UNIVERSDIDAD AMAZONICA DE PANDO

ÁREA CIENCIAS Y TECNOLOGÍA

PROGRAMA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADO

"SISTEMA DE CONTROL DE ACCESO A LOS LABORATORIOS DE INFROMATICA DEL AREA DE CIENCIAS Y TECNOLOGIA DE LA UNIVERSIDAD AMAZONICA DE PANDO"

PROYECTO DE GRADO PRESENTADO PARA OBTAR AL TÍTULO ACADÉMICO DE LICENCIADO EN INGENIERÍA DE SISTEMAS INFORMATICOS

Postulante : Univ. Erland Duran Nakashima.

Tutor : Ing. Juan Carlos Gallardo Jiménez

Asesor : Ing. Mayko Antonio Antezana Sosa

Cobija – Pando – Bolivia

2018

AGRADECIMIENTOS

Primeramente, agradecer a Dios, por darme la vida, salud, fuerza y entusiasmo para seguir adelante.

A mi familia que siempre está a mi lado dándome consejos y apoyándome en todo momento.

A mi tutor, por sus constantes sugerencias, consejo, paciencia y confianza, decirle que le guardo un profundo respeto, cariño y gratitud.

A mi asesor, por la valiosa orientación, en el avance del proyecto, decirle que le guardo un profundo respeto.

Y a todas las personas que de alguna manera me apoyaron antes, durante el proyecto, me enseñaron cosas valiosas.

Para todos ellos y a quienes no nombro muchas gracias

DEDICATORIA :

A mis padres por el apoyo que me dan día a día.

Y a todos los que hicieron posible la culminación de este proyecto

RESUMEN

Con el surgimiento de nuevas tecnologías, la informática ha llegado a niveles de especializaciones elevadas y exactas, es así que el medio donde vivimos, demanda de profesionales capaces de hacer uso de estas herramientas en el contexto del control de ingresos a ambientes restringidos, con el propósito de tener un mejor control e información actualizada del personal que ingresa a dichos ambientes.

Estos sistemas pueden utilizados para la toma de decisiones oportuna.

Al identificar como problema principal, **"Inadecuado control de acceso a los Laboratorios de Informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando"** se establece el objetivo de Implementar un sistema de control de acceso automatizado a los laboratorios de informática del área de ciencias y tecnología de la universidad amazónica de pando, utilizando chapa magnética de puerta biométrica L700 y control de acceso ZKTeco.

El mismo que es implementado de acuerdo a requerimiento

El proyecto fue implementado de acurdo a la metodología modelo funcional.

SUMMARY

With the emergence of new technologies, computer science has reached high and exact specialization levels, so that the environment where we live, demand professionals capable of using these tools in the context of income control to restricted environments, with the purpose of having a better control and updated information of the personnel that enters such environments. These systems can be used for timely decision making.

When identifying as main problem, "Inadequate access control to the Computer Science and Technology Area Laboratories of the Amazonian University of Pando" establishes the objective of Implementing an automated access control system for computer laboratories in the area of science and technology of the Amazonian University of Pando, using magnetic biometric gateway L700 and ZKTeco access control.

The same that is implemented according to requirement
The project was implemented according to the functional model methodology.

INDICE

CAPITULO I

CAPITULO II

CAPITULO III

INDICE DE FIGURA

INDICE DE FOTO

INDICE DE IMAGEN

INDICE DE TABLA

CAPITULO I
INTRODUCCION

1.1. ANTECEDENTES

El Área de Ciencia y Tecnología dependiente de la Universidad Amazónica de Pando, cuenta con tres laboratorios de informática, las mismas que prestan servicio a docentes y estudiantes de las carreras de Ing. De Sistemas, Ing. Industrial e Ing. Civil, como también a otros usuarios, siendo estos laboratorios de libre ingreso para todos, puesto que no cuenta con ningún tipo de restricción.

Es por esta razón, que se pretende implementar un sistema de control de acceso a los laboratorios de informática, para brindar un mejor control y una mejor administración de los mismos.

Se toma como referencia algunos estudios y proyectos que se hicieron relacionados a esta temática. A continuación se describen algunos proyectos realizados como referencia:

- "Prototipo de control de acceso a aulas y registro automático de asistencia" (Grupo de Investigación en Innovación y Tecnología GIIT, Soledad, Colombia.)

- "Sistemas de control de accesos a edificios mediante tarjetas criptográficas y tarjetas RFID" (Marta Velayos Sardaña, Madrid)

- "Diseño e implementación de un sistema de acceso" (Justo Javier Saavedra Guada, Caracas Venezuela)

1.2. PLANTEAMIENTO DEL PROBLEMA

Actualmente el Área de Ciencias y Tecnología no dispone de un sistema de control de acceso a los laboratorios de forma automatizada, impidiendo que se tenga un control adecuado y preciso del personal que ingresa a los laboratorios de informática ya que muchas veces los equipos electrónicos son dañado por personas ajenas a esta institución, es por esta razón, que se hace necesario implementar un Sistema de control de acceso a los laboratorios de informática para tener un control adecuado, preciso y en tiempo real, permitiendo el ingreso solo al personal autorizado y así también poder restringir el ingreso a esas personas que son ajenas a la institución.

Todo lo anterior mencionado constituye el siguiente problema principal.

“Inadecuado control de acceso a los Laboratorios de Informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando”

1.2.1. SOLUCION PROPUESTA

Se plantea la siguiente solución:

Implementar un Sistema de Acceso a los Laboratorios de Informática del Área de ciencias y Tecnología de la Universidad Amazónica de Pando utilizando chapa de puerta biométrica L700 y control de acceso ZKTeco.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un sistema de control de acceso automatizado a los laboratorios de informática del área de ciencias y tecnología de la universidad amazónica de pando, utilizando chapa magnética de puerta biométrica L700 y control de acceso ZKTeco.

1.3.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico de la situación actual de los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando.
- Realizar el diseño de la red de control de acceso a los laboratorios de informática.
- Realizar la instalación de la chapa magnética de puerta biométrica L700 y control de acceso ZKTeco de acuerdo al diseño de la red de control de acceso.
- Realizar la configuración del control de acceso ZKTeco.
- Realizar la prueba del sistema de control de acceso a los laboratorios de informática.

1.4. JUSTIFICACION

1.4.1. JUSTIFICACION ECONOMICA

El uso de sistemas de control de acceso es ahora una de las mejores formas de control, y registro del personal que ingresa a dichos establecimientos que muchas veces son restringidos para otros usuarios.

La utilización de este tipo de herramientas permite reducir los gastos o recursos invertidos para este propósito, permitiendo a la institución ahorrar en la compra de papel y otros objetos que se necesita para su registro posterior registro.

1.4.2. JUSTIFICACION SOCIAL

Con la implementación del Sistema de Control de Acceso a los Laboratorios, se beneficiara de manera directa a la Institución que es el Área de Ciencias y Tecnología de la Universidad Amazónica de Pando, como también a docentes, estudiantes, administrativos y sociedad civil.

1.4.3. JUSTIFICACION TECNICA

La implementación del Sistema de Control de Acceso a los Laboratorios de Informática se aplicara las herramientas, Chapa De Puerta Biométrica L700 Y Control De Acceso ZKTeco, este Sistema de Control de Acceso será de gran apoyo para el Área de Ciencias y Tecnología ya que permitirá el control y registro del personal que ingrese a estos Laboratorios, Ofrecerá también un método seguro de control y un mecanismo de identificación los cuales llevaran almacenada la información referente al usuario que las utilizara las cuales podrán ser reportadas posteriormente en informes concisos y precisos.

1.5. ALCANCES

El alcance del presente proyecto de grado será la implementación de un Sistema de Control de Acceso a los laboratorios de Informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando, utilizando chapa de puerta biométrica L700 y control de acceso ZKTeco.

Con la implementación del sistema de control de acceso a los laboratorios de informática, se tendrá un mejor control del ingreso del personal autorizado.

1.6. METODOLOGIA Y HERRAMIENTAS UTILIZADAS

Para el desarrollo de este proyecto de grado se utilizó la Metodología, Modelo Funcional.

La ventaja de esta metodología, es que se divide en 5 áreas funcionales que son: Configuración, fallas, rendimientos, contabilidad y seguridad, donde se define las funciones de cada una de ellas. Para el desarrollo del proyecto se utilizó tres procesos los cuales son: Administración de configuración, administración de fallas, administración de rendimientos.

1.6.1. ADMINISTRACIÓN DE CONFIGURACIÓN

Dentro del proceso de la administración de configuración, se encuentran las siguientes actividades: planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento.

1.6.2. ADMINISTRACIÓN DE FALLA

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata.

Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla

1.6.3. ADMINISTRACIÓN DE RENDIMIENTO

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

Para el desarrollo de este proyecto se utilizó las siguientes herramientas:

- **Lector biométrico de huella dactilar ZKTeco:** Se entiende por lector biométrico aquel que se caracteriza por reconocer algún parámetro físico o de comportamiento de la persona.

- **Chapa magnética de puerta biométrica:** Las chapas magnéticas son elemento indispensable de seguridad, la cerradura presenta en la actualidad un gran número de variantes, cada una asociada a distintas tecnologías.
- **Brackets:** se usa para puertas que abran en dirección del exterior al interior y se quiera que el magneto quede del lado interior.
- **Pulsador botón metálico para apertura de puerta:** son Controles alámbricos o inalámbricos que permiten abrir las puertas. Se utilizan por lo general al interior de las torres de apartamentos o pisos de oficinas, pues como el personal ya se identificó al entrar, no es necesario validar la identidad al salir.

1.7. RESULTADOS OBTENIDOS

- Se realizó un diagnóstico de la situación actual de los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando.
- Se realizó el diseño de la red de control de acceso a los laboratorios de informática.
- Se realizó la instalación de la chapa magnética de puerta biométrica L700 y control de acceso ZKTeco de acuerdo al diseño de la red de control de acceso.
- Se realizó la configuración del control de acceso ZKTeco.
- Se realizó la prueba del sistema de control de acceso a los laboratorios de informática.

1.8. ORGANIZACIÓN DEL DOCUMENTO

El presente proyecto se organiza de la siguiente manera:

CAPÍTULO I, se refiere a los antecedentes, el problema, la solución propuesta, los objetivos y la metodología adoptada para el cumplimiento de los objetivos.

CAPÍTULO II, presenta el marco teórico y conceptual del trabajo, hace referencia a la metodología, herramientas y técnicas aplicadas para el desarrollo del proyecto de grado.

CAPÍTULO III, presenta la ingeniería del proyecto, el desarrollo del proyecto, y la implementación del sistema.

CAPÍTULO IV, presenta las conclusiones y recomendaciones del proyecto

En el presente capítulo se da a conocer toda la información necesaria y relacionada con el sistema de control de acceso automatizado a los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando.

CAPITULO II

MARCO INSTITUCIONAL

MARCO LEGAL

MARCO TEORICO

2.4. MARCO INSTITUCIONAL

La Universidad Amazónica de Pando, es una Institución Pública y Autónoma de Educación Superior, que forma profesionales idóneos, con excelencia académica, pensamiento crítico y compromiso social, que desarrolle la investigación científica y tecnología, promoviendo la interacción social, en un contexto de diversidad social e interculturalidad, para contribuir al desarrollo integral de nuestra amazonia. (U.A.P. 2013)

MISION

Institución Pública (Domótica Viva s.l., 2002) y Autónoma de Educación Superior, que forma profesionales idóneos, con excelencia académica, pensamiento crítico y compromiso social, que desarrolle la investigación científica y tecnología, promoviendo la interacción social, en un contexto de diversidad social e interculturalidad, para contribuir al desarrollo integral de nuestra amazonia.

VISIÓN INSTITUCIONAL

En el año 2017 la Universidad Amazónica de Pando será una Universidad Autónoma, transparente, desconcentrada, incluyente, con libertad de pensamientos, comprometida con su población, que brinde profesionales de excelencia académica, investigación científica y tecnología pertinente hacia su entorno; enfocada en una gestión moderna y flexible basada en resultados, con todos sus programas acreditados, orientados al bienestar de la comunidad universitaria para contribuir al desarrollo integral de nuestra amazonia.

Área de Ciencias y Tecnología

El año 1996 se crea la carrera de informática a nivel técnico superior mediante la resolución N° 01/1996 del Honorable Consejo Universitario, con aproximadamente 300 estudiantes en el curso vestibular.

En 1998 se da inicio a las gestiones para ampliar la carrera de nivel técnico superior al de Licenciatura, proyecto que fue muy bien recibido e impulsado por las autoridades universitarias. Posteriormente, en la gestión 2000, del 31 de enero al 4 de febrero se realiza la primera pre-sectorial en la carrera, y la primera en la Universidad donde participan los docentes y estudiantes en sus diferentes comisiones. Resultado de dicha pre sectorial son las recomendaciones que orientaron a la carrera en su posterior desarrollo. El mismo año se logra implementar el

laboratorio Superior de Informática, LASIN, gracias a la adquisición de 15 computadoras que fueron gestionadas por el entonces Sr. Rector. Ing. Ronald Camargo S., y las autoridades de la Carrera.

El año 2006 el Área de Ciencias y Tecnología incorpora dos nuevos Programas: Ingeniería Civil e Ingeniería Industrial a nivel licenciatura. El 2009 se inicia una transición gradual del Programa de Ingeniería Informática a Ingeniería de Sistemas.

En la actualidad el Área de Ciencias y Tecnología forma profesionales en los Programas de Ingeniería de Sistemas, Ingeniería Industrial e Ingeniería Civil; albergando a un número aproximado de 297 en las tres carreras, que con sus conocimientos contribuirán en el desarrollo de la región y el País.

Misión

Es formar recursos humanos en ciencias y tecnología altamente capacitados, con espíritu crítico y de acuerdo a las exigencias de la demanda regional y nacional, generar conocimiento científico y tecnológico, estudiando problemas del medio y contribuir a la innovación y desarrollo de tecnologías apropiadas, a través de tres funciones básicas integradas: Enseñanza-Aprendizaje, Investigación Científica y Tecnológica e Interacción Social.

Visión

Formar profesionales en el pregrado con calidad y excelencia, adecuados a la demanda nacional y en el tiempo previsto, que estén en la capacidad de producir tecnología y generar conocimiento para el estudio y tratamiento de los problemas del medio. Ser un Área con reconocimiento Nacional e Internacional, con estructura matricial que permita responder rápidamente a los cambios y a las necesidades regionales y nacionales en forma eficiente y efectiva. Formar recursos humanos altamente especializados con infraestructura necesaria y equipamiento adecuado, para ejecutar satisfactoriamente las actividades de formación y de investigación.

2.5. MARCPO LEGAL

La Universidad Amazónica de Pando, fue creada mediante Decreto Supremo N° 20511 del 21 de septiembre de 1984 y sancionada mediante Ley de la Nación N° 653 de 18 de octubre de 1984.

El Estatuto Orgánico de la UAP fue aprobado en la VI Conferencia Nacional de Universidades en octubre de 1997 y por el Congreso Nacional de Universidades el mes de mayo de 1999, ambos eventos realizados en la ciudad de Trinidad Capital del Departamento del Beni.

Las actividades académicas comenzaron oficialmente el 3 de diciembre de 1993, con dos Carreras:

- Licenciatura en Biología
- Licenciatura en Enfermería.

En agosto de 1996 se incorporó la carrera de Informática a nivel de Técnico Superior. Posteriormente, consecuente con la política de diversificación de la oferta curricular, a partir de la gestión académica del 2000 se crearon los siguientes programas académicos:

- Ingeniería Agroforestal, a Nivel de Licenciatura.
- Derecho, con mención en derecho ambiental, a nivel de Licenciatura.
- Construcción Civil, a nivel de Técnico Superior
- Pesca y Acuicultura, también a nivel de Técnico Superior.

2.6. MARCO TEORICO

2.6.1. INTRODUCCIÓN

Los sistemas de control automático han jugado un papel vital en el avance de la ciencia y de la ingeniería. Además de su extrema importancia en vehículos espaciales, sistemas de guía de proyectiles, sistemas de piloto automático de aeronaves, sistemas robóticos y otros, el control automático se ha vuelto parte integral de los procesos industriales y de manufactura.

Además se puede decir que gracias a la acción del control automático ha sido posible la fabricación de productos complejos en condiciones estables de calidad y de características, condiciones que al operario le serían imposibles o muy difíciles de conseguir, realizando exclusivamente un control manual. (Carrillo, 2011)

El mercado actual, y las empresas que a ello se dedican ofrecen diversos métodos de control de acceso, entre los que se destacan los lectores biométricos y los de radiofrecuencias. (Carrillo, 2011)

Un sistema de control de acceso permite controlar el acceso libre y aleatorio, a través de puntos de acceso (puertas de seguridad, etc.), a zonas específicas en una empresa u oficina, así como formar un registro de los movimientos de cada uno de los usuarios del sistema. Ofrecen un método seguro de control mediante tarjetas con banda magnética, tarjeta de identificación por radio frecuencia (RFID), mecanismo de identificación por huellas dactilares u otro mecanismo, los cuales llevan almacenada información referente al usuario que las utiliza. Estos sistemas se encargan de la supervisión y control de los puntos de acceso de distintas zonas, registrando las actividades, las cuales pueden ser reportadas posteriormente en informes concisos. (Carrillo, 2011)

En el Área de Ciencias y Tecnología, en su papel de participantes activos por el desarrollo de su entorno y en especial de su propia institución, proponen una solución a la necesidad de control de ingreso a los laboratorios de informática, implementando tecnología de punta que ofrezca flexibilidad y confiabilidad.

La idea del proyecto surge debido a que el ingreso a los laboratorios de informática es un proceso netamente manual, que depende de una persona encargada de administrar los distintos espacios físicos. Esto se convierte en una necesidad importante para la generación de una solución tecnológica que permita realizar dicho proceso de forma automatizada, minimizando los tiempos de ingreso, realizando un control eficiente del personal debidamente autorizado y posibilitando además la generación de reportes actualizados.

Adicionalmente, se encuentra la necesidad de implementar un sistema de registro automático y sistematizado de ingreso a los laboratorios por parte de los docentes, estudiantes y otros, ya que el método empleado para dicha tarea consiste en la recolección de firmas en formatos impresos, mientras que el sistema propuesto minimizara el uso de papel aportando al cuidado del medio ambiente, al mismo tiempo que permite la generación de un reporte más preciso, real y actualizado de la asistencia a los laboratorios.

