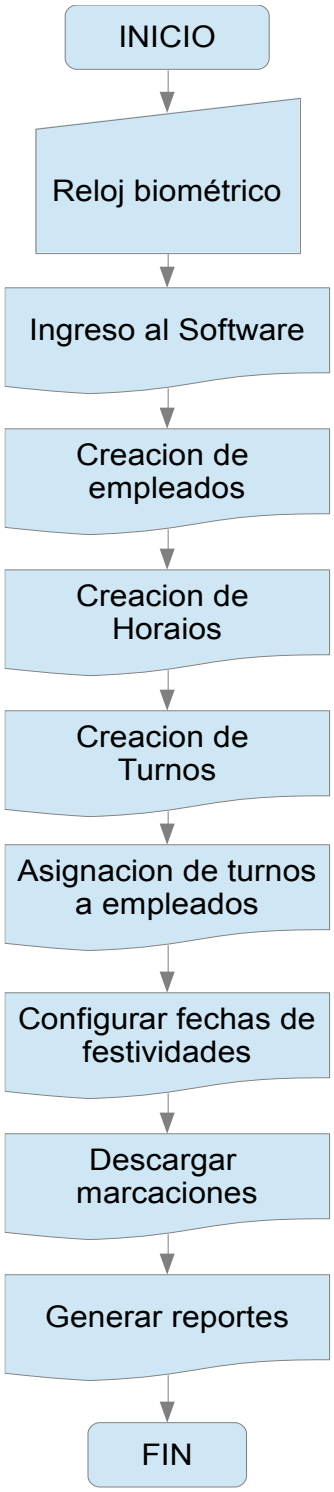
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Ingresamos al Software de control (Ver manual)	Servicio técnico Administrador del reloj biométrico
3	Creamos empleados en la ficha de Empleado (Ver manual)	Servicio técnico Administrador del reloj biométrico

4	Configuramos Horarios (Ver manual)	Servicio técnico Administrador del reloj biométrico
5	Configuramos Turnos (Ver manual)	Servicio técnico Administrador del reloj biométrico
6	Configuramos el Asignamos Turnos u Horarios al o los Empleados (Ver manual)	Servicio técnico Administrador del reloj biométrico
7	Configurar fechas de festividades (Ver manual)	Servicio técnico Administrador del reloj biométrico
8	Descargar marcaciones • A través de la red • O flash memory (Ver manual)	Servicio técnico Administrador del reloj biométrico
9	Generar e imprimir reportes del o los empleados (Ver manual)	Servicio técnico Administrador del reloj biométrico
10	Fin del proceso	

Tabla 6.26. Procedimiento 9

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

Computadora con el software de control

Tener conectividad en la red con el reloj biométrico y la computadora

PROCEDIMIENTOS # 10 PROTECCIÓN DE LA INFORMACIÓN

a) Objetivo

Describir los pasos básicos para la protección de la información en los registros.

b) Intervienen

- Técnico de la empresa que distribuye el reloj biométrico.
- Administrador del reloj biométrico designado por la empresa adquiriente.

c) Descripción del procedimiento

Manual de procedimientos:	**INSTALACION COMPLETA**
Elaborado:	Geovanny Fonseca
Aprobado:	Rene Terán

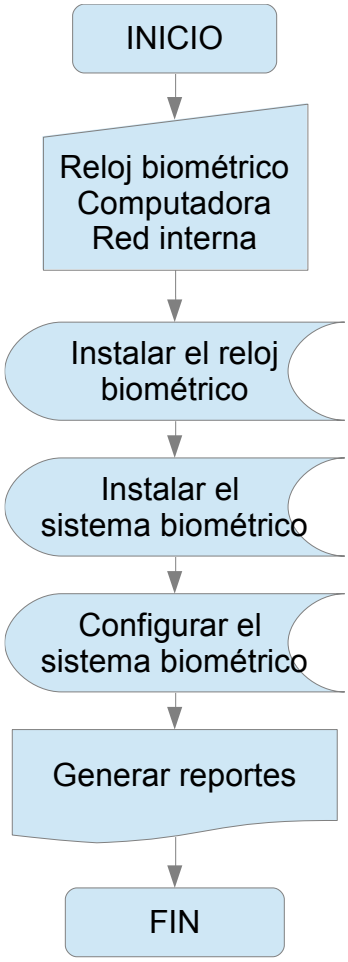
PASO	DESCRIPCIÓN	RESPONSABLE
1	Inicio del proceso	
2	Instalar el reloj biométrico P#1	Servicio Técnico
3	Configurar el direccionamiento IP P#6 **Nota:** Se recomienda tener una red privada con el reloj biométrico y la computadora en donde está instalado el sistema	Administrador del reloj biométrico
4	Tener una computadora **Nota:** Se recomienda poner una clave de seguridad para el inicio del sistema operativo.	Administrador del reloj biométrico
5	Instalar el software P#3	Servicio técnico Administrador del reloj biométrico
6	Configurar el software de control P#9	Servicio técnico Administrador del reloj biométrico
7	Ingresar la dirección IP, mascara y puerta de enlace en el reloj biométrico	Servicio técnico

		Administrador del reloj biométrico
8	Generar reportes	Servicio técnico Administrador del reloj biométrico
9	Fin del proceso	

Tabla 6.27. Procedimiento 10

Fuente: Investigador

d) Diagrama



e) Materiales

Reloj biométrico instalado

Una computadora

Instalación de red LAN

CAPÍTULO VII

Conclusiones y recomendaciones

Conclusiones

- En los relojes biométricos se puedo observar que los lectores o prismas de estos dispositivos no reconocen las huellas dactilares falsas en materiales rígidos.