El desarrollo del proyecto se basa en la implementación de un sistema de control de acceso que implemente de manera más rápida y sencilla una administración confiable, de manera que se puede obtener información precisa e instantánea sobre la ubicación de cada usuario (docentes, estudiantes), al mismo tiempo que se puede restringir el acceso no autorizado a estos laboratorios de informática. De esta manera se pretende controlar de forma sistemática el ingreso a los laboratorios maximizando la eficiencia y mejorando la productividad con una administración segura.

2.6.2. **SISTEMAS INTELIGENTES**

Un sistema inteligente es un sistema con conciencia, estructuras y organización de alta integración y sensibilidad que le permite responder adecuada, oportunamente y eficientemente a los problemas derivados de su interacción con el entorno. (Ramírez, 2005)

Un Sistema inteligente presenta, como principal característica, su capacidad de adaptación a condiciones variables de su entorno, en pos del cumplimiento de sus objetivos. Para ello debe poseer tres capacidades básicas: (D`Aguila, 2005)

- De Razonar, para obtener conclusiones y, de ahí, tomar sus propias decisiones.
- De Aprender, para adquirir nuevos conocimientos, a partir de sus experiencias.
- De Interactuar con otros Sistemas Inteligentes, mediante la comunicación y el entendimiento. (D`Aguila, 2005)

Sistemas Basados en el Conocimiento

Los Sistemas Inteligentes son sistemas computacionales que presentan la arquitectura de software. De la misma surge la presencia de tres unidades independientes: el control computacional, una base de conocimientos y una base de datos. (Proaño, 2016).

El control puede verse desde dos puntos de vista: computacional y lógico. Desde el punto computacional, es un intérprete o compilador, del programa de conocimientos, que contiene la base de conocimientos. Es decir, en una máquina, en este tipo de sistemas, se produce una doble

interpretación y compilación: la que origina el lenguaje de alto nivel que se utilice, y la producida por el programa de conocimientos. Desde el punto de vista lógico, el control representa la simulación de un mecanismo de inferencia deductiva o capacidad de razonamiento del sistema. Cualquier programa de conocimientos escrito en el lenguaje que define el control, podrá ser procesado por el mismo. (Proaño, 2016).

2.6.3. **SISTEMAS DE CONTROL DE ACCESO**

Un Sistema de control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas denominadas como protegidas, es necesario proteger áreas donde solo puede haber personal técnicamente capacitado como salas de energía, desechos peligrosos, etc. O, simplemente, el control de accesos también puede ser utilizado para contener a los obreros empleados en las áreas donde realizan sus tareas, evitando así personas deambulando por sectores donde no deberían estar para no perturbar el normal funcionamiento de una empresa o institución. (Saavedra, 2006).

Un sistema de control de acceso permite controlar el acceso libre y aleatorio a través de puntos de acceso como puertas de seguridad, a zonas específicas en una empresa u oficina, así como formar un registro de los movimientos de cada uno de los usuarios del sistema. Ofrece un método seguro de control mediante tarjetas con banda magnética, tarjetas de identificación por radio frecuencia, mecanismo de identificación por huellas dactilares u otros mecanismos, los cuales llevan almacenada información referente al usuario que la utiliza. (Saavedra, 2006).

Estos sistemas se encargan de a supervisión y control de los puntos de acceso de distintas zonas, registrando las actividades, las cuales pueden ser reportadas posteriormente en informes concisos. (Saavedra, 2006).

Un sistema en una combinación de componentes que actúan conjuntamente y cumplen un determinado objetivo. Si este objetivo es controlar un determinado proceso hablaremos entonces de sistemas de control. Básicamente existen dos clases comunes de sistemas de control, sistemas de lazo abierto y sistemas de lazo cerrado. En los sistemas de control de lazo abierto la salida se genera dependiendo de la entrada; mientras que en los sistemas de lazo cerrado la salida depende de las consideraciones y correcciones realizadas por la retroalimentación. Un sistema de lazo cerrado es llamado también sistema de control con realimentación. Los sistemas de control más

modernos en ingeniería automatizan procesos sobre la base de muchos parámetros y reciben el nombre de controladores de automatización programables. (Saavedra, 2006).

2.6.3.1. Sistema de control de lazo abierto

Es aquel sistema en que solo actúa el proceso sobre la señal de entrada y da como resultado una señal de salida independiente a la señal de entrada, pero basada en la primera. Esto significa que no hay retroalimentación hacia el controlador para que éste pueda ajustar la acción de control. Es decir, la señal de salida no se convierte en señal de entrada para el controlador. (Saavedra, 2006).

- Ejemplo 1: Un tanque con una manguera de jardín. Mientras que la llave siga abierta, el agua fluirá. La altura del agua en el tanque no puede hacer que la llave se cierre y por tanto no nos sirve para un proceso que necesite de un control de contenido o concentración.

Ejemplo 2: Al hacer una tostada, lo que hacemos es controlar el tiempo de tostado de ella misma entrando una variable (en este caso el grado de tostado que queremos). En definitiva, el que nosotros introducimos como parámetro es el tiempo. (Saavedra, 2006).

Estos sistemas se caracterizan por:

- Ser sencillos y de fácil concepto.
- Nada asegura su estabilidad ante una perturbación.
- La salida no se compara con la entrada.
- Ser afectado por las perturbaciones. Estas pueden ser tangibles o intangibles.
- La precisión depende de la previa calibración del sistema. (Saavedra, 2006).

2.6.3.2. Sistema de control de lazo cerrado

Son los sistemas en los que la acción de control está en función de la señal de salida. Los sistemas de circuito cerrado usan la retroalimentación desde un resultado final para ajustar la acción de control en consecuencia. (Pérez, 2007)

El control en lazo cerrado es imprescindible cuando se da alguna de las siguientes circunstancias:

- Cuando un proceso no es posible de regular por el hombre.
- Una producción a gran escala que exige grandes instalaciones y el hombre no es capaz de manejar.
- Vigilar un proceso es especialmente difícil en algunos casos y requiere una atención que el hombre puede perder fácilmente por cansancio o despiste, con los consiguientes riesgos que ello pueda ocasionar al trabajador y al proceso. (Pérez, 2007)

Sus características son:

- Ser complejos, pero amplios en cantidad de parámetros.
- La salida se compara con la entrada y le afecta para el control del sistema.
- Su propiedad de retroalimentación.
- Ser más estable a perturbaciones y variaciones internas. (Pérez, 2007)

Un ejemplo de un sistema de control de lazo cerrado sería el termo tanque de agua que se utiliza para bañarse.

Otro ejemplo sería un regulador de nivel de gran sensibilidad de un depósito. El movimiento de la boya produce más o menos obstrucción en un chorro de aire o gas a baja presión. Esto se traduce en cambios de presión que afectan a la membrana de la válvula de paso, haciendo que se abra más cuanto más cerca se encuentre del nivel máximo. (Pérez, 2007)

2.6.3.3. Clasificación de los sistemas de control según su comportamiento y medición

Control: selección de las entradas de un sistema de manera que los estados o salidas cambien de acuerdo a una manera deseada. Los elementos son:

- Siempre existe para verificar el logro de los objetivos que se establecen en la planeación.
- Medición. Para controlar es imprescindible medir y cuantificar los resultados.
- Detectar desviaciones. Una de las funciones inherentes al control, es descubrir las diferencias que se presentan entre la ejecución y la planeación.
- Establecer medidas correctivas. El objeto del control es prever y corregir los errores.
- Factores de control; Cantidad, Tiempo, costo, Calidad.

Controlador: Es un dispositivo electrónico que emula la capacidad de los seres humanos para ejercer control. Por medio de cuatro acciones de control: compara, calcula, ajusta y limita.

Proceso: operación o desarrollo natural progresivamente continúo, marcado por una serie de cambios graduales que se suceden uno al otro en una forma relativamente fija y que conducen a un resultado o propósito determinados. Operación artificial o voluntaria progresiva que consiste en una serie de acciones o movimientos controlados, sistemáticamente dirigidos hacia un resultado o propósito determinados. Ejemplos: procesos químicos, económicos y biológicos.

Supervisión: acto de observar el trabajo y tareas de otro (individuo o máquina) que puede no conocer el tema en profundidad. (Pérez, 2007)

2.6.3.4. Características de un sistema automático

1. Señal de Corriente de Entrada: Considerada como estímulo aplicado a un sistema desde una fuente de energía externa con el propósito de que el sistema produzca una respuesta específica.
2. Señal de Corriente de Salida: Respuesta obtenida por el sistema que puede o no relacionarse con la respuesta que implicaba la entrada.
3. Variable Manipulada: Es el elemento al cual se le modifica su magnitud, para lograr la respuesta deseada. Es decir, se manipula la entrada del proceso.
4. Variable Controlada: Es el elemento que se desea controlar. Se puede decir que es la salida del proceso.
5. Conversión: Mediante receptores se generan las variaciones o cambios que se producen en la variable.
6. Variaciones Externas: Son los factores que influyen en la acción de producir un cambio de orden correctivo.
7. Fuente de Energía: Es la que entrega la energía necesaria para generar cualquier tipo de actividad dentro del sistema.
8. Retroalimentación: La retroalimentación es una característica importante de los sistemas de control de lazo cerrado. Es una relación secuencial de causas y efectos entre las variables de estado. Dependiendo de la acción correctiva que tome el sistema, este puede apoyar o no una decisión, cuando en el sistema se produce un retorno se dice que hay una

retroalimentación negativa; si el sistema apoya la decisión inicial se dice que hay una retroalimentación positiva.

9. Variables de fase: Son las variables que resultan de la transformación del sistema original a la forma canónica controlable. De aquí se obtiene también la matriz de control habilidad cuyo rango debe ser de orden completo para controlar el sistema. (Gómez, 2005)

2.6.4. **COMPONENTES DE UN SISTEMA DE CONTROL DE ACCESO**

La característica común que tienen una vivienda, una empresa y los lugares de celebración de eventos, es que todos ellos disponen de una puerta de acceso. La misión principal de una puerta es controlar quién puede entrar y quién no; por ejemplo, la puerta de una vivienda permite entrar a los miembros de una familia, en una empresa permite controlar la entrada a los empleados, visitas y mensajeros. Este proceso se llama control de acceso. (Saavedra, 2006)

Los tres componentes básicos de un sistema de Control de Acceso son: la puerta, la cerradura, la llave.

Si se quiere disponer de una seguridad más alta se puede instalar un sensor de puerta en la parte superior de la misma y así conocer el estado de la puerta, de esta forma cualquier situación anormal disparará la alarma y avisará a la empresa de seguridad o a la policía. (Saavedra, 2006)

La gestión administrativa de un control de acceso es de gran laboriosidad.

En un sistema tradicional de bloqueo mecánico, si se añade un nuevo miembro es necesaria una nueva llave, a la vez en la oficina se utilizan relojes de fichar en papel para controlar la asistencia y tiempos de trabajo de los empleados, que hace que el recuento sea laborioso y propicie los errores y omisiones. (Saavedra, 2006)

La introducción de un sistema moderno de control de acceso en red puede simplificar y mejorar el proceso simplemente conectándose a Internet, entrando en el servidor web del sistema, y añadiendo o eliminando los niveles de autorización del personal, tantos como usted desee, y conocer sus condiciones de entrada y salida. Es más, el informe de asistencia y tiempos se puede generar de forma fácil y editarlo con menos mano de obra y mayor precisión. (Saavedra, 2006)

Teniendo en cuenta la tendencia actual en el crecimiento de las empresas, es común que una empresa tenga delegaciones en distintas partes de la ciudad o del país. Esta es la razón por la que se necesita un servicio de sincronización de datos. La creación de redes de sistemas de control de acceso proporciona una buena solución para gestionar y controlar las filiales desde la oficina central, ajustando los días libres en cada una o las horas de trabajo de una manera más eficiente y cómoda, por lo que supera sobradamente a los sistemas tradicionales de control de acceso mecánico. (Saavedra, 2006)

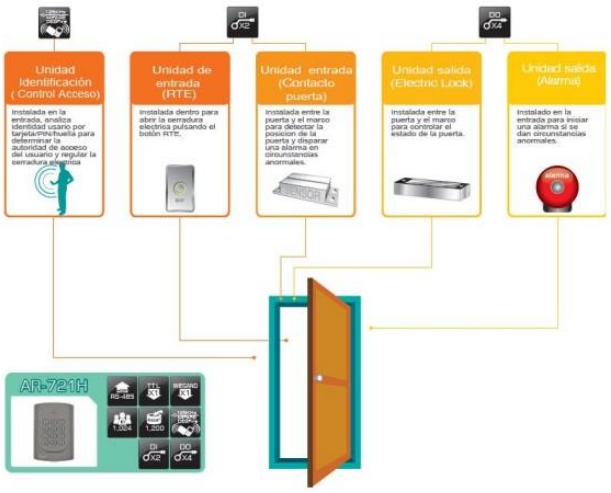


FIGURA Nº 1: Componentes del sistema de control de ingreso
FUENTE: (I. B. Isidro)

Las partes de las que consta un sistema de control de accesos van en función del tipo de sistema de control de accesos que se disponga, estas son las siguientes:

- **Lector/ terminal:** es el dispositivo que adquiere la información para identificar a la persona que desea ganar el acceso. Éste se comunica con una credencial y envía su información al controlador para determinar el permiso de acceso, en el caso de sistemas autónomos la información la posee el terminal, no necesita comunicarse con el controlador. Existen diversos tipos de dispositivos, cada uno con sus propias características. (Saavedra, 2006)

- **Credencial:** es lo que identifica a una persona y de la que se requiere información para obtener el acceso a las zonas permitidas. Puede definirse como algo que una persona posee, sabe o es. Podrían ser códigos de seguridad, parámetros biométricos, tarjetas, etc.

- **Servidor:** normalmente es un PC que se encarga de almacenar la información de cada intento de acceso, sea exitoso o no, para llevar un registro. Además es la unidad donde se ejecutan las instrucciones de los programas. En el caso de los sistemas autónomos no necesitan el servidor para funcionar, sino que el que almacena la información es el terminal directamente.

- **Controlador:** es el único elemento encargado de decidir a quienes se les permite el acceso, a qué zonas y en qué momentos. Todos los demás elementos solo generan información o ejecutan acciones. También es función del controlador comunicarse con el servidor que concentra la información del sistema en general, tanto la información de configuración y programación como la de eventos producidos. Es consultado en cada intento de ingreso.

- **Mecanismo de apertura:** Cuando se determina que el usuario tiene permiso de acceso, se le debe permitir el ingreso, normalmente mediante la apertura de una puerta. Esto suele hacerse mediante la activación de contactos magnéticos o pulsores eléctricos, según la aplicación.

- **Elementos de alimentación:** no todos los elementos electrónicos que forman parte de un sistema de control de accesos están alimentados a la misma tensión, por lo que se hacen necesarios elementos que alimenten dichos dispositivos de una manera independiente.

Este Trabajo Final de Grado se va a centrar en las partes de un control de accesos automático y personal. En concreto se van a ver los componentes de un sistema con conexión a un ordenador.

Las cuales son: lector biométrico ZKTeco, chapa magnética de puerta biométrica L700, servidor del sistema, controlador, mecanismo de apertura y elementos de alimentación. (Saavedra, 2006)

2.6.5. **SISTEMA BIOMETRICO**

Según (T. B. Cesar), Un sistema biométrico en general consta de componentes tanto hardware como software necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen

principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

Para cada uno de estos sistemas se ha descrito su funcionamiento y algunas de las técnicas que se utilizan para procesar los datos obtenidos a partir de los sensores.

Los sistemas biométricos se han desarrollado como respuesta a la creciente demanda de seguridad existente en la actualidad y aunque algunos de ellos son altamente fiables, ningún sistema es efectivo al 100%, y estos sistemas también son susceptibles de ser engañados. (Tolosa, 2009)

2.6.5.1. Biometría

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos. (Delgado, 2011)

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, geometría de la mano, reconocimiento visual y otras técnicas. (Delgado, 2011)

De esta forma con los sistemas biométricos que reconocen las características singulares de las huellas digitales, por ejemplo, se logra evitar fraudes en la banca, en el sistema de salud por suplantación de pacientes, controlar el acceso en el desplazamiento de seres humanos al interior de las empresas, tiempos desperdiciados, accesos no deseados; sin necesidad de utilizar contraseñas, carnes, tarjetas magnéticas u otros medios de identificación vulnerables. Esto hace que los sistemas biométricos sean el medio más rápido y seguro mediante la utilización de la huella digital como validador de operaciones y de control de acceso. (Delgado, 2011)

2.6.5.2. Funcionamiento de un sistema biométrico

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad. (Moreno, 2017)

La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas, passwords, pin numbers, códigos u otros que sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos. (Moreno, 2017)

La identificación biométrica es utilizada para verificar la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física y comparando esas medidas con aquéllas de la misma persona guardadas en archivo en una base de datos o algunas veces en una tarjeta inteligente que lleva consigo la misma persona. Las características físicas utilizadas son huellas digitales, huellas de la voz, geometría de la mano, el dibujo de las venas en la articulación de la mano y en la retina del ojo, la topografía del iris del ojo, rasgos faciales y la dinámica de escribir una firma e ingresarla en un teclado. (Moreno, 2017)

El funcionamiento de estos sistemas implica de la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje. Éstas son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptografía se limita a un uso secundario como

el cifrado de los datos biométricos almacenados en la base de datos o la trasmisión de los mismos. (Moreno, 2017)

Los escáners de huellas digitales y equipos de medición de geometría de la mano son los dispositivos más corrientemente utilizados. Independiente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico. (Moreno, 2017)

2.6.5.3. Sensores biométricos

En lo que a sensores para sistemas biométricos se refiere, aunque hay diferentes fabricantes, hablando en términos generales se utiliza el mismo sistema de captación de la característica deseada, es decir, para reconocimiento de iris se emplea una cámara o para reconocimiento de voz un micrófono. El único campo donde parece existir una mayor variedad de métodos es en el de captación de huella dactilar. (Giz, 2012)

A continuación se muestran diferentes tipos de sensores:

Sensores Ópticos

El método óptico es uno de los más comunes que suele estar formado por cámaras de vídeo de tipo CCD. Estos sensores se emplean tanto en reconocimiento de huella dactilar como de ojo.

El corazón de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada). Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI. (Giz, 2012)

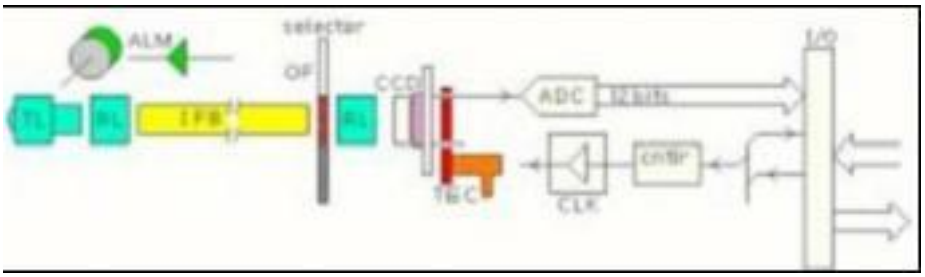


FIGURA Nº 2: Diagrama del circuito integrado
FUENTE: (I. B. Isidro)

Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la cámara), almacenando una pequeña carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y

verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo. (Giz, 2012)

Sensores Termoeléctricos

El sensor termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip para reconocimiento de huella dactilar.

El Fingerchip utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris. (Giz, 2012)

El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huellas dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua. (Giz, 2012)

Además, también cuenta con la ventaja de auto limpiado del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta calidad y siempre un sensor limpio. La desventaja es que la cualidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente. (Giz, 2012)

Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona. (Giz, 2012)

Sensores Capacitivos

El método capacitivo es uno de los más populares para reconocimiento de huella dactilar. Al igual que otros escáner, genera una imagen de las cresta y valles del dedo. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato. (Giz, 2012)

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor, tendremos un efecto de solapamiento sobre los platos (píxel) vecinos, lo que provocará que el área sensor aumente de tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen. (Giz, 2012)

Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos óptimas en la piel. Cuando el dedo está sucio, con frecuencia no existirá aberturas de aire en valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento. (Giz, 2012)

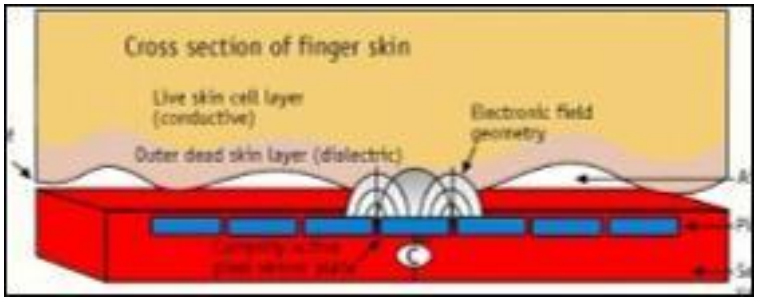


FIGURA Nº 3: Sensores capacitivos
FUENTE: (I. B. Isidro)

Entre las empresas líderes en este sector se encuentran: Infineon, Verdicom, Sony y ST Microelectronics.

Sensores E-Field (de Campo Eléctrico)

El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del "mundo real", como por ejemplo piel húmeda, seca o dañada. (Giz, 2012)

Esta tecnología para reconocimiento de huella dactilar origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador under-píxel para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podría. (Giz, 2012)

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma. (Giz, 2012)

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Desde hace poco existe también un sensor más fuerte basado en esta tecnología que saldrá al mercado en pocos meses. (Giz, 2012)

Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

Sensores sin contacto

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras

se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico con la correspondiente distorsión de la imagen. Otro punto es que las huellas escaneadas son esféricas lo que origina un complejo algorítmico mucho más complejo. (Giz, 2012)

Micrófonos ópticos unidireccionales

La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada. (Giz, 2012)

Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido. Es utilizado en reconocimiento de voz. (Giz, 2012)

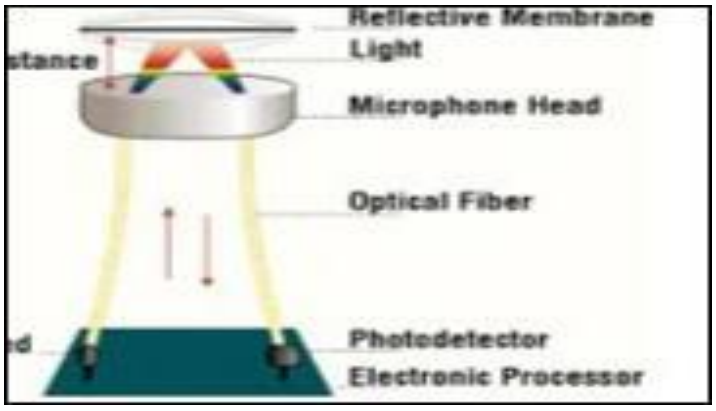


FIGURA Nº 4: Micrófono óptico unidireccionales
FUENTE: (I. B. Isidro)

2.6.5.4. Procesamiento de la información

Aunque estos dispositivos se basan en tecnologías muy diversas, si se consideran de forma genérica se puede considerar un sistema biométrico genérico de identificación, dividido en cinco subsistemas: recolección de datos, transmisión, procesado de señal, decisión y almacenamiento de datos. (Giz, 2012)

La siguiente figura muestra de manera esquemática estos cinco subsistemas y como se relacionan entre sí:

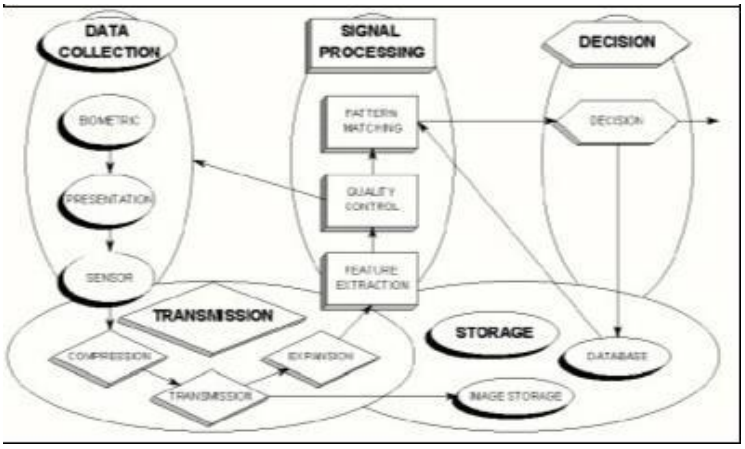


FIGURA Nº 5: Procesamiento de la información
FUENTE: (I. B. Isidro)

2.6.5.5. Recolección De Datos

Los sistemas biométricos comienzan con la medida de una característica del comportamiento o fisiológica. La clave de todos los sistemas es la hipótesis subyacente que la característica biométrica medida es distintiva entre los individuos y en un cierto plazo repetible para el mismo individuo. (Giz, 2012)

Es decir, las características deben variar en gran magnitud entre individuos, pero deben variar muy poco para cada individuo de medida a medida. Los problemas en medir y controlar estas variaciones comienzan en el subsistema de la colección de datos. La característica del usuario se debe presentar a un sensor. Según lo observado ya, la presentación de la característica biométrica al sensor introduce un componente del comportamiento. (Giz, 2012)

Los cambios inevitables en el comportamiento afectarán la capacidad de repetición y la distinción de la medida.

Si un sistema pretende ser abierto, presentación y sensor deben ser estandarizados para asegurar que la característica biométrica recogida sea la misma que recogería otro sistema para el mismo individuo. (Giz, 2012)

2.6.5.6. Transmisión

Algunos, pero no todos, los sistemas biométricos recogen datos en una localización pero se almacenan y/o procesan en otra. Tales sistemas requieren la transmisión de datos. Si está

implicada una gran cantidad de datos, la compresión es fundamental, a fin de requerir poco ancho de banda y poco espacio para su almacenamiento.

El cuadro anterior muestra la compresión y la transmisión que ocurren antes de procesar de señal y del almacenamiento de la imagen. (Giz, 2012)

En tales casos, los datos comprimidos transmitidos o salvados se deben descomprimir antes de que sean usados. El proceso de la compresión y de la descompresión causa generalmente pérdida de la calidad en la señal restablecida.

La técnica de compresión usada dependerá de la señal biométrica. Un campo de investigación interesante consiste en encontrar, para una técnica biométrica dada, métodos de la compresión con impacto mínimo en el subsistema del proceso de señal. Si un sistema es abierto, los protocolos de la compresión y de la transmisión deben ser estandardizados de modo que cada usuario de los datos pueda reconstruir (aunque con pérdida de la calidad) la imagen original.

Los estándares existentes actualmente son: para la compresión de la huella digital (WSQ), de las imágenes faciales (JPEG), y de los datos de la voz (CELP). (Giz, 2012)

2.6.5.7. Procesado De Señal

Adquirida y transmitida una característica biométrica, debemos prepararla para corresponder con otra. El cuadro anterior divide el subsistema de proceso de señal en tres tareas: extracción, control de calidad, y concordancia con el modelo.

La primer meta es analizar el modelo biométrico verdadero de la presentación y las características del sensor, en presencia de las pérdidas por ruido y de señal impuestas por la transmisión. (Giz, 2012)

La segunda meta, es preservar el modelo biométrico para que esas calidades que sean distintivas y repetibles, y desechar las que no lo sean, o sean redundantes.

En un sistema de reconocimiento de la voz, se deseará encontrar las características, tales como los lazos armónicos en las vocales, que dependen solamente del hablante y no de las palabras que son habladas. (Giz, 2012)

Y, desearemos centrarnos en esas características que deberán ser invariantes incluso si el hablante está resfriado o no está hablando directamente en el micrófono.

Hay muchos acercamientos matemáticos para realizar estos procesos. En general, la extracción de la característica es una forma de compresión irreversible, significando esto que la imagen biométrica original no se puede reconstruir de las características extraídas.

En algunos sistemas, la transmisión ocurre después de la extracción de la característica para reducir el requisito de mínimo ancho de banda. (Giz, 2012)

Después de la extracción de la característica, o quizá antes o durante, desearemos controlar si la señal recibida del subsistema de colección de datos tiene la calidad requerida, a fin de solicitar si es necesario una nueva muestra del usuario.

El desarrollo de este proceso de "control de calidad" ha mejorado sensiblemente el funcionamiento de los sistemas biométricos en los últimos años.

El propósito del proceso de concordancia con el modelo es comparar una muestra actual con la característica de una muestra salvada, llamada un modelo, y enviar al subsistema de decisión la medida cuantitativa de la comparación. (Giz, 2012)

Las distancias raramente, serán fijadas en cero, pues siempre habrá alguna diferencia relacionada con el sensor o relacionada con el proceso de transmisión o con el comportamiento propio del usuario.

2.6.5.8. Decisión

La política del sistema de decisión dirige la búsqueda en la base de datos, y determina los "matching" o los " no-matching" basándose en las medidas de la distancia recibidas de la unidad de procesado de señal. (Giz, 2012)

Este subsistema toma en última instancia una decisión de "acepta/rechaza" basada en la política del sistema. Tal política podría ser declarar un "matching" para cualquier distancia más baja que un umbral fijo y "validar" a un usuario en base de este solo "matching", o la política podría ser declarar un "matching" para cualquier distancia más baja que un umbral dependiente del usuario, variante con el tiempo, o variable con las condiciones ambientales.

Una política posible es considerar a todos los usuarios por igual y permitir sólo tres intentos con una distancia alta para el "matching" para luego volver una medida baja de la distancia.

La política de decisión empleada es una decisión de la gerencia que es específica a los requisitos operacionales y de la seguridad del sistema. En general, bajar el número de no-matching falsos se puede negociar contra levantar el número de matching falsos. (Giz, 2012)

La política óptima del sistema depende de las características estadísticas de las distancias de comparación que vienen de la unidad de "matching " del modelo y de las penas relativas para el matching falso y el no-matching falso dentro del sistema.

En cualquier caso, en la prueba de dispositivos biométricos, es necesario evaluar el funcionamiento del subsistema de procesado de señal con independencia de las políticas puestas en ejecución mediante el subsistema de decisión. (Giz, 2012)

2.6.5.9. Almacenamiento

El subsistema restante que se considerará es el del almacenamiento. Habrá una o más formas de almacenamiento a usar, dependiendo del sistema biométrico. Los modelos de la característica serán salvados en una base de datos para la comparación en la unidad de matching. (Giz, 2012)

Para los sistemas que realizan solamente una correspondencia "uno a uno", la base de datos se puede distribuir en las tarjetas magnéticas llevadas por cada usuario. Dependiendo de la política del sistema, no es necesaria ninguna base de datos centralizada.

Aunque, en esta aplicación, una base de datos centralizada se puede utilizar para detectar tarjetas falsificadas o para reeditar tarjetas perdidas sin recordar el modelo biométrico. (Giz, 2012)

Los requisitos de velocidad del sistema dictan que la base de datos esté repartida en subconjuntos más pequeños, tales que cualquier muestra de la característica necesita solamente ser correspondida con la de los modelos salvados en una partición. Esta estrategia tiene el efecto de aumentar velocidad del sistema y de disminuir matching falsos a expensas de aumentar la tasa de no-matching falsos. Esto significa que las tasas de error del sistema no son constantes con el aumento del tamaño de la base de datos y, además, esta relación no es lineal. (Giz, 2012)

Por lo tanto, las estrategias para particionar la base de datos representan una decisión bastante compleja.

Si existe la posible necesidad de reconstruir los modelos biométricos a partir de los datos salvados, será necesario el almacenamiento de datos sin procesar.

El modelo biométrico, en general, no es reconstituible a partir de los datos salvados. Además, los modelos son creados usando algoritmos propietarios de extracción de características, propios de cada fabricante. (Giz, 2012)

El almacenamiento de informaciones en bruto permite cambios en el sistema o de equipamiento sin que sea necesario registrar nuevamente a todos los usuarios.

Estos cinco pasos se refieren a la captación y verificación de una característica biométrica determinada de una persona pero para que el sistema sea capaz de verificar dicha característica es necesario un paso previo a estos cinco en el que la persona debe registrarse en el sistema ("enroll en inglés"). Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como, por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia ("reference template" en inglés.) El modelo de referencia debe ser guardado en una base de datos, una tarjeta inteligente ("smart card" en inglés), o en algún otro lugar del cual será extraído en cualquier ocasión futura para realizar la verificación. (Giz, 2012)

A pesar de que es poco probable obtener dos tomas iguales aún del mismo individuo, a causa de diferencias ambientales y otras condiciones en el momento de la captura, el sistema aún debe poder funcionar correctamente. La mayoría de los algoritmos de comparación generan un ámbito para cada ensayo de comparación el cual es cotejado dentro de determinados umbrales antes de ser aceptados o rechazados. (Giz, 2012)

Es en este punto donde entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él. (Giz, 2012)

Cada proveedor de tecnología biométrica configura la falsa aceptación, rechazo de forma diferente.

La figura siguiente muestra esta relación de compromiso.

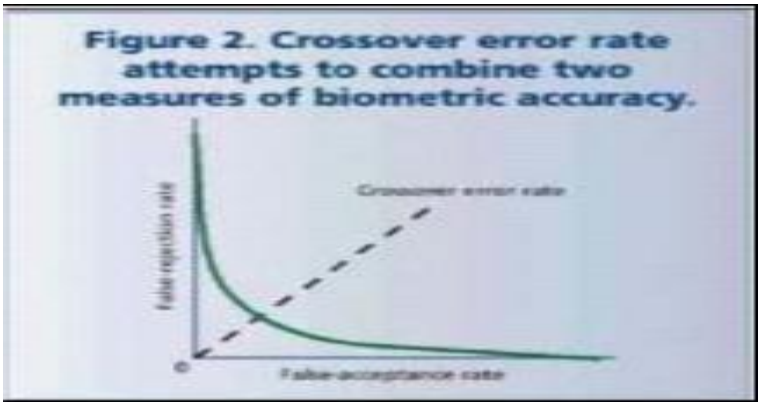


FIGURA Nº 6: Características básicas de fiabilidad del sistema biométrico
FUENTE: (I. B. Isidro)

Como puede observarse, si el umbral es demasiado bajo, se vuelve demasiado fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas. (Giz, 2012)

2.6.5.10. Clasificación de los sistemas biométricos

Aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento (por ejemplo la medición de la biometría basada en huella digital variará de acuerdo a la manera en que se coloca el dedo), la clasificación de las técnicas biométricas facilita su estudio. La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo. (Rosales, 2009)

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual. (Rosales, 2009)

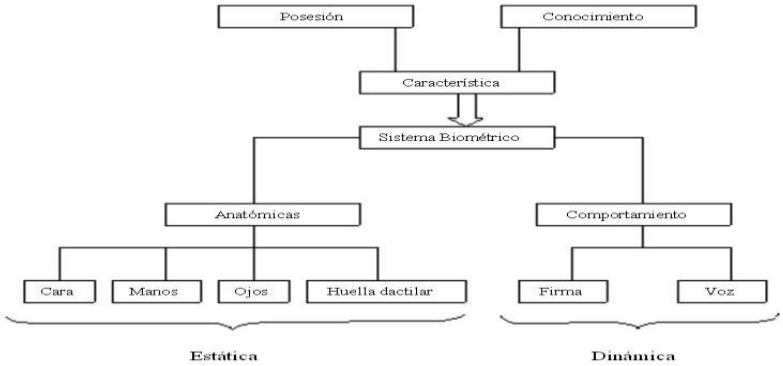


FIGURA Nº 7: Clasificación de los sistemas biométricos
FUENTE: (I. B. Isidro)

Sin tener en cuenta la clasificación anterior, las técnicas biométricas se pueden clasificar atendiendo a cuál es la característica observada y aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mesurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en seis grandes grupos: (Rosales, 2009)

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

Cada sistema biométrico utiliza una cierta clase de interfaz para recopilar la información sobre la persona que intenta acceder. Un software especializado procesará esa información en un conjunto de los datos que se pueden comparar con los modelos de los usuarios que se han introducido previamente al sistema. Si se encuentra un "matching" con la base de datos, se confirma la identidad de la persona y se concede el acceso. (Rosales, 2009)

En la siguiente tabla se muestra una comparativa de sus rasgos más generales:

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándars	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 1997 (USD)	5000	5000	1200	2100	1000	1200

TABLA Nº 1: Comparación de los rasgos más generales
FUENTE: (I. B. Isidro)

2.6.6. **BIOMETRÍA ESTÁTICA**

2.6.6.1. **Huella dactilar**

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. (Delgado, 1996)

Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella. (Delgado, 1996)

FIGURA Nº 8: Huella dactilar
FUENTE: (I. B. Isidro)

2.6.6.2. Identificando patrones

A simple vista, el patrón que siguen las líneas y surcos de una huella se puede clasificar según tres rasgos mayores: arco, lazo y espiral. Cada dedo presenta al menos una de estas características. Por otro lado, en determinados puntos las líneas de la huella dactilar se cortan bruscamente o se bifurcan. Estos puntos reciben el nombre de minucias, y juntos suman casi el 80% de los elementos singulares de una huella. (Delgado, 1996)

FIGURA Nº 9: Identificación de patrones
FUENTE: (I. B. Isidro)

Todo esto da lugar a un patrón complejo único para cada individuo, distinto incluso en gemelos idénticos. En concreto, se estima que la probabilidad de que dos personas tengan las mismas huellas dactilares es aproximadamente de 1 en 64.000 millones. (Delgado, 1996)

Cuando se digitaliza una huella, los detalles relativos a las líneas (curvatura, separación), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten obtener un índice numérico correspondiente a dicha huella. En el momento en que un usuario solicita ser identificado, coloca su dedo sobre un lector (óptico, de campo eléctrico, por presión) y su huella dactilar es escaneada y analizada con el fin de extraer los elementos característicos y buscar su homóloga en la base de datos. El resultado es un diagnóstico certero en más del 99% de los casos. (Delgado, 1996)

Las técnicas utilizadas para la comparación de la huella dactilar se pueden clasificar en dos categorías:

La técnica de puntos Minucia primero encuentran estas minucias y posteriormente procede a su colocación relativa en el dedo. (Delgado, 1996)

Es difícil extraer los puntos de las minucias exactamente cuando la huella dactilar es de baja calidad. También este método no considera el patrón global de crestas y de surcos.