- La base de datos de los sistemas biométricos no cuentan con alguna seguridad la cual esta propensa a perder la información de las marcaciones y configuraciones del software Attendace Management debido que se puede compartir la carpeta para poder tener instalado en varias máquinas en una red local

- Los archivos de ejecución del software Attendace Management se encuentran sin ninguna seguridad lo cual permite manipular las configuraciones internas de este programa.

- Se puede concluir que los relojes biométricos no están propensos no tiene vulnerabilidades poa infiltraciones debido que tiene

Recomendaciones

- El Reloj no debe estar expuesto a la intemperie, en lugares con alta concentración de partículas de polvo, aerosoles o humedad porque puede causar daños o mal funcionamiento después de un periodo de tiempo.

- Igualmente, no se recomienda dejar el reloj expuesto a la luz directa del sol ya que podría dificultar la correcta lectura e identificación de las huellas.

- A pesar de que el Reloj almacena 5000 huellas, se recomienda que por cada uno se manejen 150 usuarios máximo, con dos huellas diferentes por lo mínimo, así mismo, agilizar la búsqueda e identificación de la huella por parte del Reloj al momento de marcar.

- El reloj captura e identifica las huellas utilizando un sensor óptico el cual requiere que las características físicas y morfológicas de las mismas estén en las mejores condiciones.

- El sensor óptico del Reloj y las huellas de los usuarios deben estar libres de grasa, cremas, polvo y, en general, relativamente limpias en el momento de realizar la marcación.

- El sistema biométrico no se recomienda instalarse en la ruta predeterminada sino en una ruta diferente puesto que dependiendo del sistema operativo la base de datos se crea como archivo de lectura.

- Se recomienda socializar el manual para un mejor conocimiento de políticas y utilización de los relojes biométricos a los administradores de los mismos.

Glosario de términos

AMENAZA: Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos

ATAQUE: Amenaza de origen intencionado

BUGS: comúnmente conocido como **bug** (bicho), es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado.

DERMIS se encuentran las terminaciones nerviosas que corresponden a los receptores sensibles de la piel. El tacto, el dolo, el calor y el frío se perciben gracias a las señales que son enviadas desde la piel al sistema nervioso central.

DISPONIBILIDAD: Situación que se produce cuando se puede acceder a la información contenida en un Sistema, a sus recursos y servicios, conforme a las especificaciones del mismo.

EPIDERMIS o cutícula es una capa superficial delgada de entre1/4 y 1/8 de milímetros de espesor. Recubre la dermis en toda su extensión, y se divide en varias capas, que de la superficie hacia dentro son: estrato córneo, estrato lúcido, estrato granuloso, estrato espinoso y estrato basal.

EXPLOIT: (del inglés to exploit, 'explotar' o 'aprovechar') es una pieza de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con

el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo

FIREWALL.- Literalmente " Muro de Fuego". Se trata de cualquier programa que protege a una red de otra red.

FREEWARE.- Programas de dominio público, programas de libre distribución, programas gratuitos.

INTEGRIDAD: Condición de seguridad que garantiza que la información/sistema no ha sido modificada o alterada por personas, entidades o procesos no autorizados.

INTRÍNSECOS: Que constituye una característica imprescindible e inevitable de algo propio o esencial de una cosa.

KNOPPIX: es una distribución de GNU/Linux basada en Debian y que por defecto utiliza KDE aunque en el menú de arranque se puede especificar el tipo de interfaz gráfica a usar.

PASSWORD.- Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

RIESGO: Posibilidad de que se produzca un impacto determinado en un activo, en un conjunto de activos o en toda la organización causando un daño en alguna de sus dimensiones.

PULPEJO: Parte carnosa, blanda y redondeada de algunas partes pequeñas del cuerpo, especialmente el lóbulo de la oreja, las zonas blandas del dorso de cada dedo, y la parte de la mano que sale del pulgar.

PLAN DE SEGURIDAD: Conjunto de proyectos de seguridad priorizados y presupuestados que permiten materializar las decisiones de gestión de riesgos.

SEGURIDAD INFORMÁTICA: Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los recursos de información tecnológicos de una organización.

SLAX es un Live CD del sistema operativo GNU/Linux basada en la distribución Slackware. No necesita ser instalado, es capaz de arrancar y funcionar desde una unidad de CD, siendo innecesario el uso de un disco duro.

SPYWARE o **programa espía** es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenado

VULNERABILIDAD: Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.

WHOPPIX es una distribución Live de linux que nació con la intención de proporcionar un entorno unificado para la auditoría de seguridad. Su nombre deriva de White Hat Knoppix.

Bibliografía

[1] D. Morales y J. Ruiz-del-Solar, «BuenasTareas,» Abril 2013. [En línea]. Available: http://www.buenastareas.com/ensayos/Sistemas-Bimetricos/24694622.html. [Último acceso: 28 Noviembre 2011].

[2] M. Martinez Dias, «http://arantxa.ii.uam.es/,» Septiembre 2006. [En línea]. Available: http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDcQFjAA&url=http%3A%2F%2Farantxa.ii.uam.es%2F~jms%2Fpfcsteleco%2Flecturas%2F20060926MarcosMartinezDiaz.pdf&ei=ZZQfUuHlGYrAsAT93oCwBg&usg=AFQjCNFc-bLqEdm-VkK0VQec1CjY6KPDxQ&sig2=uhdLrI. [Último acceso: 28 Noviembre 2011].

[3] Maersa, «maersa,» maersa, [En línea]. Available: http://www.maersa.com.mx/historia.html#. [Último acceso: 25 7 2013].

[4] M. Martinez, VULNERABILIDADES EN SISTEMAS DE RECONOCIMIENTO BASADOS EN HUELLAS DACTILAR, Madrid, 2006.

[5] P. L. Brown, «SAS The power to know,» Inc, Copyright © 2009 SAS Institute, 2009. [En línea]. Available: http://www.sas.com/offices/europe/spain/prodsol/spotlights/gestioninformacion.html. [Último acceso: 20 Agosto 2013].

[6] Wikipedia, «Wikipedia,» Wikipedia, 28 1 2008. [En línea]. Available: http://es.wikipedia.org/wiki/Lofoscopia. [Último acceso: 2 8 2013].

[7] «WIKIPEDIA La enciclopedia libre,» WIKIPEDIA , 29 Julio 2013. [En línea]. Available: https://es.wikipedia.org/wiki/Huella_dactilar. [Último acceso: 30 Julio 2013].

[8] E. Saavedra, «Slideshare,» Pen Telematics, [En línea]. Available: http://www.slideshare.net/estebansaavedra/biometria-de-huella-dactilar-dactiloscopia. [Último acceso: 27 7 2012].

[9] A. M. Moreno, «El Blog de leiterantoniomosqueramoreno,» Obolog, 9 Noviembre 2011. [En línea]. Available: http://leiter.obolog.com/huellas-dactilares-1312739. [Último acceso: 28 Agosto 2013].

[10] PatruBOT, «WIKIPEDIA La enciclopedia libre,» WIKIPEDIA , 2 Septiembre 2012. [En línea]. Available:

https://es.wikipedia.org/w/index.php?title=BackTrack&oldid=59331492. [Último acceso: 10 Septiembre 2012].

[11] J. R. Valencia, «CÓMO ELABORAR Y USAR LOS MANUALES ADMINISTRATIVOS,» de *Tercera Edición*, Mexico, ECAFSA - THOMSON LEARNING, 2002, p. 179.

[12] Wikimedia , «Wikimedia La enciclopedia libre,» Fundación Wikimedia, Inc, 28 6 2013. [En línea]. Available: http://es.wikipedia.org/wiki/Huella_dactilar. [Último acceso: 25 7 2013].

ANEXOS

CROQUIS


ATIEMPOFFICE CIA. LTDA.
Montalvo
Mirabeles
La Delicia
Chirimoyas
Delicia
Av. Rodrigo Pachano
Av. Los Guaytambos
Ambato - Quis
Oliero
Los Pepinos
Raimundo De Salazar
Monumento A La Primera Imprenta
Uvas
Moriños
Pepinillo

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

OBJETIVOS: RECABAR INFORMACIÓN QUE PERMITE DESARROLLAR LA INVESTIGACIÓN TITULADA "VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS EN LOS REGISTROS DEL PERSONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN EN DETERMINADAS EMPRESAS DE AMBATO"

CUESTIONARIO: RESPONDA CON SINCERIDAD LAS SIGUIENTES PREGUNTAS.

- **¿EL SISTEMA BIOMÉTRICO HA SUFRIDO ATAQUES EN EL FUNCIONAMIENTO INTERNO?**

1. SI ( )
2. NO ( )

- **¿QUÉ TIPO DE SUPLANTACIONES CONOCE USTED?**

a. HUELLAS FALSAS ( )
b. INFILTRACIÓN DE INFORMACIÓN ( )
c. OTROS ( )

- **¿QUÉ TIPO DE RELOJES CUENTAN EN LA EMPRESA?**

a. LECTOR DE HUELLAS DACTILARES ( )
b. LECTOR DE TARJETAS DE PROXIMIDAD ( )
c. LECTOR DE LA PALMA DE LA MANO ( )
d. TARJETEROS ( )
e. OTROS ( )

- **¿CON RESPECTO A LA TECNOLOGÍA QUE TIPO DE USUARIOS CUENTAN SU EMPRESA?**

a. EXPERTO ( )
b. PRINCIPIANTE ( )
c. INEXPERTO ( )

- **¿LOS DATOS QUE ARROJA EL SISTEMA BIOMÉTRICO LE AYUDA A USTED EN SU LABOR DIARIA?**

a. SI ( )
b. NO ( )

PORQUE: _____

- **¿CÓMO SE DESCARGA LA INFORMACIÓN DEL SISTEMA BIOMÉTRICO?**

a. FLASH MEMORY ( )
b. CABLE DE RED ( )
c. DIRECTAMENTE DEL RELOJ ( )

- **¿QUÉ TIPO DE SEGURIDAD CUENTA EN LOS RELOJES BIOMÉTRICOS?**

a. CÁMARAS ( )
b. GUARDIA ( )
c. NINGUNA ( )
d. OTROS ( )

GRACIAS POR SU COLABORACIÓN

CARACTERÍSTICAS DE LOS RELOJES BIOMÉTRICOS

Biosystem es una marca americana que consta de un dispositivo biométrico de huella digital con un lector óptico de 3ra generación, el cual reconoce dedos húmedos, con polvo y dedos con cortes. El dispositivo digital I360C posee una tarjeta de red incorporada, y un puerto U Disk (USB), lo cual hace muy efectiva la comunicación y la descarga de datos desde el dispositivo. El sistema biométrico viene incluido con un software de control de asistencia y administración del personal, una herramienta muy útil para el departamento de RRHH.