El método correlación puede superar algunas de las dificultades de la comparación por puntos Minucia; sin embargo, tiene algunos inconvenientes propios. Las técnicas de correlación requieren una localización precisa de un punto de registro y se ve afectada por el desplazamiento y rotación de la imagen. (Delgado, 1996)

2.6.6.3. Clasificación de la Huella

La clasificación de las huellas dactilares es una técnica consistente en asignar a una huella uno de los varios tipos previamente especificados en la literatura y registrarla con un método de indexación de las direcciones. Una huella dactilar de entrada es primeramente clasificada a un nivel grueso en uno de los tipos: (Peralta, 2012)

- Whorl
- Lazo derecho
- Lazo izquierdo
- Arco
- Tented el arco

Entonces, en un nivel más fino, se compara con el subconjunto de la base de datos que contiene solamente ese tipo de huella dactilar. Se utilizan algoritmos desarrollados para identificar a cuál de estos tipos le pertenece una huella en concreto. (Peralta, 2012)

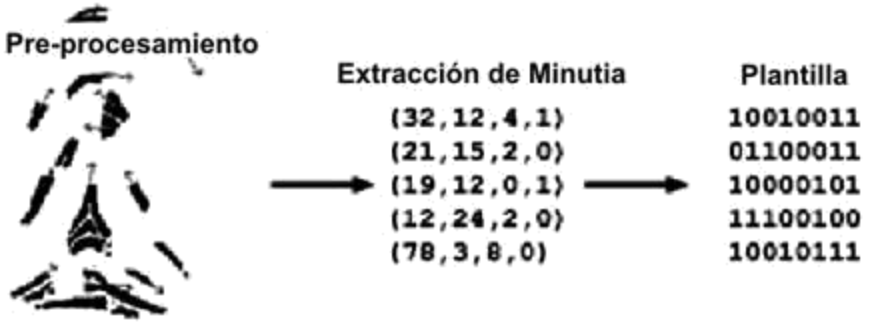


FIGURA Nº 10: Algoritmos desarrollados para identificar una huella
FUENTE: (I. B. Isidro)

2.6.6.4. Realce de la Huella

Un paso crítico en la clasificación automática de la huella dactilar está en extraer mediante un algoritmo las minucias de las imágenes de la huella dactilar de la entrada. El funcionamiento de un algoritmo de extracción de las minucias confía totalmente en la calidad de las imágenes de la huella dactilar de la entrada. Para asegurarse de que el funcionamiento de un sistema automático de identificación/verificación de huella dactilar sea robusto con cierta independencia de la calidad de las imágenes de la huella dactilar, es esencial incorporar un algoritmo del realce de la huella dactilar en el módulo de la extracción de las minucias. De este modo se puede mejorar de forma adaptativa la claridad de las estructuras de la cresta y del surco de las imágenes de las huella dactilares de entrada. (Peralta, 2012)

2.6.6.5. Reconocimiento de iris

El iris es una membrana coloreada y circular que separa la cámara anterior y posterior del ojo. Posee una apertura central de tamaño variable, la pupila. Las fibras musculares del iris la constituyen dos músculos, el esfínter del iris y el dilatador de la pupila. (Peralta, 2012)

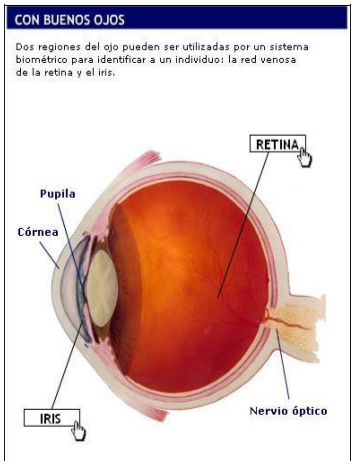


FIGURA Nº 11: Reconocimiento del iris
FUENTE: (I. B. Isidro)

El iris está constantemente activo permitiendo así a la pupila dilatarse (midriasis) o contraerse (miosis). Está función tiene su objetivo en la regulación de la cantidad de luz que llega a la retina.

Se trata de la estructura indivisible del cuerpo humano más distintiva matemáticamente. En sus 11 milímetros de diámetro cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar. (Peralta, 2012)

Hay que tener en cuenta que el iris no cambia a lo largo de la vida, y que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes. Asimismo, se trata de un órgano interno protegido -por la córnea y el humor acuoso- pero visible externamente a una distancia de hasta un metro. Las lentes de contacto y las gafas no afectan a la identificación. Y, por si todo esto fuera poco, los sistemas basados en el reconocimiento de iris son veinte veces más rápidos que cualquier otro sistema biométrico. (Peralta, 2012)

2.6.6.6. Funcionamiento

El procedimiento, base de los dispositivos actuales, resulta extraordinariamente sencillo. Basta con colocarse frente a una cámara, con los ojos correctamente alineados en su campo de visión. La cámara genera una imagen que es analizada por medio de los algoritmos de

Daugman para obtener el Iris Code personal, un patrón único del iris que apenas ocupa 256 bytes de información. Tan reducido tamaño permite una rápida búsqueda de su homólogo en una base de datos hasta identificar a su propietario. (Peralta, 2012)

Para la codificación del patrón del iris, usualmente se realiza una conversión de la imagen del iris de coordenadas cartesianas a polares para facilitar la extracción de información, al pasar de una forma circular a una rectangular. A la nueva representación, se le aplican filtros multicanal, ya sean de Gabor, Fourier o Wavelet, para extraer los coeficientes que finalmente conformaran el código del iris. (Peralta, 2012)

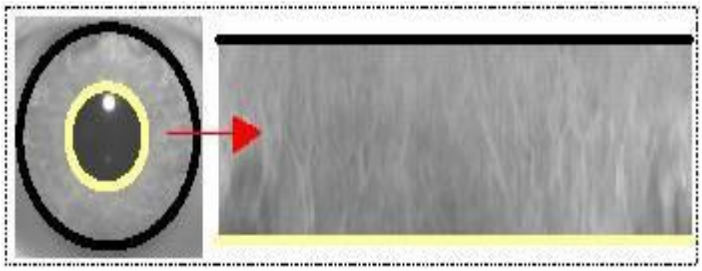


FIGURA Nº 12: Conversión de la imagen del iris
FUENTE: (I. B. Isidro)

2.6.6.7. Geometría de la mano

La forma de la mano puede ser de gran valor en biometría. A diferencia de las huellas dactilares, la mano humana no es única, y sus características individuales no son suficientes para identificar a una persona. Sin embargo, su perfil resulta útil si el sistema biométrico lo combina con imágenes individuales de algunos dedos, extrayendo datos como las longitudes, anchuras, alturas, posiciones relativas, articulaciones,… Estas características se transforman en una serie de patrones numéricos que pueden ser comparados. Su principal aplicación es la verificación de usuario. (Zuleta, 2015)

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser. (Zuleta, 2015)

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura.

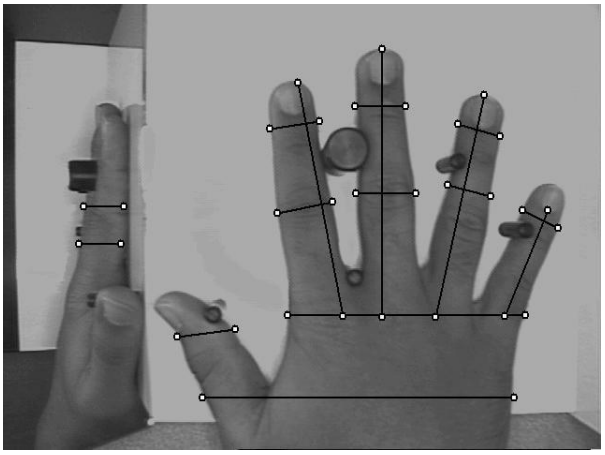


FIGURA Nº 13: Conversión de la imagen del iris
FUENTE: (I. B. Isidro)

Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones. (Zuleta, 2015)

No es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez. (Zuleta, 2015)

2.6.6.8. Reconocimiento Facial Escáner de Rostro

Un sistema de reconocimiento facial es una aplicación dirigida por ordenador para identificar automáticamente a una persona en una imagen digital mediante la comparación de determinadas características faciales en la imagen y en la base de datos facial. (Correa, 2013)

El reconocimiento facial automatizado es relativamente un concepto nuevo. Desarrollado en los años 60, el primer sistema semiautomático para reconocimiento facial requería del administrador para localizar rasgos (como ojos, orejas, nariz y boca) en las fotografías antes de que este calculara distancias a puntos de referencia en común, los cuales eran comparados luego con datos de referencia. (Correa, 2013)

El método más común utiliza una cámara para capturar una imagen de nuestra cara, que es analizada en función de ciertos 'puntos clave', como la distancia entre los ojos o la anchura de la nariz.

2.6.6.9. Funcionamiento

El primer paso en el reconocimiento facial es la adquisición de una imagen real o una imagen bidimensional del objetivo. El sistema determina la alineación de la cara basándose en la posición de la nariz, la boca, etc. En una imagen en 2D no debe estar más desplazada de 35 grados. Después de la alineación, orientación y ajuste de tamaño, el sistema genera una plantilla facial única (una serie de números) de modo que pueda ser comparada con las de la base de datos. (Correa, 2013)

FIGURA Nº 14: Reconocimiento facial
FUENTE: (I. B. Isidro)

Un factor importante en los sistemas de reconocimiento facial es su capacidad para distinguir entre el fondo y la cara. El sistema hace uso de los picos, valles y contornos dentro de un rostro (los denominados puntos duros del rostro) y trata a estos como nodos que puedan medirse y compararse contra los que se almacenan en la base de datos del sistema. Hay aproximadamente 80 nodos en un rostro de los que el sistema hace uso (entre ellos se incluye el largo de la línea de la mandíbula, la profundidad de los ojos, la distancia entre los ojos, la forma del pómulo, la anchura de la nariz). (Correa, 2013)

Los nuevos sistemas de reconocimiento facial hacen uso de imágenes tridimensionales, y por lo tanto son más precisos que sus predecesores. Al igual que en los sistemas de reconocimiento facial en dos dimensiones, estos sistemas hacen uso de distintas características de un rostro humano y las utilizan como nodos para crear un mapa del rostro humano en tres dimensiones de la cara de una persona. Empleando algoritmos matemáticos similares a los utilizados en búsquedas de Internet, la computadora mide las distancias entre determinados puntos de la muestra en la superficie del rostro. Estos sistemas en 3D tienen la capacidad de reconocer una cara incluso cuando se encuentra girada 90 grados. Por otra parte, no se ven afectados por las diferencias en la iluminación y las expresiones faciales del sujeto. (Correa, 2013)

2.3.6.1.0. Otros sistemas de reconocimiento facial

Ciertos softwares interpretan cada imagen facial como un conjunto bidimensional de patrones brillantes y oscuros, con diferentes intensidades de luz en el rostro. Estos patrones, llamados eigenfaces, se convierten en un algoritmo que representa el conjunto de la fisionomía de cada individuo. Cuando un rostro es escaneado para su identificación, el sistema lo compara con todas las eigenfaces guardadas en la base de datos. (Correa, 2013)

Este tipo de sistemas está sujeto a limitaciones, como las condiciones ambientales en el momento de capturar la imagen. Así, aunque normalmente interpreta correctamente los cambios de luz en interiores, su funcionamiento al aire libre, con luz natural, es todavía una asignatura pendiente. También la posición de la cabeza y la expresión del rostro pueden influir en el "veredicto". (Correa, 2013)

2.6.6.10. Reconocimiento del Retina

La retina es la capa más interna de las tres capas del globo ocular. Es el tejido sensible a la luz (fotorreceptor) que se encuentra en la parte posterior interna del ojo y actúa como la película en una cámara: las imágenes pasan a través del cristalino del ojo y son enfocadas en la retina. La retina convierte luego estas imágenes en señales eléctricas y las envía a través del nervio óptico al cerebro. (Correa, 2013)

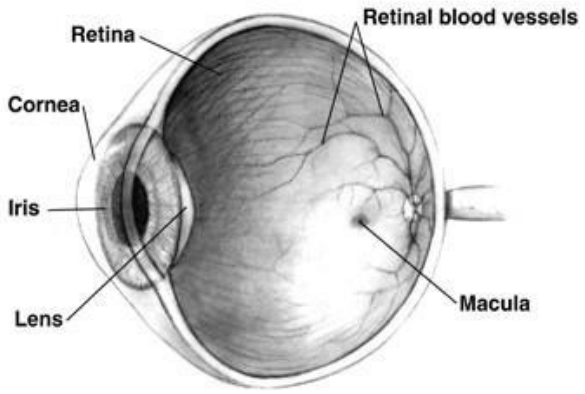


FIGURA Nº 15: Reconocimiento de retina
FUENTE: (I. B. Isidro)

Los sistemas basados en las características de la retina analizan la capa de vasos sanguíneos localizados en la parte posterior del ojo.

FIGURA Nº 16: Reconocimiento de retina
FUENTE: (I. B. Isidro)

Esta técnica requiere del uso de una fuente de luz de baja intensidad para desvelar el modelo único de la retina (irrepetible en otros individuos, como las propias huellas digitales), lo que le convierte en una de las más seguras tecnologías biométricas de "identificación" de individuos. El

escaneo retinal puede ser sumamente preciso pero requiere que el usuario mire en un receptáculo y enfoque la vista hacia un punto específico, lo que redunda en un proceso intrusivo y un contacto cercano con el dispositivo de lectura. Su uso no resulta conveniente cuando se utiliza lentes.

El lector escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso. (Correa, 2013)

2.6.6.11. Acceso Físico

En la actualidad, la mayor aplicación de la biometría se produce en la seguridad física, para controlar el acceso a zonas restringidas.

2.6.7. BIOMETRIA DINÁMICA

2.6.7.1. Dinámica del tecleo

El principal mecanismo de interacción de una persona con un ordenador es el teclado. Uno de los dispositivos de comportamiento biométrico es el análisis "key-stroke", también llamado "typing biometrics". Este último comportamiento biométrico se refiere a la velocidad con que un individuo emplea el teclado para introducir su identificación o User ID y su clave de acceso o password, lo cual puede ser indicativo de la autenticidad del usuario. (Delgado, 2006)

En la actualidad, la utilización de este método se vincula, fundamentalmente, a la seguridad informática y, concretamente, al uso de Internet, para aplicaciones de comercio electrónico.

Los antecedentes históricos de esta dinámica de tecleo se hallan en los primeros sistemas de telégrafos de los EE.UU., en los que se comenzó a observar la capacidad de los operadores para identificarse entre sí, en diferentes estaciones, gracias al ritmo de las pulsaciones del código morse que cada uno de ellos generaba al transmitir mensajes codificados. (Delgado, 2006)

2.6.7.2. Adquisición

Una muestra del tecleo en biometría está representada por el conjunto de información que un ordenador puede capturar de una secuencia de teclas pulsadas por un usuario en el teclado de una PC. En el momento de la captura de la muestra, se tendrá en cuenta:

- Tiempo entre pulsaciones (latencias): se mide el intervalo entre la pulsación de una tecla y la siguiente, dentro de una determinada secuencia de tecleo.
- Tiempo de pulsaciones (duraciones): en una pulsación específica, se mide cuánto tiempo se mantiene presionada una tecla.
- Una vez obtenidas la latencia y la duración en el tecleo, se hace un patrón estadístico y se determina una firma de tecleo para cada usuario.

Ventajas

- Bajo costo.
- No requiere de equipamiento especial.
- No es intrusivo en absoluto.
- Puede cargar un alto número de usuarios en el sistema.

Desventajas

- No es muy utilizado en el mercado.
- FA y FR son de 0,1%, pero debe complementarse con el sistema de ID y password.

Está sujeto a alteraciones de los usuarios por lesiones sufridas en las manos. (Delgado, 2006)

2.6.7.3. Firma manuscrita

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además de la forma de firmar, las características dinámicas (por eso se les suele denominar

Dynamic Signature Verification, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo. (Delgado, 2006)

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente.

Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decrementa su seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). (Delgado, 2006)

La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

Por lo tanto, en lo referente al reconocimiento de firma, existen dos líneas de investigación claramente diferenciadas: reconocimiento de firma estática (off-line) y reconocimiento de firma dinámica (on-line). La principal diferencia entre ambas líneas radica en la información de firma de partida para el reconocimiento. (Delgado, 2006)

2.6.7.4. Propiedades magnéticas

Otro dispositivo que se puede utilizar para el reconocimiento y validación de firmas es el basado en propiedades magnéticas de alambres amorfos. Estos alambres tienen la capacidad de cambiar su magnetización cuando están sujetos a esfuerzos pequeños de compresión-tensión, por lo que pueden usarse como transductores magneto elásticos de este tipo de esfuerzos a señales eléctricas. (Delgado, 2006)

El dispositivo consiste en una pluma convencional entre cuya punta y base se sujeta el alambre amorfo. El arreglo incluye una pequeña bobina de inducción, la cual detecta los cambios de magnetización producidos por los movimientos de la mano del firmante al ejecutar su rúbrica (esfuerzos de tensión-compresión), generándose así una señal eléctrica

manejable. El reconocimiento de la firma consiste de tres etapas: adecuación, entrenamiento y reconocimiento; cada una de ellas involucra tanto electrónica analógica como digital.

En la etapa de adecuación, la señal se filtra, se amplifica y se homogeniza el nivel de las componentes espectrales de la señal dentro del ancho de banda en estudio. Posteriormente se digitaliza la señal empleando un convertidor A/D y un filtro digital de preénfasis. (Delgado, 2006)

Asimismo, se caracteriza el ruido de fondo para tener una referencia que determine la parte de la señal que pertenece a la firma, obteniéndose así umbrales de energía que indican el momento para comenzar a digitalizar la señal. En la etapa de entrenamiento se digitaliza varias veces un mismo tipo de firma y se guardan en archivos para análisis posterior. Este análisis consiste en la extracción de patrones de la señal, mediante técnicas como la autocorrelación, análisis de predicción lineal, segmentación y cuantificación vectorial. (Delgado, 2006)

De esta forma se obtienen los prototipos o centroides de la firma en estudio, los cuales a su vez son características significativas de la señal (energía o coeficientes LPC por cada trama estudiada). Una vez obtenidos los patrones, se almacenan en la memoria del sistema. En la etapa de reconocimiento, se captura una firma a validar, la cual es sometida al mismo proceso de extracción de patrones, aplicándose ahora una técnica de comparación basado en la medida de distancia entre los patrones obtenidos y los previamente almacenados. En función de dicha distancia se valida o rechaza la firma. (Delgado, 2006)

2.6.7.5. Reconocimiento de voz

La voz es otra característica que las personas utilizan comúnmente para identificar a los demás. Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares.

En los sistemas de reconocimiento de voz no se intenta reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación. (Delgado, 2006)

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique. (Delgado, 2006)

Como veremos a continuación, estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va `proponiendo' a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales).

Conforme va hablando el usuario, el sistema registra toda la información que le es útil y mediante el análisis de los sonidos que emitimos, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos. (Delgado, 2006)

El principal problema del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos.

Sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona reconocimiento de voz posee la cualidad de una varía su timbre). (Delgado, 2006)

A su favor, la excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

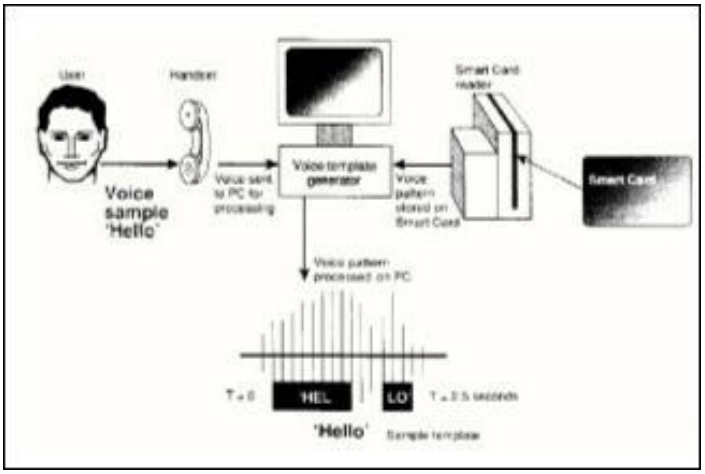


FIGURA Nº 17: Reconocimiento de voz
FUENTE: (I. B. Isidro)

2.6.7.6. Elementos de un reconocedor de voz

El reconocimiento de voz generalmente consta de los tres pasos siguientes:

- Pre procesamiento
- Reconocimiento
- Comunicación

2.6.7.7. Pre procesamiento de la señal de voz

Los sonidos consisten en cambios de presión del aire a través del tiempo y a frecuencias que podemos escuchar. Estos sonidos pueden ser digitalizados por un micrófono o cualquier otro medio que convierte la presión del aire en pulsos eléctricos. La voz es un subconjunto de los sonidos generados por el tracto vocal. En el procesamiento de la señal se extraen las características que utilizará posteriormente el reconocedor. En el proceso de extracción de características se divide la señal de voz en una colección de segmentos. Posteriormente, se obtiene una representación de características acústicas más distintivas para cada segmento. Con estas características obtenidas, se construye un conjunto de vectores que constituyen la entrada al siguiente módulo. (Delgado, 2006)

Un reconocedor debe extraer de la señal acústica solo la información que requiere para poder reconocer una frase.

2.6.7.8. Reconocimiento

En la etapa de reconocimiento se traduce la señal de entrada a su texto correspondiente. Este proceso se puede llevar a cabo de diversas formas utilizando enfoques como Redes Neuronales Artificiales (RNA) y Modelos Ocultos de Markov (HMM), entre otros. (Delgado, 2006)

2.6.7.9. Comunicación

El resultado de la etapa de reconocimiento será enviado al sistema que lo requiere.

Cabe de todas formas hacer una mención aparte al reconocimiento biométrico de la voz como sistema eficaz para la identificación remota. Es decir, cuando una persona desea realizar una transacción o acceder a unos datos, desde, pongamos, un teléfono móvil, el reconocimiento biométrico de la voz puede ser una herramienta muy útil, y hasta muy segura si se añaden sistemas de verificación basados en desafíos dinámicos, y el registro inicial (Enrollment) se ha hecho correctamente. (Delgado, 2006)

2.6.8. **CONTROL DE ACCESO**

2.6.8.1. Lectores Biométricos

Se entiende por lector biométrico aquel que se caracteriza por reconocer algún parámetro físico o de comportamiento de la persona que lo identifique unívocamente para determinar o verificar su identidad, como por ejemplo, la huella dactilar, el reconocimiento facial o de la voz. La biometría es un excelente sistema de identificación que se aplica en muchos procesos ya que aporta seguridad y es muy cómodo. Todos los seres humanos tienen características morfológicas únicas que les diferencian. (Saavedra, 2006)

El proceso de autenticación general que se sigue es, en primer lugar los lectores biométricos poseen un mecanismo automático que lee y captura la imagen digital o analógica a analizar, a continuación, dichos lectores poseen una base de datos para el almacenamiento y comparación de los datos capturados y el proceso finaliza con la decisión de si el usuario es válido o no.

El falso rechazo y la falsa aceptación son dos parámetros que se usan para medir la exactitud del equipo biométrico. El falso rechazo se produce cuando a una persona de la que se tienen guardados sus datos en el sistema, por un fallo en el lector se le niega el acceso. Esto puede suceder debido a que la persona puede haber sufrido algún cambio temporal o que influya algún

parámetro ambiental en la lectura. Este defecto es incómodo pero no es un defecto grave para la seguridad. Por otro lado falsa aceptación se produce cuando se identifica a una persona como si fuera otra. Este defecto es un error grave. (Saavedra, 2006)

Todos los sistemas biométricos realizan reconocimientos para "volver a conocer" a una persona que ya había sido registrada previamente. La autenticación puede realizarse de dos maneras diferentes identificación y verificación. La identificación consiste en la comparación de la muestra recogida del individuo frente a una base de datos de rasgos biométricos registrados previamente. No se precisa de declaración inicial de su identidad por parte del usuario, es decir, el único dato que se utiliza es la muestra biométrica recogida en el momento de uso, sin apoyo de un registro anterior ni un nombre de usuario o cualquier otro tipo de reconocimiento.

Este método requiere de un proceso de cálculo complejo, puesto que se ha de comparar esta muestra con cada una de las anteriormente almacenadas para buscar una coincidencia. Sin embargo en el sistema de verificación el primer paso del proceso es la identificación del individuo mediante un nombre de usuario, tarjeta o algún otro método. De este modo se selecciona de la base de datos el patrón que anteriormente se ha registrado para dicho usuario. (Saavedra, 2006)

Posteriormente, el sistema recoge la característica biométrica y la compara con la que tiene almacenada. Es un proceso simple, al tener que contrastar únicamente dos muestras, en el que el resultado es positivo o negativo.

Los sistemas biométricos tienen ventajas y desventajas respecto al resto de sistemas de control de accesos, entre ellos destacan:

Ventajas:

- Los rasgos biométricos no pueden ser olvidados ni perdidos, garantizando el acceso constante a la persona que tiene que ser identificada. El medio de identificación es único y personal.
- Los rasgos biométricos no pueden ser robados, garantizando la seguridad de la empresa. Seguridad jurídica: quien ha registrado, qué, cuándo y dónde.

- Uso sencillo, seguro y cómodo.
- Integración sencilla en sistemas ya existentes.
- Organiza las horas de ingreso y salida de los empleados.
- No se puede “fichar” por los compañeros.

Inconvenientes

- Son lentas.
- Son caras.
- Menos resistentes al vandalismo que las tarjetas de proximidad.
- No son totalmente precisas.

Existen numerosas características biométricas del ser humano que pueden ser medidas, pero no todas ellas pueden ser usadas para la biometría. Solo podrán ser usadas aquellas que cumplan los siguientes criterios:

- Universalidad: cualquier individuo debe poseer esa característica.
- Unicidad: dos sujetos cualesquiera deben poder ser diferenciados gracias a dicha característica.
- Permanencia: la característica del individuo no debe cambiar en el tiempo.
- Coleccionabilidad: la característica debe poder ser medida por métodos cuantitativos.
- Rendimiento: relativo a la precisión y a la velocidad de ejecución, así como a los recursos necesarios para conseguir dicha precisión.
- Aceptabilidad: indica el grado de aceptación o rechazo de la población sobre el uso de un sistema biométrico en su vida diaria.
- Resistencia a fraude: relativo a la posibilidad de engañar al sistema usando métodos fraudulentos.
- Fiabilidad: refleja el grado de dificultad encontrado para burlar el sistema.

Se pueden encontrar las siguientes tecnologías biométricas:

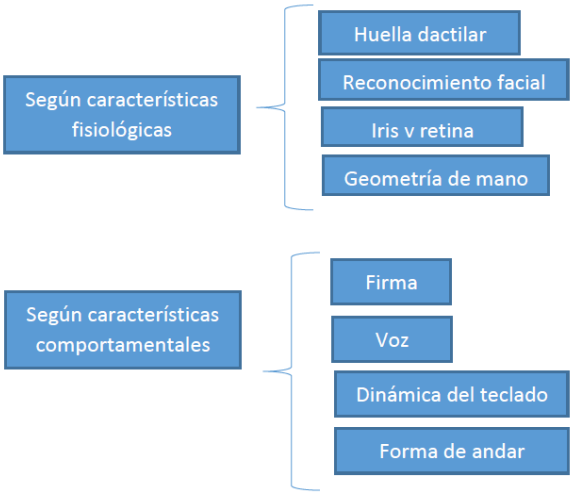


FIGURA Nº 18: Esquema de lectores biométricos
FUENTE: (www.cronos.com.ar)

Cada una de estas opciones tiene unas ventajas y desventajas diferentes, que deben tenerse en cuenta en el momento de decidir que técnica utilizar, ya que dependiendo de dónde se vaya a instalar será mejor una opción u otra. Los sistemas biométricos más conocidos son los siguientes: (Saavedra, 2006)

2.6.8.2. Huella dactilar

Es el sistema biométrico más popular y antiguo utilizado con éxito en muchas aplicaciones. La tecnología ha ido avanzando rápidamente y cada vez es más asequible para muchas aplicaciones y más exacta y difícil de falsificar. Las huellas digitales tienen rasgos que las hacen únicas e inequívocas. Incluso, los 10 dedos de la mano de una persona tienen diferentes rasgos únicos entre ellos. Para evitar errores o problemas por heridas en los dedos, el proceso de escáner de la huella y almacenamiento se suele realizar con dos o más dedos. (Saavedra, 2006)

El modo de funcionamiento es el siguiente, a partir de las características distintivas de la yema del dedo, la unidad de lectura biométrica crea un patrón de identificación único, que no es más que una descripción matemática de datos de posición que identifican los puntos finales de las líneas de los dedos o sus bifurcaciones. (Saavedra, 2006)

Ventajas:

- Los seres humanos tienen múltiples huellas

- Las huellas son únicas para cada dedo de cada individuo y la configuración de surcos se mantiene permanente durante toda una vida
- Son fáciles de usar
- Requieren poco espacio
- Sistemas de captura no invasivos y de bajo coste
- Técnica muy desarrollada

Desventajas:

- Necesidad de elevada calidad de la imagen digital
- Necesidad de contacto físico con la superficie del sensor
- Se asocia a temas penales

FIGURA Nº 19: Lector de huella dactilar
FUENTE: (www.cronos.com.ar)

2.3.8.9. Reconocimiento facial

Es un método poco invasivo, se basa en características de la cara como los lados de la boca, los pómulos, el perfil de los ojos y la posición de la nariz. Una cámara toma una foto a la cara y mide las distancias y proporciones entre los puntos que separan la parte interior y exterior de los ojos, nariz, boca, etc., obteniendo así una plantilla única que permite autentificar a una persona de forma precisa. (Saavedra, 2006)

Ventajas:

- No requiere contacto, método no intrusivo
- Chequeo fácil por parte del ser humano

- Máxima higiene al no requerir contacto entre el usuario y el terminal
- Aporta información adicional de expresión, estado de ánimo

Desventajas:

- El rostro puede ser tapado por el pelo, sombreros, pañuelos, etc.
- Los rostros se modifican con el paso del tiempo
- Variaciones sufridas en los rasgos faciales debido a la posición de la cabeza, el corte de la barba o del pelo
- Sensible a los cambios en la luz
- No es tan fiable como otro tipo de característica biométrica

FIGURA Nº 20: Lector de reconocimiento facial
FUENTE: (www.cronos.com.ar)

2.3.8.10. Iris

El iris es una membrana muscular de ojo utilizada como diafragma, ubicada detrás de la córnea y enfrente del cristalino. El iris de cada individuo es único y cuenta con 200 rasgos individuales diferentes. A menos que sufra heridas, estos rasgos se mantienen inalterables en el tiempo. La identificación se realiza a través de una cámara que realiza un escáner ocular convirtiendo la información en un código único. (Saavedra, 2006)

Ventajas:

- No hay necesidad de contacto
- Es un órgano interno y protegido, por lo que tiene menor probabilidad de sufrir lesiones

Desventajas:

- Intrusivo
- La captura en algunos individuos es muy difícil

- Requiere de un mayor entrenamiento y mayor atención que el resto de sistemas biométricos

FIGURA Nº 21: Lector de reconocimiento de iris
FUENTE: (www.cronos.com.ar)

2.3.8.11. Retina

Es la capa más interna de las tres capas del globo ocular. Es el tejido sensible a la luz que se encuentra en la parte posterior interna del ojo y actúa como la película en una cámara: las imágenes pasan a través del cristalino del ojo y son enfocadas en la retina. (Saavedra, 2006)

La retina convierte luego estas imágenes en señales eléctricas y las envía a través del nervio óptico al cerebro. Los sistemas basados en las características de la retina analizan la capa de vasos sanguíneos localizados en la parte posterior del ojo.

En estos sistemas el usuario a identificar debe mirar a través de unos binoculares, ajustar la distancia inter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. (Saavedra, 2006)

En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en la base de datos, si la muestra coincide para el usuario que el individuo dice ser, se permite el acceso. (Saavedra, 2006)

Ventajas

- Alta seguridad

Desventajas

- Escasa aceptación entre los usuarios

- Es muy preciso pero se considera intrusivo
- El uso de lentes de contacto puede modificar los valores de la medida obtenida
- Sistemas demasiado caros

Debido a las desventajas que presenta, el uso de esta tipología de sistema biométrico se ve reducida a la identificación en sistemas de alta seguridad, como el control de accesos a instalaciones militares. (Saavedra, 2006)

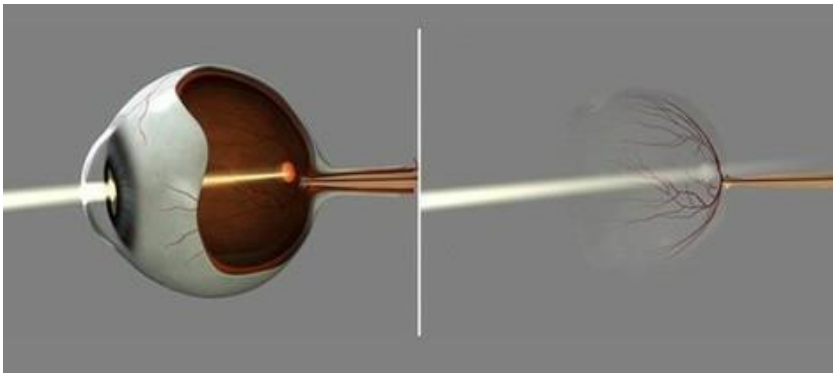


FIGURA Nº 22: Reconocimiento de la retina
FUENTE: (www.cronos.com.ar)

2.3.8.12. Geometría de la mano

Estos sistemas crean una imagen tridimensional de la mano y analizan diferentes características como las medidas de la mano, la longitud de los dedos, la curvatura, las áreas, las posiciones relativas de los dedos, nudillos, etc. La mano se apoya con la palma hacia abajo en una superficie que mediante una cámara digital recoge el modelo descriptivo que posteriormente se compara con los datos almacenados. (Saavedra, 2006)

Ventajas:

- Fácil captura
- Se cree que tiene un diseño estable a lo largo de la vida adulta
- Poco intrusivo

Desventajas:

- El sistema requiere de mucho espacio físico
- Su utilización requiere de entrenamiento

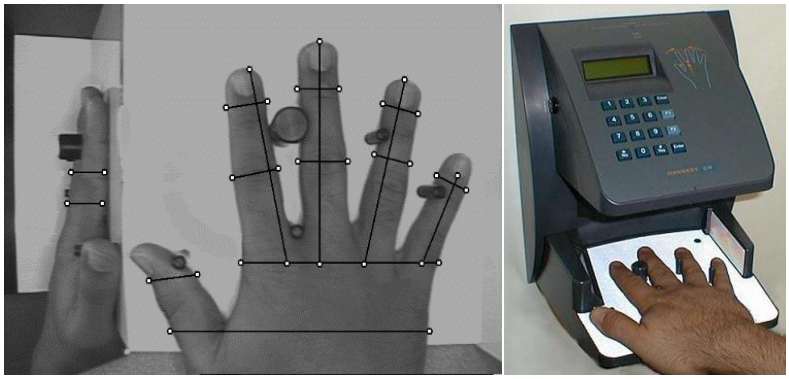


FIGURA Nº 23: Geometría dela mano
FUENTE: (www.cronos.com.ar)

Otros sistemas biométricos que se pueden encontrar, pero que no están tan extendidos a día de hoy son los siguientes:

2.3.8.13. Firma

Para utilizar este sistema se solicita en primer lugar un número determinado de firmas ejemplo a los individuos a los que se les va a permitir el acceso, de las cuales el sistema extrae y almacena ciertas características. Sin embargo, la firma de una persona no es idéntica cada vez que la hace. Hay dos métodos de identificar una firma, el estático que usa solo las características geométricas de una firma, su figura, y el dinámico que también toma en cuenta otras variables como velocidad, aceleración, presión y trayectoria de la firma. (Saavedra, 2006)

2.3.8.14. Voz

Es posible detectar patrones del espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares. En estos sistemas lo que se intenta reconocer no es lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para un correcto registro de los datos se requiere ausencia de ruidos, reverberaciones o ecos. La voz depende de características físicas como las cuerdas vocales y los conductos nasales, que juntos dan como resultado la voz. La voz de una persona es bastante única pero no lo suficiente como para tener un nivel de distinción confiable. Un problema de este sistema es que puede ser engañado por una cinta grabada. Hay muchos avances en esta técnica que le hacen contar con un gran futuro. (Saavedra, 2006)

2.3.8.15. Venas de las manos

Este reconocimiento consiste en acercar (sin tocar) la palma de la mano a un sensor, que en cuestión de segundos, por medio de rayos infrarrojos captura el patrón de las venas. Esto sucede porque la hemoglobina absorbe la luz y hace que las venas se muestren negras dibujando una especie de mapa, y dicho mapa se traduce en una representación matemática. Al estar las venas a unos milímetros por debajo de la piel, su copia e intento de falsificación se hace casi imposible.