BENEFICIOS:

- Reloj biométrico de huella digital con Web Server, permite ver registros desde cualquier navegador de Internet por medio de la red.
- Podemos registrar hasta las 10 huellas de un empleado.
- La huella digital es infalsificable e intransferible, lo cual ayuda a evitar fraudes
- Disminuye tiempo y gastos en el proceso de control de asistencia.
- Puede trabajar en red o fuera de ella.
- CPU americano Intel 32 bit X-scale.
- Puede identificar la huella con una rotación de 180^0, es decir cualquier ángulo de posición
- Sensor óptico de 500 DPI, acepta dedos secos, húmedos y con polvo.
- Confirmación de lectura de registro por medio de:

- Voz en español
- Luz indicadora verde o roja.
- Mensaje escrito de acceso
- Nombre del Empleado y código

ESPECIFICACIONES TÉCNICAS:

- Comunicaciones con el Dispositivo: USB, TCP/IP, RS232, RS485
- Tarjeta de red incorporada, permite comunicación entre lugares distantes.
- Capacidad de huellas: 3000 huellas digitales upgrade de 5.000 huellas digitales
- Capacidad de almacenamiento: 100.000 registros
- Sistema Operativo: Linux
- Tiempo de identificación: Menor o igual a 0.7 segundos
- FAR: $\leq 0.0001\%$
- FRR: $\leq 0{,}01\%$
- LED: Rojo, Verde
- LCD: 128 x 64 luz azul de fondo
- Temperatura de operación: 0^0C a 45^0C
- Humedad de operación: 20% a 80%
- Idiomas: Inglés / Español
- Adicionales: Timbre de horario con melodías internas, webserver,
- Función de impresión (Varios modelos de impresión)
- Puede grabar 10 códigos para enrolar a un empleado.
- Batería de reserva de energía: UPS 5v (5 horas)
- Batería de memoria interna: Tiempo Indefinido
- Pantalla a color con menú interactivo multimedia

RELOJ BIOSYSTEM MODELO STYLUS 980

CARACTERÍSTICAS:

- Multimedia
- Pantalla: 3.5” TFT Full color, con diferentes formatos multimedia
- Cámara de Fotos móvil integrada en el dispositivo
- Función Photo-ID que fotografía al empleado y almacena la imagen junto a la fecha y hora de marcación cuando registra su asistencia
- Batería de reserva integrada, no externa
- Sensor óptico resistente a rasguños
- Registra 8.000 huellas digitales
- Memoria interna de 200.000 registros
- Práctica Función SMS
- Múltiples formas de autenticación mediante combinaciones de: Huella Digital, Password o Tarjeta RFID 125 KHz
- Teclas de función definidas por el usuario
- Control de Accesos
- Tarjeta de Red incorporada
- Función de monitoreo para seguimiento de empleados
- Idioma Español

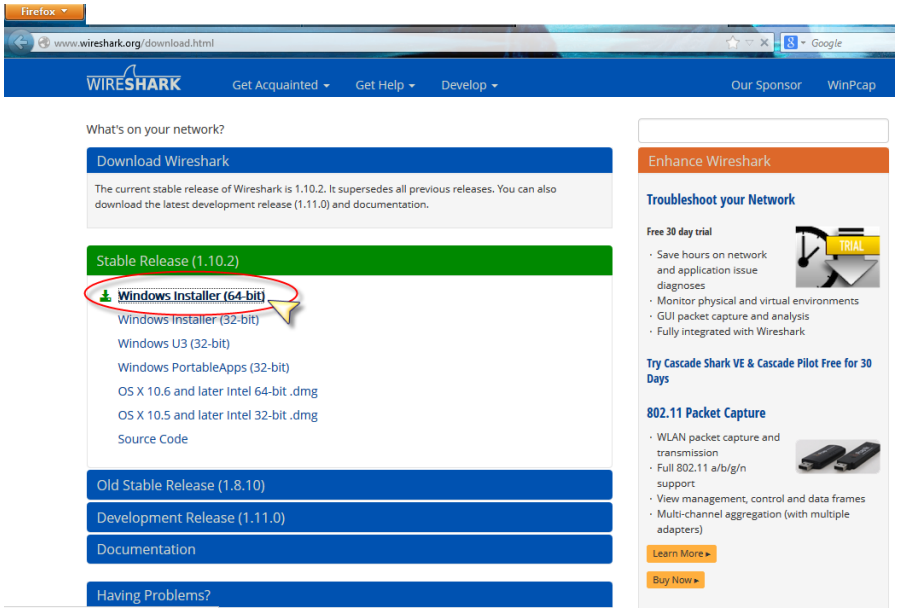
- Varias opciones de comunicación que incluyen TCP/IP, USB Host, USB Cliente

ESPECIFICACIONES TÉCNICAS:

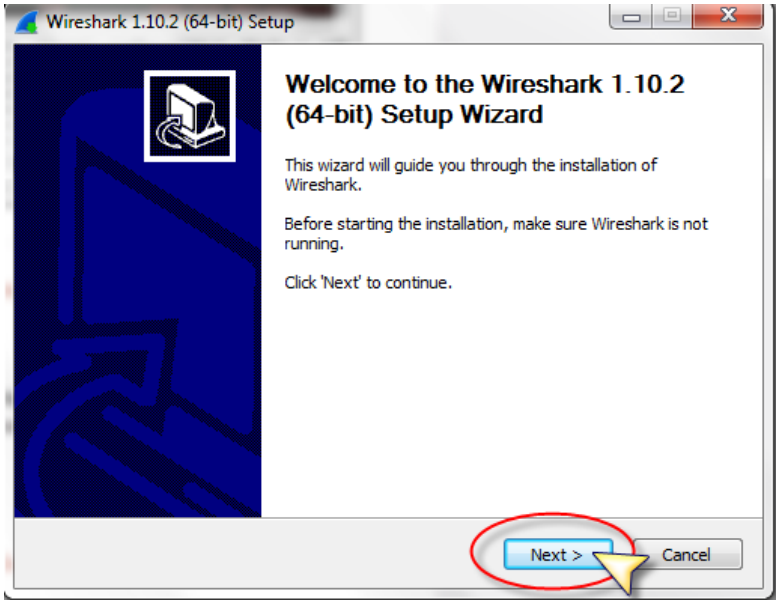
- Capacidad de Huellas: 8.000 huellas
- Capacidad de registros: 200.000 marcaciones
- Plataforma de Hardware: ZEM600
- Sensor: Óptico
- Identificación: 1:1 o 1:N
- Tasa de Falsa Aceptación <= 0.0001%
- Tasa de Falso Rechazo <= 1%
- Pantalla: 3.5” TFT Full Color
- Comunicación : TCP/IP, USB-Cliente, USB-Host
- Funciones estándar: Photo ID, 8 teclas de función, Web server, cámara de fotos móvil incorporada, batería de reserva incorporada, SMS
- Suministro de Energía: 12V DC 3A
- Tamaño: 213 mm (largo) x 178.2 mm (ancho) x 47.5 mm (profundidad)
- Inteface para control de Accesos: Cerradura magnética, botón de salida, alarma
- Señal Wiegand: Entrada y Salida

Instalación de Wireshark

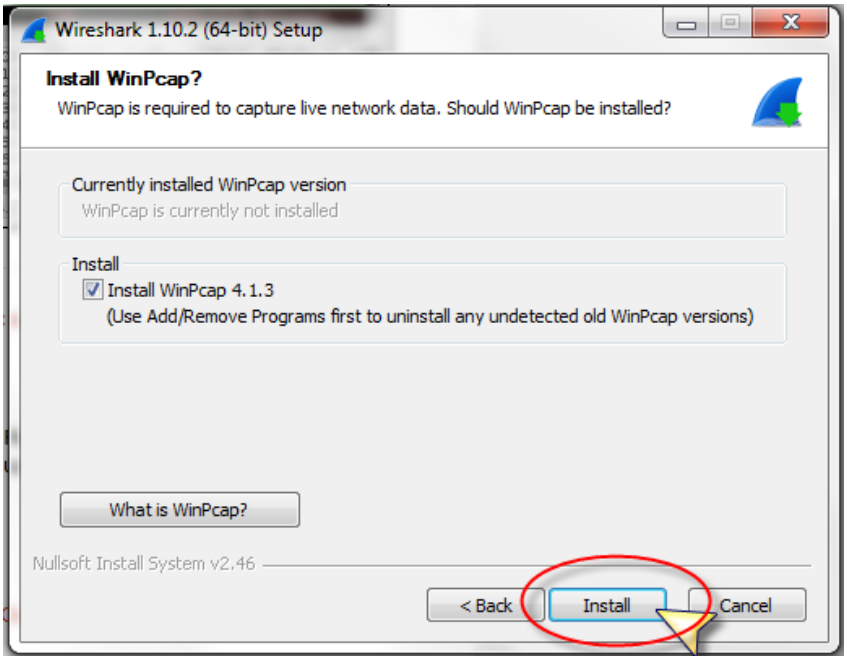
- Descargamos la última versión de Wireshark desde la página oficial http://www.wireshark.org/



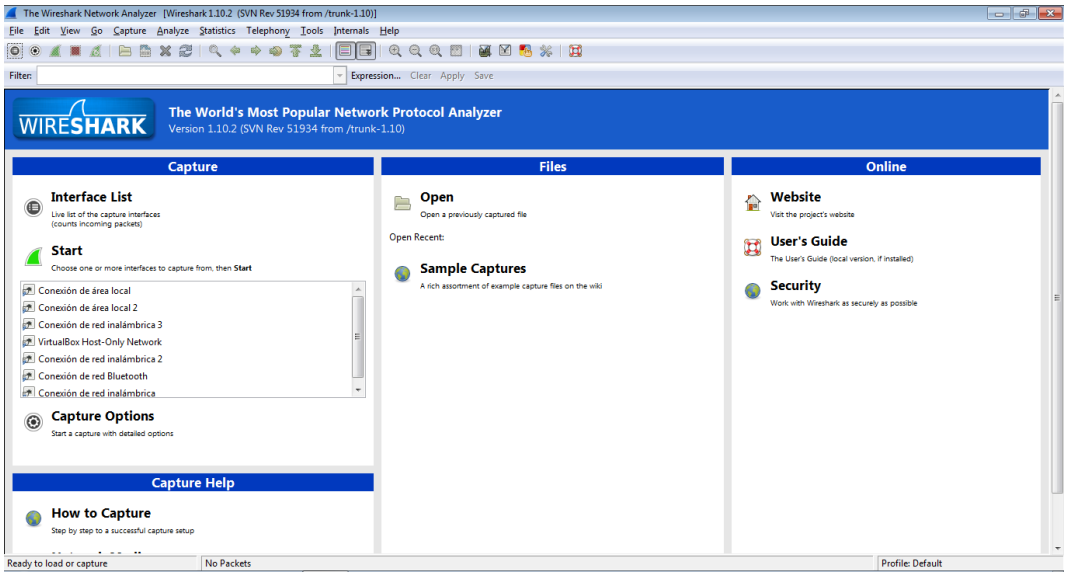
- La instalación es igual que la mayoría de programas de Windows Double clic en el archivo de instalación que ha descargado anteriormente y mostrará la siguiente pantalla.



- Continuamos con la instalación aceptamos los términos de referencia, paquetes incluidos y comenzará la instalación.