A continuación se muestra una tabla comparativa de los diferentes sistemas biométricos realizada por Cesar Tolosa Borja y Álvaro Giz Bueno y completada con otra tabla realizada por Carmen Sánchez Ávila. (Saavedra, 2006)

	Iris	Retina	Huellas dactilares	Geometría de la mano
Fiabilidad	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta
Prevención de ataques	Alta	Alta	Alta	Alta
Aceptación del usuario	Media	Media	Media	Media
Estabilidad	Alta	Alta	Alta	Media
Intrusismo	No	Alto	Bajo	No
Identificación y verificación	Ambas	Ambas	Ambas	Verificación
Interferencias	Iluminación inadecuada	Irritaciones, Gafas, lentillas	Suciedad, heridas, asperezas, sequedad, edad, ...	Artritis, reumatismo, edad, lesiones varias, ...

TABLA Nº 2: Comparación entre sistemas biométricos 1
FUENTE: (www.cronos.com.ar)

	Escritura	Firma	Voz	Reconocimiento facial
Fiabilidad	Baja	Baja	Alta	Media
Facilidad de uso	Alta	Alta	Alta	Media
Prevención de ataques	Media	Media	Media	Media
Aceptación del usuario	Alta	Media	Alta	Media
Estabilidad	Baja	Media	Media	Media
Intrusismo	No	No	No	No
Identificación y verificación	Verificación	Verificación	Verificación	Verificación
Interferencias	Lesiones de mano, cansancio	Firmas fáciles o cambiantes, cambio de escritura	Ruido, resfriados	Pelo, gafas, edad, iluminación...

TABLA Nº 3: Comparación entre sistemas biométricos 2
FUENTE: (www.cronos.com.ar)

2.3.8.16. Lectura de tarjetas de banda magnéticas

Este sistema funciona mediante tarjetas codificadas magnéticamente, las cuales al pasarse por un lector adecuado a ellas descifra su código y en caso de ser un código valido para el sistema, activa un relé que permite la apertura de la puerta. (Saavedra, 2006)

Cuenta con diversas ventajas, entre ellas que tienen un bajo costo, es una tecnología ya probada, no son fáciles de duplicar, tienen un gran periodo de vida y proporcionan agilidad en el acceso. Sin embargo, a consecuencia de la fricción en el momento de la lectura, las deteriora. Además, si se acercan a una fuente electromagnética relativamente fuerte, puede modificarse la información que contiene, perdiendo así su utilidad. (Saavedra, 2006)

Las dimensiones de las tarjetas de bandas magnéticas están estandarizadas por el ANSI (American National Standard Institute) y por las normas ISO (International Standard Organization), y fueron definidas para facilitar la manipulación y almacenamiento de las mismas.

FIGURA Nº 24: Lector de tarjetas de banda magnética
FUENTE: (www.cronos.com.ar)

2.3.8.17. Lectura de tarjetas con código de barras u ópticas

Usa una tarjeta de apariencia similar a la magnética, pero en lugar de una banda, lleva impreso un código de barras, el cual puede incluso ser protegido con una banda protectora que evita la duplicación de la tarjeta por fotocopias. El código de barras es un arreglo en paralelo de barras y

espacios en diferentes grosores que contienen información codificada. La ventaja es que al pasar la tarjeta por el lector no existe rozamiento, solo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es aún mayor y son baratas. Además, la impresión tiene un bajo coste y la personalización y codificación es sencilla y se puede realizar bajo demanda. Sin embargo su principal desventaja es que no admite que se rayen, ya que de esa manera se altera el código, además son fácilmente falsificables, siendo esto un gran problema para un sistema estricto de control de accesos. (Saavedra, 2006)

FIGURA Nº 25: Lector de código de barra
FUENTE: (www.cronos.com.ar)

2.3.8.18. Acceso mediante clave

El funcionamiento de este sistema es mediante la captura de una clave de acceso, la cual se introduce a través de un teclado numérico o alfanumérico. Cada persona posee un único número de identificación que será usado para acceder a todos los lugares que cuenten con un acceso mediante clave.

A pesar de ser económico, su gran desventaja es que ofrece un bajo grado de seguridad ya que los usuarios en ocasiones para que no se les olvide la clave la apuntan en una libreta, perdiendo así toda la confidencialidad que se buscaba con esta tipología. (Saavedra, 2006)

FIGURA Nº 26: Control de acceso mediante clave
FUENTE: (www.cronos.com.ar)

2.3.8.19. Acceso por proximidad

Este sistema trabaja por Radio Frecuencia, comúnmente conocidos por el anglicismo RFID (Radio Frequency IDentification). Esta tecnología permite identificar automáticamente un objeto gracias a una onda emisora incorporada en el mismo que transmite por radiofrecuencia los datos identificativos de dicho objeto, es decir, se permite la identificación de cualquier objeto o cosa sin mantener un contacto entre el emisor y el receptor, solo es necesario acercar la tarjeta al radio de recepción de la antena.

La distancia de lectura cambia dependiendo de la tecnología empleada, siendo desde unos centímetros para las tarjetas pasivas a unos metros para las activas.

La principal ventaja del control de accesos por proximidad es que el reconocimiento de la identidad de una persona que quiere acceder a un determinado lugar se realiza sin contacto físico, por lo tanto el desgaste es mucho menor que los tipos vistos anteriormente. (Saavedra, 2006)

Esta tipología puede presentar diversos formatos, pulsera, tarjeta, llavero, etc.
Existen diferentes tipos de etiquetas RFID dependiendo de la fuente de energía que utilicen, la forma física que tengan, el mecanismo empleado para almacenar los datos, la cantidad de datos que sean capaces de almacenar, la frecuencia de funcionamiento o de la comunicación que utilizan para transmitir la información al lector, etc. Gracias a esto es posible elegir la etiqueta más adecuada para cada aplicación específica.

Según el tipo de frecuencia, los dos más importantes son los siguientes:

a) **Tipo transponder o tag RFID**, cuya frecuencia es de 125 Khz. Este tipo son para servicios que no requieren más de un dato, por ejemplo, solo permiso de acceso.

b) **Mifare**, cuya frecuencia de emisión es de 13.56 Mhz. Sirven para el uso de varios servicios con una misma tarjeta, ya que permite almacenar información.

Todos los tags independientemente de la tecnología están formados por una antena y un micro. La antena es la que permite emitir la información almacenada en el micro a una distancia

apropiada. El micro es el que almacena dicha información, normalmente esta información es un numero de longitud variable, dependiendo del tipo de tag y alguna información de más cuya longitud dependerá de la capacidad del micro y la tecnología usada.
A grandes rasgos, en función de la fuente de energía que utilicen, se pueden encontrar con los siguientes tipos:

1) Tag o etiquetas pasivas: no disponen de ningún tipo de batería para emitir su información. Para su correcto funcionamiento es necesaria la intervención de un agente externo, lector de tags. Dependen del radio de recepción de la antena (suelen estar comprendidas entre los 10 cm y pocos metros) y por lo tanto no tienen límites de duración en el tiempo.

La corriente eléctrica necesaria para su funcionamiento se obtiene por inducción en su antena de la señal de radiofrecuencia procedente de la petición de lectura de la estación lectora. De este modo, cuando el lector interroga a la etiqueta, genera un campo magnético que produce en la micro antena del tag un campo eléctrico suficiente para transmitir una respuesta. (Saavedra, 2006)

2) Etiquetas activas: poseen una pequeña batería o fuente de energía interna que permiten incrementar el radio de lectura (mucho mayores que las pasivas y las semi pasivas) además de ser más eficaces en entornos adversos. Son más costosas y tienen un mayor tamaño que las otras dos. Pueden permanecer dormidas hasta que se encuentran dentro del rango de algún lector o pueden transmitir datos sin necesidad de obtener la energía de un lector.

3) Etiquetas semiactivas o semipasivas: (el nombre depende del lugar de construcción de las mismas). Este tipo posee una mezcla de características de los dos tipos anteriores. Son muy similares a las pasivas, salvo que este tipo obtienen energía de una pequeña batería. Esta batería permite al circuito integrado en la etiqueta estar constantemente alimentado, y elimina la necesidad de diseñar una antena para recoger potencia de una señal entrante. Estas etiquetas responden más rápido que las pasivas, por lo que el ratio de lectura es ligeramente superior.

Son más grandes y más caras que las etiquetas pasivas (ya que disponen de una batería) y más baratas y pequeñas que las activas. Sus capacidades de comunicación son mejores que las pasivas aunque no alcanzan a las activas en estas características.

4) Sistemas combinados: Es muy importante tener en cuenta el grado de seguridad que se busca, ya que, una solución para incrementar la protección en aquellas áreas en la que se quiera dotar de más seguridad se podrían combinar dos o tres sistemas de control de accesos en un solo dispositivo. Es importante realizar un adecuado diseño para lograr la seguridad deseada sin comprometer el tiempo de autenticación.

Para ello se podrían hacer por ejemplo las siguientes combinaciones:

- Huella dactilar + clave
- Tarjeta de proximidad + clave
- Huella dactilar + tarjeta de proximidad
- Huella dactilar + tarjeta de proximidad + clave

2.3.9. CHAPA MAGNÉTICA O CERRADURAS PARA CONTROL DE ACCESO

Una cerradura electromagnética se compone de dos partes: una placa hecha por un material magnético y una placa metálica rodeada por una bobina. Cuando la corriente eléctrica es pasada por la bobina, la placa metálica es magnetizada y atrae fuertemente a la placa del material magnético, cerrando así la puerta.

Todas las cerraduras electromagnéticas son tipo “Fail Safe” y existen diferentes grados de presión que ejerce el magneto.

Están diseñadas para puertas con un ángulo de apertura de 90 grados. Son ideales para puertas internas como oficinas, puertas de emergencias, etc., que no requieren un alto grado de seguridad. Con los accesorios adecuados se pueden usar en puertas de madera, vidrio y metal.

2.3.9.1.Tipos de cerraduras electromagnéticas

Simples: Son el tipo más común. Para puertas regulares que abren en dirección del exterior al interior, el magneto queda viendo al exterior. si se quiere que el magneto quede del lado del interior se debe usar un bracket ZL. Si la puerta abre en dirección del interior al exterior, entonces el magneto queda del lado interior.

FIGURA Nº 27: Cerradura electromagnética
FUENTE: (www.biotracksoftware.com)

Dobles: Se usan para puertas de doble hoja

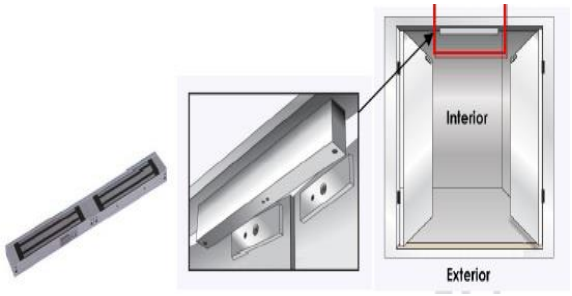


FIGURA Nº 28: Cerradura electromagnética dobles
FUENTE: (www.biotracksoftware.com)

Empotrables: se usan cuando no se quiere que la cerradura quede expuesta y se tiene la posibilidad de hacer un bosquete a la puerta y al marco.

FIGURA Nº 29: Cerradura electromagnética empotrables
FUENTE: (www.biotracksoftware.com)

2.3.9.2.Comparación De Las Cerraduras

	 Electromagnética	 Recibidor	 Picaporte
Tipo de Cerradura	Fail Safe	Fail Safe, Fail Secure	Fail Safe
Angulo de apertura de la puerta	90º	90º	90º , 180º, corredizas
Materiales de la puerta	Madera, metal, vidrio	Madera, metal	Madera, metal, vidrio

TABLA Nº 4: Comparación dela cerraduras
FUENTE: (www.biotracksoftware.com)

2.3.10. METODOLOGIA Y HERRAMIENTAS UTILIZADAS

La metodología utilizada para el desarrollo de este proyecto es, la metodología modelo funcional para la administración de redes, implementación de equipos de cámaras IP, lectores biométricos IP, estos modelos detallan las tareas y funciones que deben ser ejecutadas en cada proceso.

La ventaja de esta metodología, es que se divide en 5 áreas funcionales que son: Configuración, fallas, rendimientos, contabilidad y seguridad, donde se define las funciones de cada una de ellas. Para el desarrollo del proyecto se utilizó tres procesos los cuales son: Administración de configuración, administración de fallas, administración de rendimientos.

2.3.11. DESARROLLO DE LA METODOLOGÍA

2.3.11.1. Administración de la configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

a) Planeación y diseño de la red. La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser:

- Multicast
- Voz sobre IP (VoIP)
- Calidad de servicio (QoS)

Algunas necesidades cuantitativas pueden ser

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

- Diseñar la topología de la red
- Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
- Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.
- Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

Selección de la infraestructura de red: Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más

recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

b) Instalaciones y Administración del software. El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

- **Instalaciones de hardware:** Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.

Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.

Notificar anticipadamente a los usuarios sobre algún cambio en la red.

Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.

Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.

Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.

Documentar el cambio para futuras referencias.

- **Administración del software.** Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

- Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de FTP.

c) **Provisionamiento:** Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

✓ **Administración del rendimiento:** Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

✓ **Monitoreo:** El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) **Utilización de enlaces:** Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) **Caracterización de tráfico:** Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) **Porcentaje de transmisión y recepción de información:** Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) **Utilización de procesamiento:** Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

✓ **Análisis:** Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) **Utilización elevada:** Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b*)* **Tráfico inusual**: El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) **Elementos principales de la red:** Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra

dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) Calidad de servicio: Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico: El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

Interacción con otras áreas: La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.3.11.2. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- **Monitoreo de alarmas.** Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.

- **Localización de fallas.** Determinar el origen de una falla.

- **Pruebas de diagnóstico.** Diseñar y realizar pruebas que apoyen la localización de una falla.

- **Corrección de fallas.** Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.

- **Administración de reportes.** Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

Monitoreo de alarmas: Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red.

Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

Tipo de las alarmas

- **Alarmas en las comunicaciones.** Son las asociadas con el transporte de la información, como las pérdidas de señal.

- **Alarmas de procesos.** Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.

- **Alarmas de equipos.** Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.

- **Alarmas ambientales.** Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.

- **Alarmas en el servicio.** Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

Severidad de las alarmas.

 Crítica. Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

- **Mayor.** Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.

- **Menor.** Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

- **Indefinida.** Cuando el nivel de severidad no ha sido determinado por alguna razón.

Localización de fallas: Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

 Pruebas de diagnóstico: Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar.

 Pruebas de conectividad física: Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

 Pruebas de conectividad lógica: Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son "ping" y "traceroute".

 Pruebas de medición: Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

Corrección de fallas: Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

- **Entre los mecanismos más recurridos**, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- **Reemplazo de recursos dañados**. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.

- **Aislamiento del problema**. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.

- **Redundancia**. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.

- **Recarga del sistema**. Muchos sistemas se estabilizan si son reiniciados.

- **Instalación de software**. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.

- **Cambios en la configuración**. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

Administración de reportes: Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

Creación de reportes: Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte de be contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.

- Fecha y hora del reporte

Seguimiento a reportes: La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y este debe poder ser consultada en cualquier momento por el administrador.

Manejo de reportes: El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

Finalización de reportes: Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.3.11.3. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

Prevención de ataques: El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

Detección de intrusos: El objetivo es detectar el momento en que un ataque se esta llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

Respuesta a incidentes: El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

Políticas de Seguridad: La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

Servicios de seguridad: Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. Identifica el "que".

De acuerdo a la Arquitectura de Seguridad OSI, un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

Mecanismos de seguridad: Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras. Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

Proceso: Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.

Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.

Implementar las políticas de seguridad mediante los mecanismos adecuados.