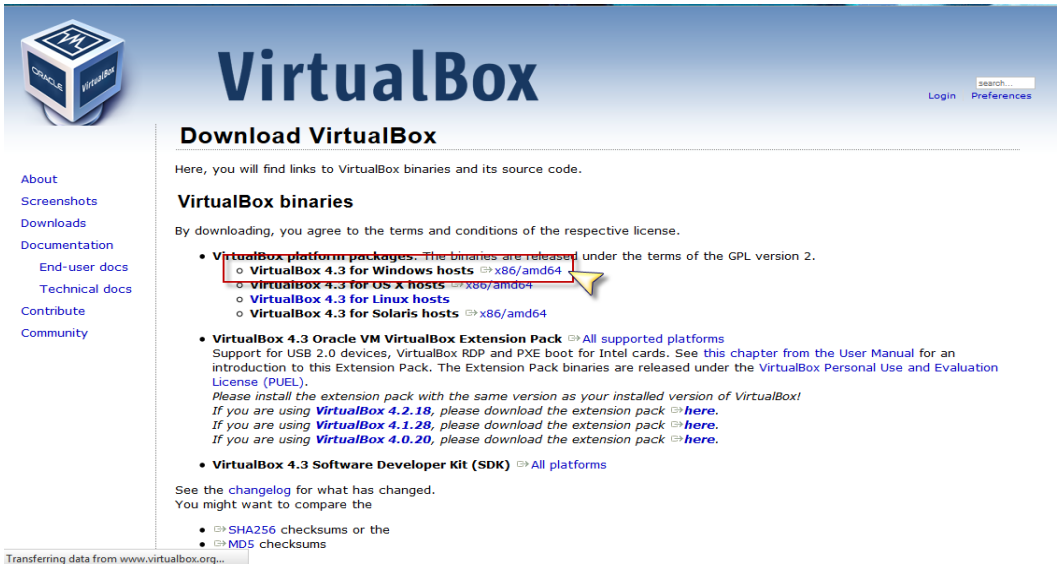


- Una vez finalizada la instalación procedemos abrir y el programa de Wireshark.

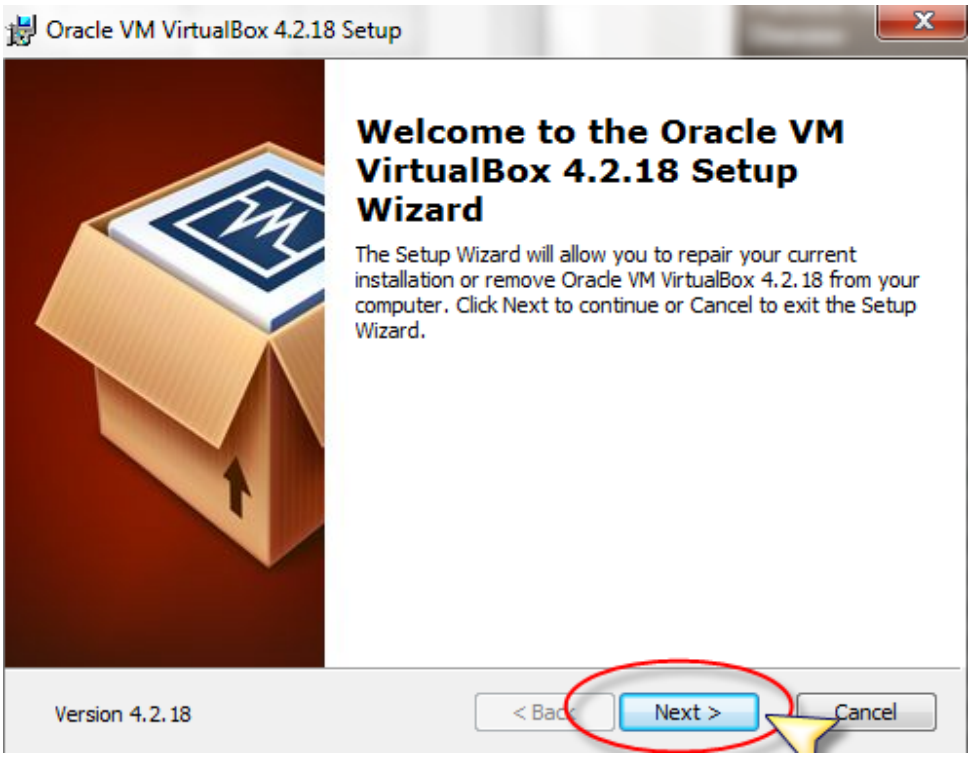


Instalación de Oracle VM VirtualBox Manager

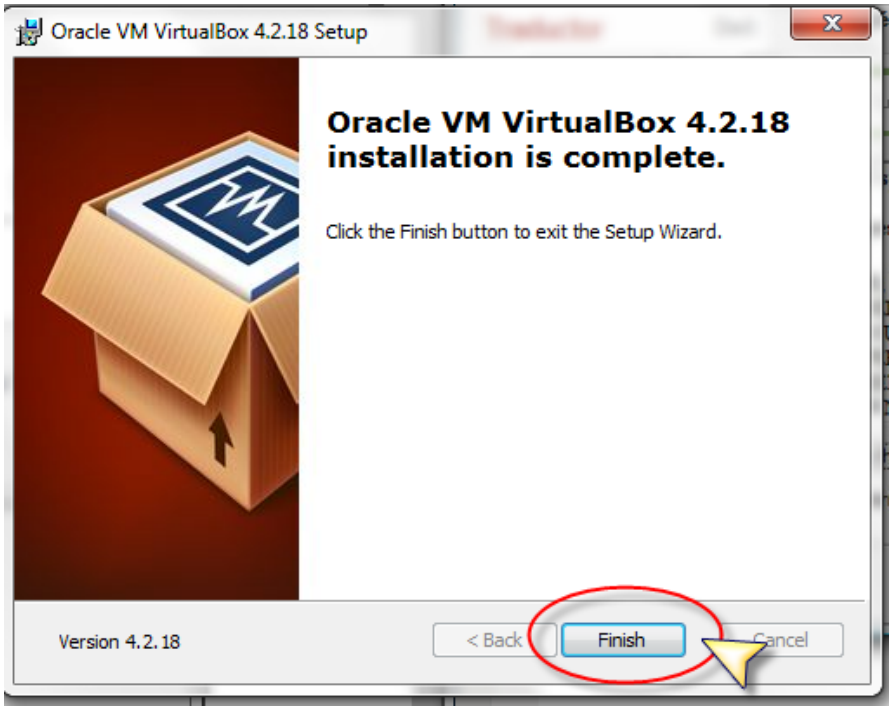
- Descargamos la última versión de VirtualBox desde la página oficial https://www.virtualbox.org.



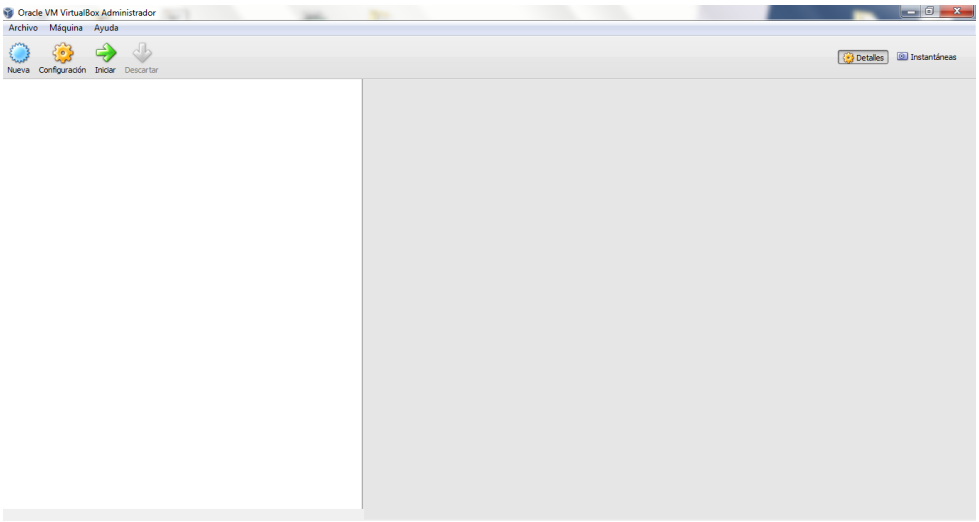
- La instalación es igual que la mayoría de programas de Windows Double clic en el archivo de instalación que ha descargado anteriormente y mostrará la siguiente pantalla.



- Continuamos con la instalación aceptamos los términos de referencia y comenzará la instalación una vez terminada la instalación nos aparecerá la siguiente imagen donde damos clic en finalizar.



- Una vez finalizada la instalación procedemos abrir y a configurar una máquina para instalar backtrakin en este programa ayudándonos a virtual izar una maquina real.