HERRAMIENTAS UTILIZADAS

ZKTeco uFace800 Reconocimiento Facial y Huella Digital: Es múlti-Biométrica para gestión de tiempo y asistencia además de aplicaciones de control de acceso, la cual soporta hasta 3,000 plantillas de rostros, 4,000 de huellas digitales y 10,000 tarjetas (opcional). Está equipada con la última plataforma de hardware y algoritmo de ZKTeco, que proporciona a los clientes, una interfaz de usuario más intuitiva y fácil de utilizar. Con el avanzado algoritmo para rostro y la tecnología múlti-biométrica, el nivel de seguridad de las verificaciones es mucho mayor.

FIGURA Nº 30: Biometrico uface 800 ZKTeco
FUENTE: (www.biotracksoftware.com)

Brackets: Se usa para puertas que abran en dirección del exterior al interior y se quiera que el magneto quede del lado interior.

FIGURA Nº 31: Brackets
FUENTE: (www.biotracksoftware.com)

Botones de Apertura: Los Botones son Controles alámbricos o inalámbricos que permiten abrir las puertas. Se utilizan por lo general al interior de las torres de apartamentos o pisos de oficinas, pues como el personal ya se identificó al entrar, no es necesario validar la identidad al salir.

FIGURA Nº 32: Boton de apertura
FUENTE: (www.biotracksoftware.com)

CHAPA MAGNETICA L700: Sistema, crea un flujo magnético que hace que la placa de armadura, atraiga. Las cerraduras electromagnéticas de gran calidad.

FIGURA Nº 33: Chapa magnetica L 700
FUENTE: (www.biotracksoftware.com)

El presente capitulo describe de acuerdo a la Metodología, los procesos que se aplican para la implementación del sistema de control de acceso a los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando.

CAPITULO III
MARCO APLICATIVO

3. MARCO APLICATIVO.

Para llevar a cabo la implementación del sistema de control de acceso automatizado a los laboratorios de informática del área de ciencias y tecnología de la universidad amazónica de pando, utilizando chapa magnética de puerta biométrica L700 y control de acceso ZKTeco, se realizó haciendo seguimiento a la Metodología Modelo, la misma que se describe en el Marco Metodológico.

Cabe recalcar, que de las cinco áreas funcionales que forman parte de la metodología solo se tomó en cuenta tres de ellas, las cuales son:

1. Administración de configuración
2. Administración de falla
3. Administración de seguridad

3.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son: Planeación y diseño de la red, instalación y administración del software, administración de hardware.

3.1.1. Planeación y diseño de la red de conexión del biométrico.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son: Reunir las necesidades de la red, Diseñar el tipo de red, Determinar y seleccionar la infraestructura.

3.1.1.1. Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas y cuantitativas.

A) **Necesidades específicas o Generales:** Para la implementación del sistema de control de ingreso a los laboratorios de informática se utilizaron los siguientes equipos y accesorios tecnológicos, los cuales son:

ZKTeco uFace800 Reconocimiento Facial y Huella Digital:	
Brackets	
Botones de Apertura	
CHAPA MAGNETICA L700:	
Antena de red inalambrica NanoStation M5 Ubiquiti 5GHz Indoor/ Outodoor airmax 16dbi	 
Switch D-LINK des-1016d	
Conectores RJ45	

Cable utp categoría 6ª	

B) Necesidades tecnológicas cuantitativas

Para la implementación del sistema de vigilancia y monitoreo se requerirá lo siguiente:

- Tres ZKTeco uFace800 Reconocimiento Facial y Huella Digital
- Nueve Brackets
- Tres Botones de Apertura
- Tres Chapa Magnética L700
- Dos Antena de red inalámbrica NanoStation M5 Ubiquiti 5GHz Indoor/ Outodoor airmax 16dbi
- UN Switch D-LINK des-1016d
- Diez Conectores RJ45
- doscientos metros de Cable utp categoría 6ª

3.1.1.2. Diseñar la topología de la red:

A) La topología utilizada para la implementación de los biométricos en el Área de Ciencias y Tecnología es topología estrella**.**

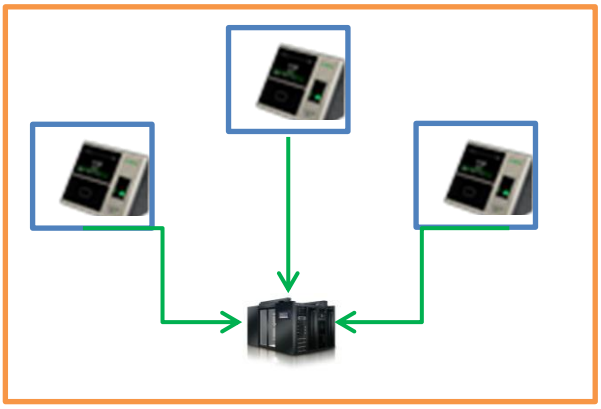


FIGURA Nº 34: Diseño Red Del Centro De Monitoreo
FUENTE: Elaboración propia

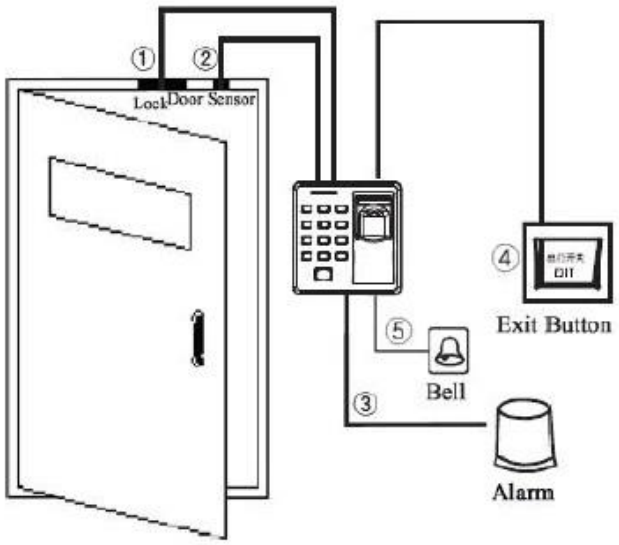


FIGURA Nº 35: Diseño Red Del Centro De Monitoreo
FUENTE: Elaboración propia

3.1.1.3. Determinar y seleccionar la infraestructura:

En esta parte se seleccionara la infraestructura a ser controlada donde estarán ubicados los biométricos y también se seleccionara la infraestructura donde será el centro de datos.

- Selección infraestructura a ser controlado con biométrico

FIGURA Nº 36: Infraestructura seleccionada para control biométrico
FUENTE: Elaboración propia

3.1.2. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

3.1.2.1 Instalaciones de hardware

En esta parte se contempla toda la parte hardware que se utilizó para la implementación del sistema de control de ingresos a los laboratorios del Área de Ciencias y Tecnología.

a) **Laboratorios de Informática:** En estos laboratorios se instaló los siguientes equipos hardware:

- ZKTeco uFace800 Reconocimiento Facial y Huella Digital
- Brackets
- Botones de Apertura
- Chapa Magnética L700
- Acometida de energía eléctrica

Toda la implementación de la parte hardware se hizo de acuerdo al diseño de la red.

FOTOS Nº 1: Instalación de los biométricos de control de acceso
FUENTE: Elaboración propia

FOTOS Nº 2: Instalación de la toma de corriente
FUENTE: Elaboración propia

b) Centro de datos: En el Centro de datos se Instaló los siguientes equipos hardware.

- NVR marca dahua modelo dhi-nrv4216
- CPU delux Intel core (TM)i5-4460 de 3.20 GHz, memoria de 4.00 GB, sistema operativo Windows 7 de 64 bit.
- Monitor Samsung s19 c150.
- Tv irt led 2496 cmbblue tv led 24 p
- Cableado UTP categoría 6ª
- Acometida de energía eléctrica

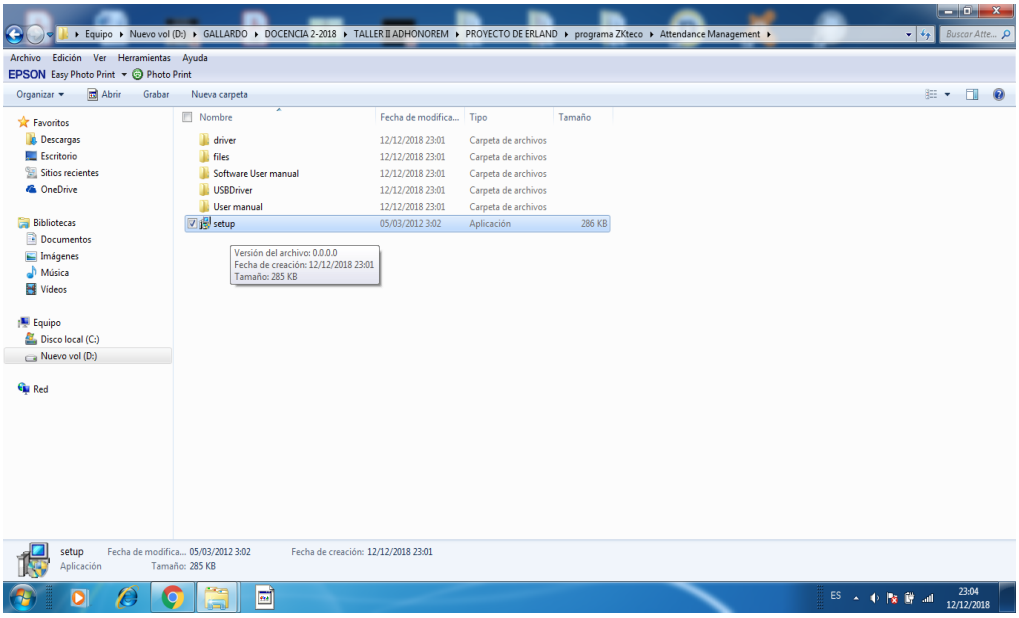
Toda la implementación de la parte hardware se hizo de acuerdo al diseño de la red.

FOTOS Nº 3: Centro De Datos
FUENTE: Elaboración Propia

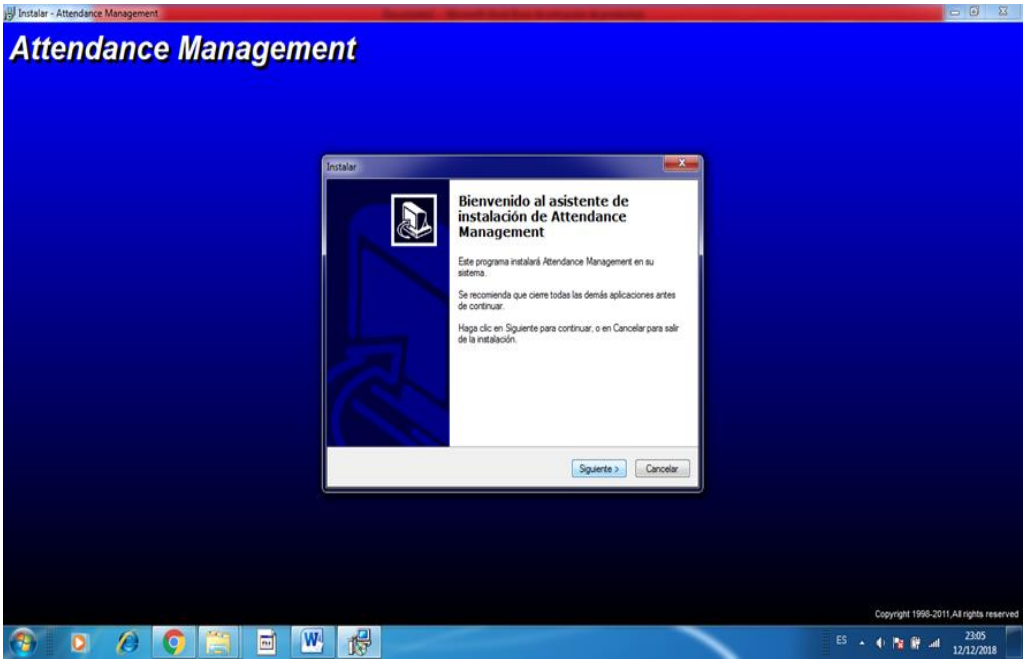
3.1.2.2. Administración del Software.

3.1.2.2.1. Instalación del software biométrico

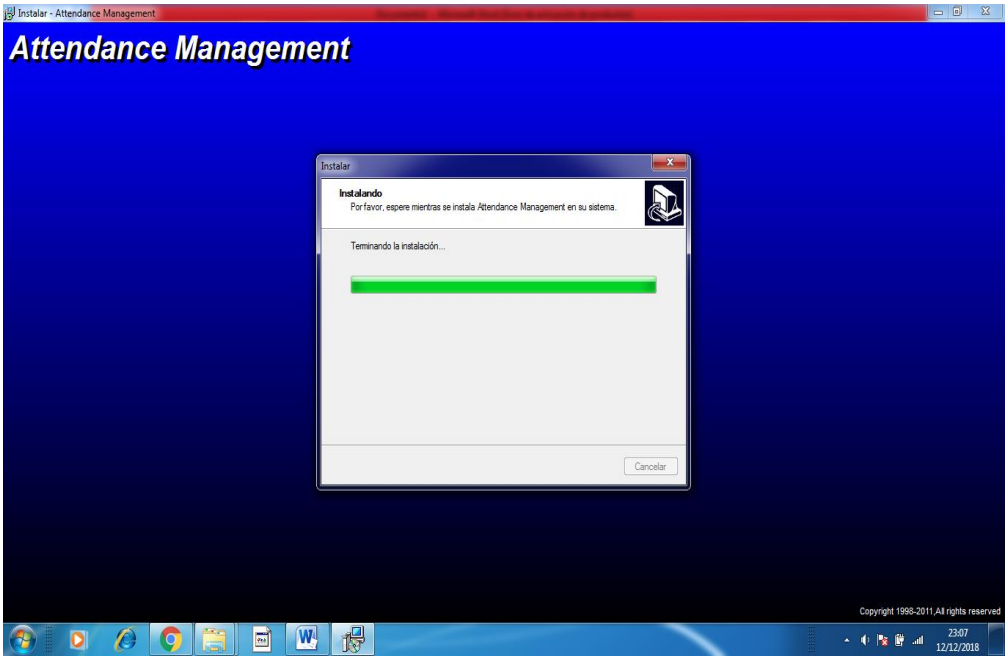
Lo primero que se hace es instalar el software en el computador que se encuentra en el centro de datos para luego hacer la debida configuración de los biométricos instalados en los laboratorios de informática



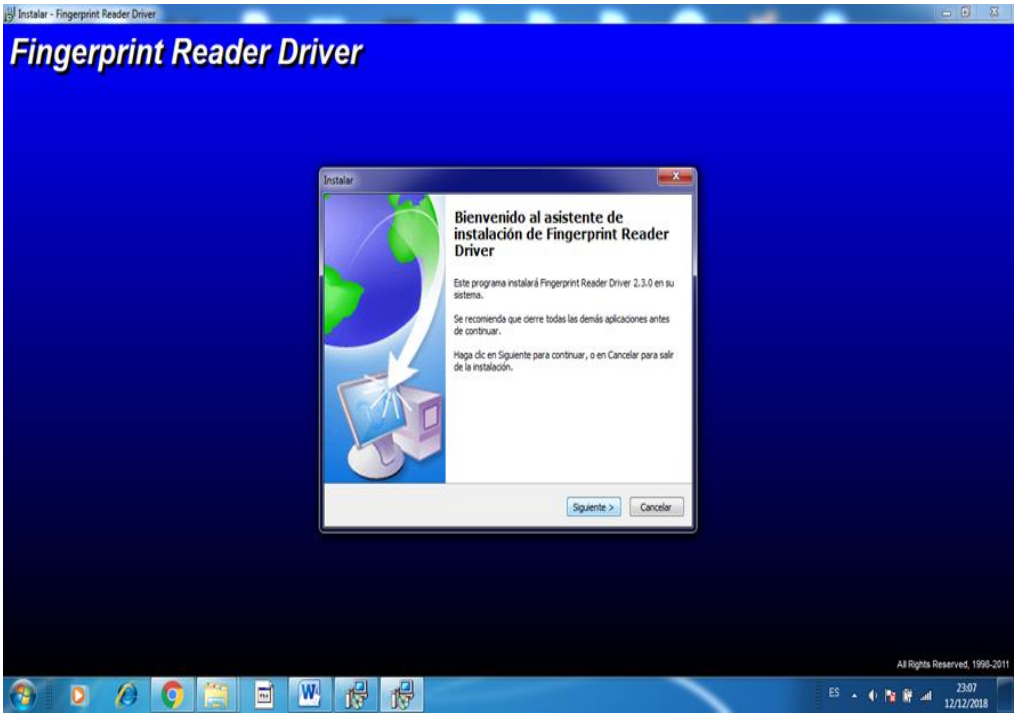
FOTOS Nº 4: Instalación del software del biométrico
FUENTE: Elaboración propia



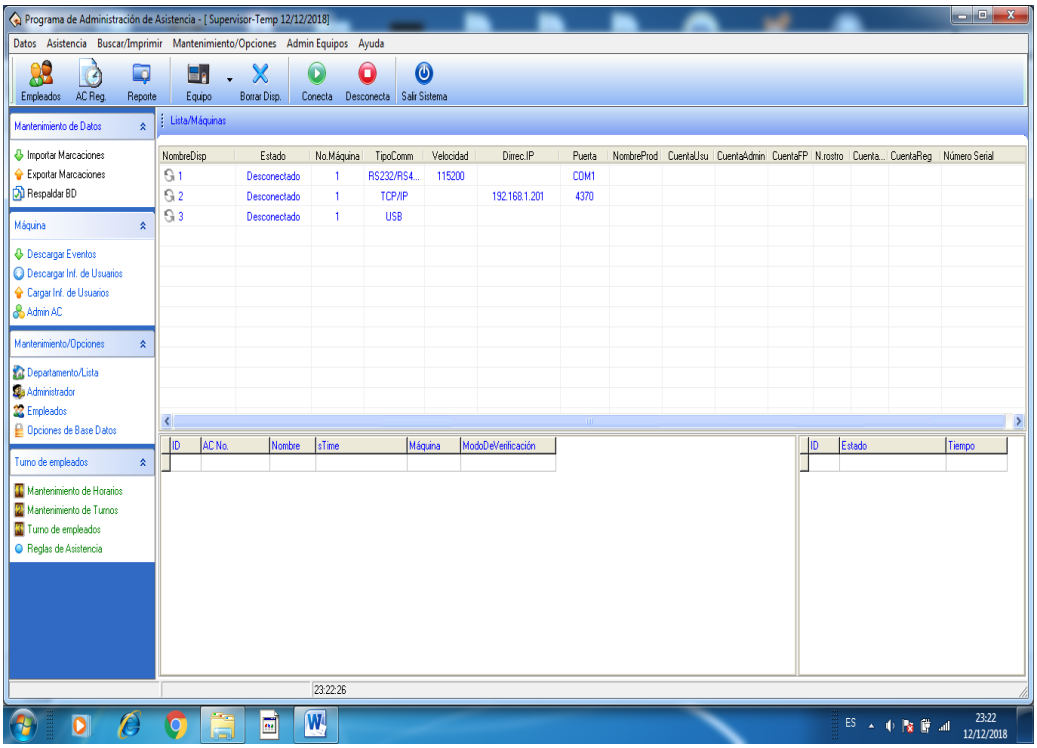
FOTOS Nº 5: Instalación del software del biométrico
FUENTE: Elaboración propia