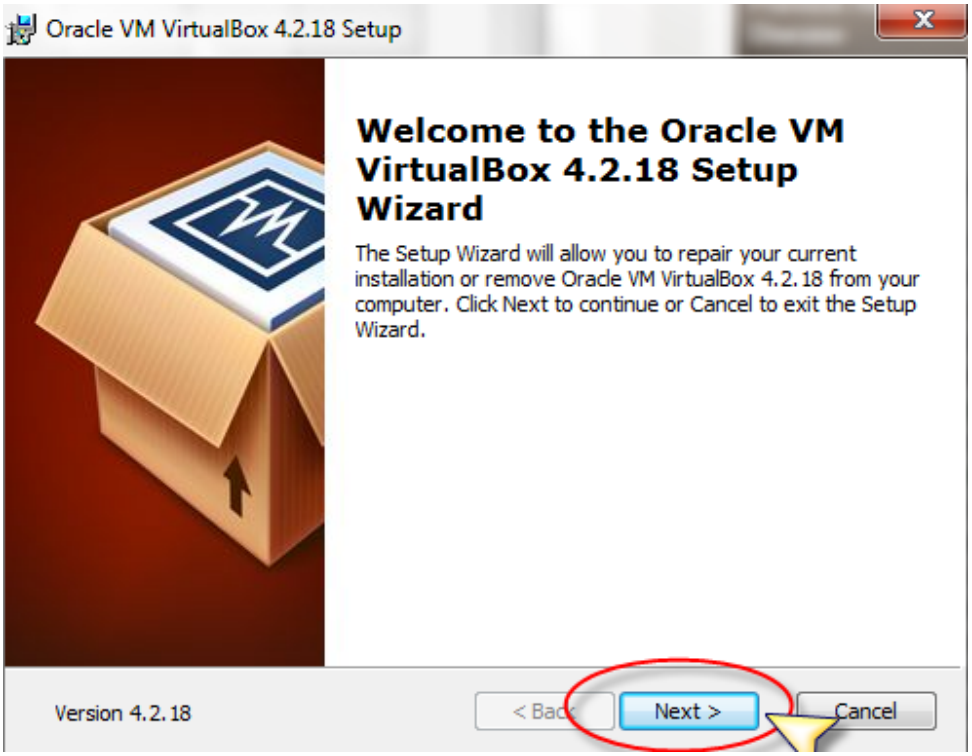


Servicio de Nessus

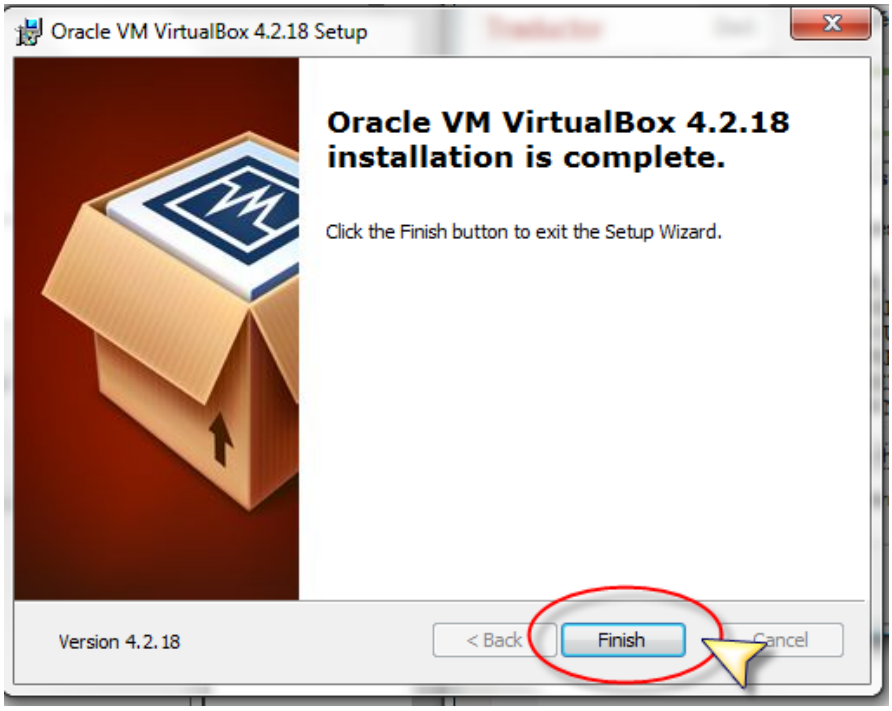
- Prendemos la máquina virtual de BACKTRACK con el Usuario de *root* y Contraseña *toor* e ingresamos en modo gráfico con el comando *startx* como nos muestra en la imagen.

- Antes de ingresar a NESSUS tenemos que iniciar el servicio en Applications – BackTrack – Vulnerability Assessment – Network Assessment – Vulnerability Scanners y nessus start.
- Una ves iniciado nessus podemos ingresar a un Browser e ingresamos la siguiente dirección https://127.0.0.1:8834

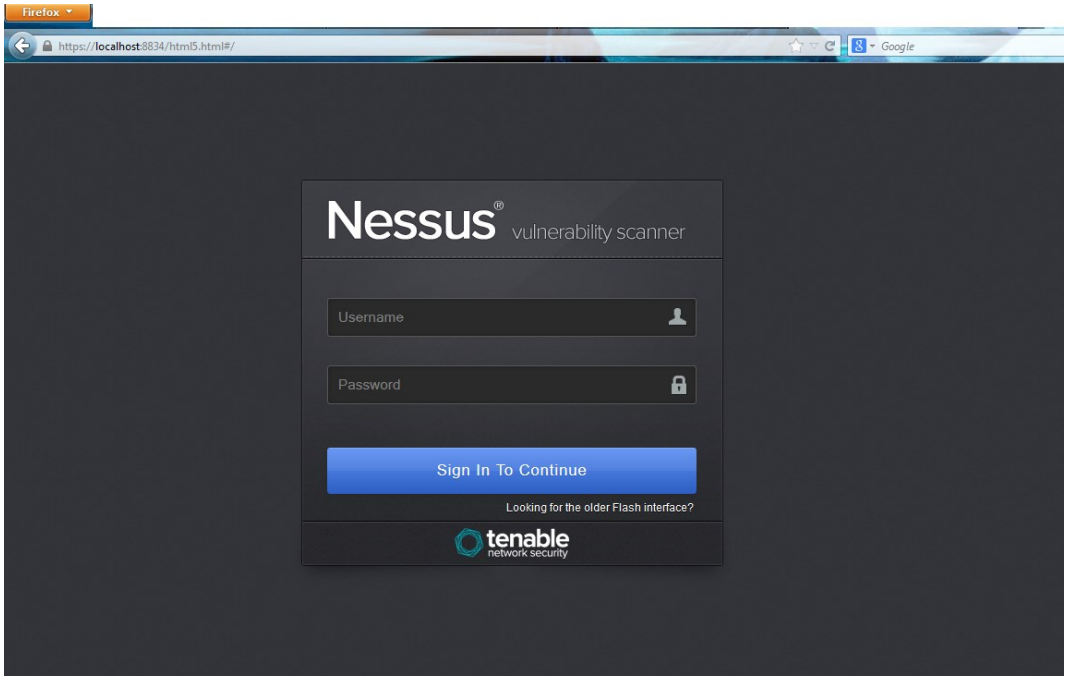
- La instalación es igual que la mayoría de programas de Windows Double clic en el archivo de instalación que ha descargado anteriormente y mostrará la siguiente pantalla.



- Continuamos con la instalación aceptamos los términos de referencia y comenzará la instalación una vez terminada la instalación nos aparecerá la siguiente imagen donde damos clic en finalizar.



- Una vez finalizada la instalación procedemos abrir y a configurar una máquina para instalar backtrakin en este programa ayudándonos a virtual izar una maquina real.


Firefox
https://localhost:8834/html5.html#/
Google
Nessus® vulnerability scanner
Username
Password
Sign In To Continue
Looking for the older Flash interface?
tenable network security

Reporte del CVE

Unencrypted Telnet Server

Family: Misc.

Nessus Plugin ID: 42263 ()

Bugtraq ID:

CVE ID:

Synopsis :

The remote Telnet server transmits traffic in cleartext.

Description :

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.

Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Solution :

Disable this service and use SSH instead.

Risk factor :

Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)