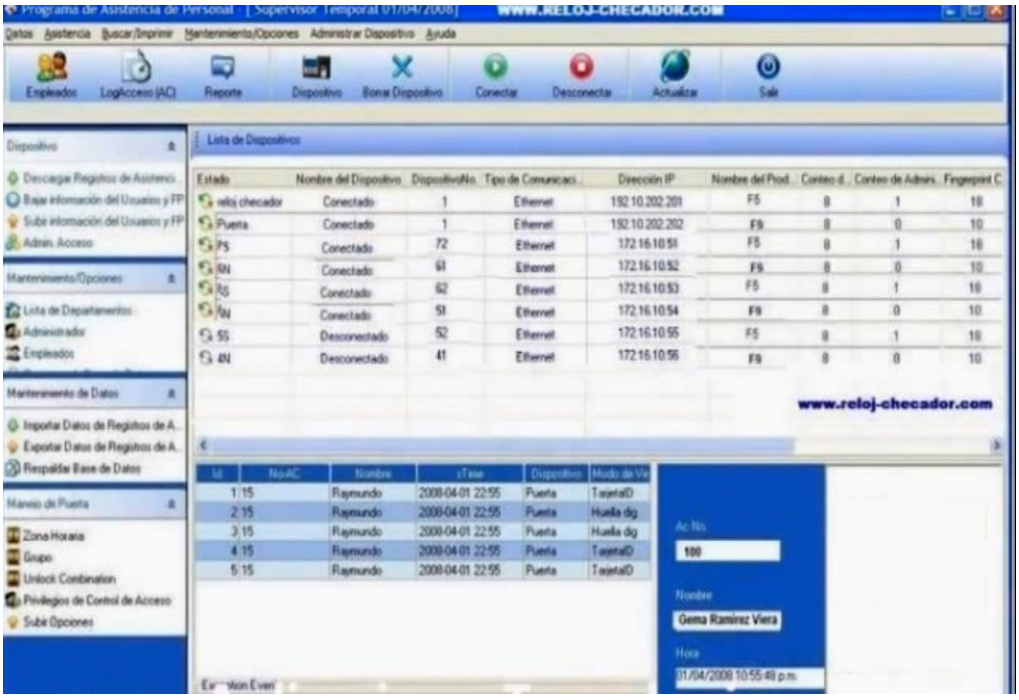
FOTOS Nº 6: Instalación del software del biométrico
FUENTE: Elaboración propia



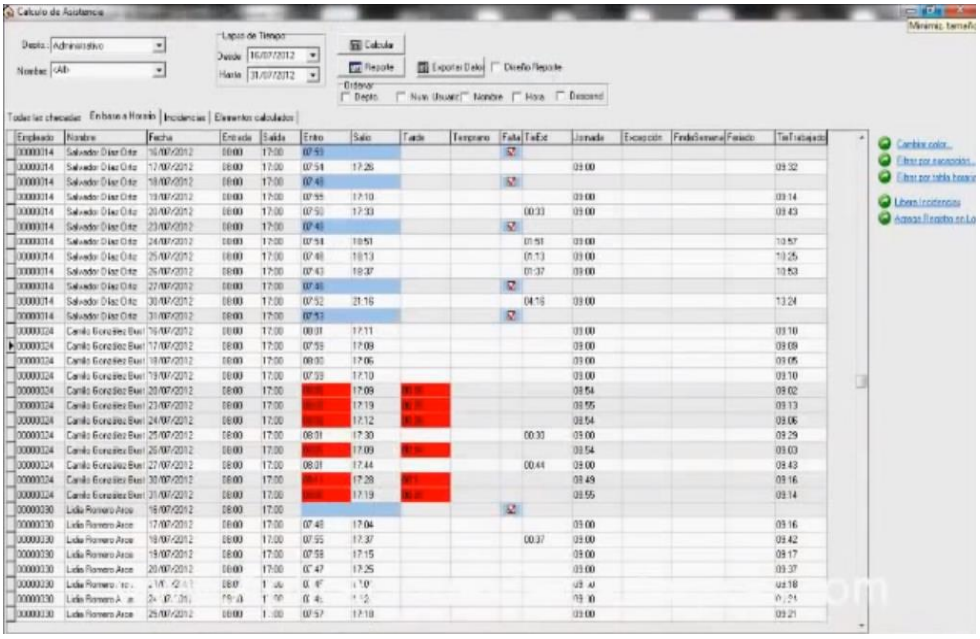
FOTOS Nº 7: Instalación del software del biométrico
FUENTE: Elaboración propia



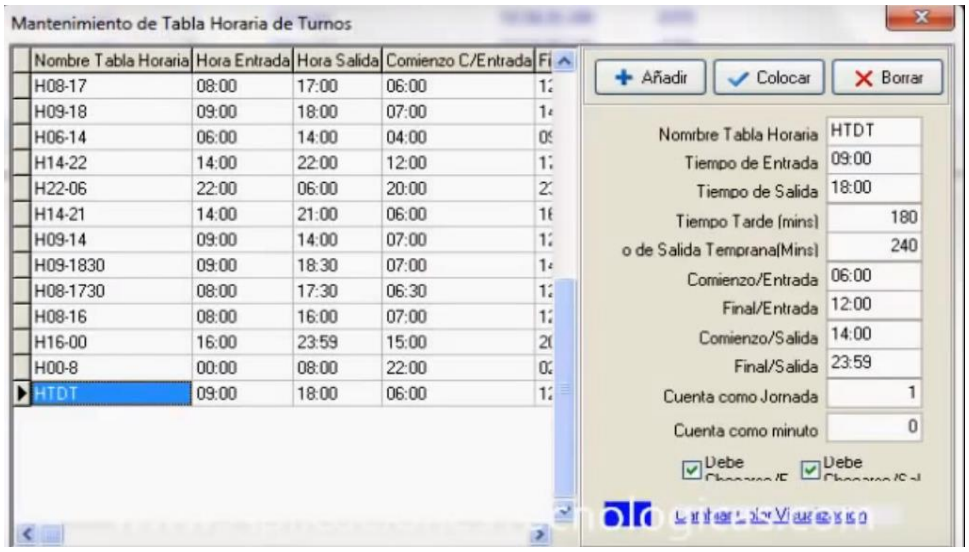
FOTOS Nº 8: Instalación del software del biométrico
FUENTE: Elaboración propia



FOTOS Nº 9: Instalación y configuración del software del biométrico
FUENTE: Elaboración propia



FOTOS Nº 10: Instalación y configuración del software del biométrico
FUENTE: Elaboración propia



FOTOS Nº 11: Instalación y configuración del software del biométrico
FUENTE: Elaboración propia

3.1.2.1.3. Configuración de los biométricos de marca ZKTeco uFace800 Reconocimiento Facial y Huella Digital

En esta parte se hace la configuración del biométrico para poder asignar al administrador, quien será la persona encargada de registrar a todos los usuarios como ser docentes, estudiantes y administrativos que tendrán acceso a los laboratorios de informática.

La configuración consiste en registrar su huella dactilar y facial de la persona, la misma que será asignado al grupo que corresponde.

El primer grupo será solo para personal autorizado, quienes podrán acceder a los laboratorios previo registro de su huella o facial, entonces la chapa magnética se activara para que pueda ingresar.

El segundo grupo solo podrá registrar su asistencia y no estará permitido el ingreso al laboratorio ya que la chapa magnética no se activara, impidiendo el ingreso al laboratorio de informática.

FOTOS Nº 12: Configuración del biométrico
FUENTE: Elaboración Propia

FOTOS Nº 13: Configuración del biométrico
FUENTE: Elaboración Propia

3.2. ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata.

Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla.

Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla. El proceso de la administración de fallas consiste de distintas fases.

a) Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.

IMAGEN Nº 1: Falla existente en la red del centro de datos
FUENTE: Elaboración Propia

b) Localización de fallas. Determinar el origen de una falla.

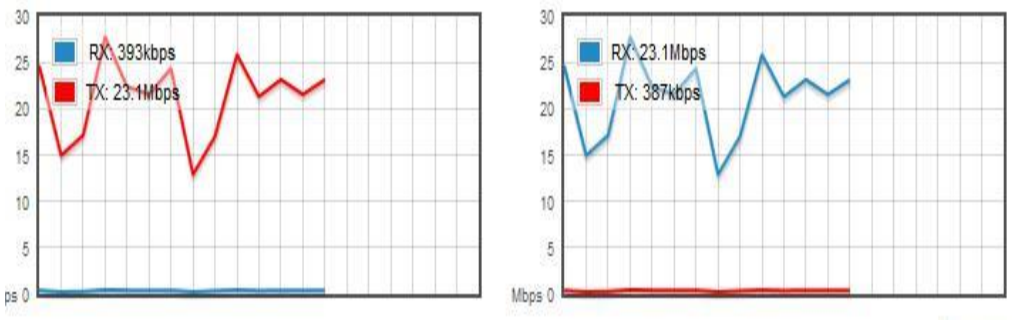


IMAGEN Nº 2: Falla encontrada en la red del centro de datos
FUENTE: Elaboración Propia

3.3. ADMINISTRACIÓN DE LA SEGURIDAD

El objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

a) **Prevención de ataques:** El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

- **Seguridad de los biométricos:** Para brindar seguridad a cada uno de los lectores biométricos, se le asigna una contraseña

IMAGEN Nº 3: Seguridad del lector biométrico
FUENTE: Elaboración Propia

- **Seguridad de la red inalámbrica de enlace:** Para brindar seguridad al enlace de la red inalámbrica entre el centro de monitoreo y el bloque “G” se le asigna una contraseña.

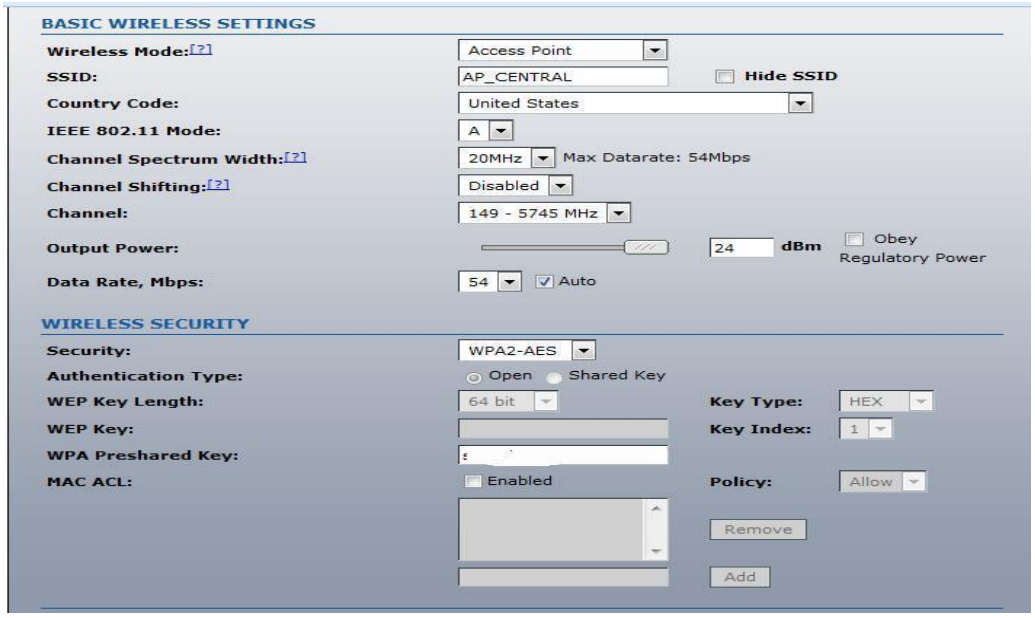


IMAGEN Nº 4: Seguridad de la red inalámbrica
FUENTE: Elaboración Propia

CAPITULO IV

CONCLUSIONES
RECOMENDACIONES

4.1. CONCLUSIONES

Al concluir con el desarrollo del Sistema de control de ingresos a los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando, se puede demostrar que es de gran importancia para la seguridad y el resguardo de todos los bienes de la institución que se encuentran en los laboratorios mencionados.

Con el sistema implementado y en funcionamiento, se ven los siguientes resultados:

- Se realizó el diagnóstico de la situación actual de los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando.
- Se realizó el diseño de la red de control de acceso a los laboratorios de informática.
- Se realizó la instalación de la chapa magnética de puerta biométrica L700 y control de acceso ZKTeco de acuerdo al diseño de la red de control de acceso.
- Se realizó la configuración del control de acceso ZKTeco.
- Se realizó la prueba del sistema de control de acceso a los laboratorios de informática.

Por lo cual se tiene ahora:

"Mayor eficiencia en la vigilancia, monitoreo y administración de los laboratorios de informática del Área de Ciencias y Tecnología de la Universidad Amazónica de Pando".

Esto proporciona:

- Monitoreo constante de los laboratorios de informática permitiendo el ingreso solo al personal autorizado.
- Información oportuna del personal que ingrese a los laboratorios de informática.
- El sistema facilitará la investigación en caso de robo o mal uso de los activos.
- Finalmente se tiene un sistema, que facilita la toma de decisiones de manera oportuna, reduciendo en gran manera los daños económicos que se producen en los laboratorios de informática del Área de Ciencias y Tecnología.

4.2. RECOMENDACIONES

Al culminar este proyecto se plantea las siguientes recomendaciones:

- Continuar con la implementación a medida.
- Permitir el flujo de otro tipo de información en el sistema.
- Implementar una red con fibra óptica para una mejor transmisión de información.
- Implementar un Sistema de Seguridad en el centro de datos.

BIBLIOGRAFIA

Carrillo, A. J, (2011). Sistema automático de control. Recuperado en agosto de 2018; http://150.185.9.18/fondo_editorial/images/PDF/CUPUL/SISTEMA%20DE%20CONTROL%20%201.pdf

Ramírez, T. A, (2005). Sistemas inteligentes. Recuperado en agosto de 2018; http://pedrobeltrancanessa-biblioteca.weebly.com/uploads/1/2/4/0/12405072/sisinteli.pdf

D`Aguila, R. O, (2005). Sistemas inteligentes. Recuperado en agosyto de 2018; http://www.acadning.org.ar/anales/2005/I%20-%20Incorporaciones/Titulares/1.%20DAquila%20-%202005/3.%20Conferencia%20Ing.%20DAquila.pdf

Proaño, R. A, (2016). Sistema basado en conocimiento. Recuperado en agosto de 2018; http://oaji.net/articles/2017/1783-1488462033.pdf

Saavedra, J. J, (2006). Sistema de control de acceso. Recuperado en agosto 2018; http://159.90.80.55/tesis/000132745.pdf

Saavedra, J. J, (2006). Sistema de control de lazo abierto. Recuperado en agosto 2018; http://159.90.80.55/tesis/000132745.pdf

Pérez, M. A, (2007). Sistema de control de lazo cerrado. Recuperado en agosto de 2018; http://dea.unsj.edu.ar/control1/apuntes/unidad1y2.pdf

Gómez, F. E, (2005). Características de un sistema automático. Recuperado en agosto de 2018; http://www.esi2.us.es/~fabio/TransASP.pdf

Saavedra J. J, (2006). Componentes de un sistema de control de acceso. Recuperado en Septiembre de 2018; http://159.90.80.55/tesis/000132745.pdf

Tolosa C. B, (2009). Sistemas biométricos. Recuperado en septiembre de 2018; https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia%20/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Delgado, G. E, (2011). Biometría. Recuperado en septiembre de 2018; https://upload.wikimedia.org/wikipedia/commons/c/ce/Articulo_gerson_delgado_congsistel.pdf

Moreno, I. J, (2017). Funcionamiento de un sistema biométrico. Recuperado en septiembre de 2018; http://repository.udistrital.edu.co/bitstream/11349/7502/1/MarquezMorenoIngridJulieth2017Ni%C3%B1oGarzonMichaelJohanes2017.pdf

(Giz, A. B, (2012). Sensores biométricos. Recuperado en octubre de 2018; https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia%20/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Rosales, A. C, (2009). Clasificación de los sistemas biométricos. Recuperado en octubre de 2018; https://ccc.inaoep.mx/~esucar/Clases-mgp/Proyectos/reporte_modelos_huellas.pdf

Delgado, G. E, (1996). Biometría estática. Recuperado en octubre 2018; https://upload.wikimedia.org/wikipedia/commons/c/ce/Articulo_gerson_delgado_congsistel.pdf

Peralta, D, (2012). Biometría estática. Recuperado en octubre de 2018; http://simd.albacete.org/actascaepia15/papers/00831.pdf

Zuleta, I. M, (2015). Geometría de la mano. Recuperado en octubre de 2018; http://polux.unipiloto.edu.co:8080/00002894.pdf

Correa, A. C, (2013). Reconocimiento Facial Escáner de Rostro. Recupaerado en octubre 2018; https://www.researchgate.net/publication/299497542_Reconocimiento_de_rostros_y_gestos_faciales_mediante_un_analisis_de_relevancia_con_imagenes_3D

Delgado, G. E, (2006). Biometría dinámica. Recuperado en octubre de 2018; https://upload.wikimedia.org/wikipedia/commons/c/ce/Articulo_gerson_delgado_congsistel.pdf

Saavedra, J. J, (2006). Controlo de acceso. Recuperado en octubre de 2018; http://159.90.80.55/tesis/000132745.pdf