Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Reconocimiento biométrico mediante identificación de huella dactilar aplicado a las instituciones educativas escolares

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTORES

Alejandro ARBILDO GRÁNDEZ

Anselmo VALENZUELA ZEGARRA

ASESOR

Armando David ESPINOZA ROBLES

Lima, Perú

2008

Referencia bibliográfica

Arbildo, A. & Valenzuela, A. (2008). *Reconocimiento biométrico mediante identificación de huella dactilar aplicado a las instituciones educativas escolares*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

RESUMEN

RECONOCIMIENTO BIOMÉTRICO MEDIANTE IDENTIFICACIÓN DE HUELLA DACTILAR APLICADO A LAS INSTITUCIONES EDUCATIVAS ESCOLARES.

La presente Tesina trata sobre la aplicación de la biometría dactilar en las Instituciones Educativas Escolares orientado específicamente al control de asistencia del personal docente y administrativo de dichas Instituciones.

La identificación por medio de huellas dactilares constituye una de las formas más representativa de la utilización de la biometría. Una huella digital está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados 'puntos de minucia'. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

Aprovechando esta tecnología se plantea una solución al problema del control de asistencia en las Instituciones Educativas Escolares, que en la mayoría de los casos presenta una serie de deficiencias ocasionando un costo económico y social para el Estado Peruano.

Palabras Claves:

Biometría, Huella Dactilar, Patrón.

SUMMARY

RECOGNITION THROUGH BIOMETRIC IDENTIFICATION FINGERPRINT APPLICABLE TO SCHOOL, EDUCATIONAL INSTITUTIONS STATE

The Tesina present deals with on the application of the digital biometry in the Scholastic Educative Institutions oriented specifically to the attendance control of the educational and administrative personnel these Institutions.

The identification by means of digital tracks constitutes one of the forms most representative of the use of the biometry. A fingerprint is formed by a series of furrows. The completions or bifurcations of the same are called 'points of minucia'. Each of these points has a characteristic and a unique position, that can be measured. Comparing this distribution it is possible to obtain the identity of a person who tries to accede generally to a system.

Taking advantage of this technology a solution to the problem of the control of attendance in the Scholastic Educative Institutions considers, that in the majority of the cases a series of deficiencies presents/displays causing an economic and social cost for the Peruvian State.

Keywords:

Biometrics, Fingerprint, Patterns.

A la memoria de mis padres Alberto y Mercedes, que desde el cielo siempre me iluminan para seguir avanzando a todos aquellos que confiaron en mí infinitas gracias.

Alejandro Arbildo Grández

Gracias a mis padres, esposa por toda su confianza y comprensión.

A Olenka, Piero y Camila, mis hijos que iluminan mi sendero.

Anselmo Valenzuela Zegarra

Un agradecimiento profundo a nuestro asesor Lic.Armando Espinoza Robles por su experiencia, colaboración y disposición para realizar esta investigación.

Los autores

INDICE

INDICE DE FIGURAS, DIAGRAMAS Y TABLAS

.

.

1.-INTRODUCCIÒN

1.1. ANTECEDENTES

Sostener que la biometría es una técnica de identificación futurista, hoy en día no tiene sustento, pues desde hace varios siglos los hombres se han identificado por medio de este sistema. Esta comprobado, que en la época de los faraones, en el Valle del Nilo (Egipto) se utilizaban los principios básicos de la biometría para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

Muchas son las referencias de personas, que en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como eran sus rasgos físicos.

En la cultura China era utilizada desde al menos el siglo XIV para luego tomar presencia en las culturas occidentales a finales del siglo XIX. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En Occidente, la identificación confiaba simplemente en la "memoria fotográfica" hasta que Alphonse Bertillon, jefe del departamento fotográfico

de la Policía de París, desarrolló el sistema antropométrico (también conocido más tarde como Bertillonage) en 1883. Éste era el primer sistema preciso, ampliamente utilizado científicamente para identificar a criminales y convirtió a la biométrica en un campo de estudio.

Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema - principalmente problemas con métodos distintos de medidas y cambios de medida. Después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar, esencialmente el mismo sistema visto en China cientos de años antes.

En estos últimos años la biometría ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas físicas y de comportamiento. Las aplicaciones de la biometría también han aumentado, desde sólo identificación hasta sistemas de seguridad y más.

Una de las muchas aplicaciones que se pueden implementar con la biometría es el control de acceso a un centro de trabajo. En nuestro país encontramos instituciones tales como ONPE entre otras que optaron por implementar sistemas biométricos convencidos de la fiabilidad que ofrecen especialmente en el campo de la identificación.

Las Instituciones Educativas publicas son organizaciones en las que el control de acceso de su personal se realiza en la mayoría de los casos consignando los datos del trabajador , su hora de entrada de salida y su firma ; este sistema es muy vulnerable ya que la hora de entrada y salida puede ser alterada , se presta a la suplantación de personal , muchas veces se pierde la hoja de registro entre otras

deficiencias , es necesario pues la implementación de un sistema fiable y precisamente es aquí donde surge la idea de recurrir a una de las muchas aplicaciones de la biometría .

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. DETERMINACIÒN DEL PROBLEMA

Las Instituciones Educativas públicas son organizaciones sujetas entre otros aspectos a horarios fijos de trabajo surgiendo el problema de cómo controlar en forma eficiente la hora de ingreso y salida de sus trabajadores .Actualmente este control en la mayoría de los casos es de forma manual , el personal registra su asistencia consignando en una hoja de papel sus apellidos y nombres , su hora de ingreso , hora de salida y firma ; esta forma de control es altamente deficiente ya que en muchos casos se modifica la hora real , existe la posibilidad de suplantar a otra persona o en el peor de los casos desaparece las hojas de control de asistencia .Algunas Instituciones Educativas optaron por el uso de tarjetas que también resultan ser vulnerables siendo los casos más resaltantes los de suplantación o pérdida . El otro aspecto donde fallan estos sistemas de control es que al final de cada mes los Directivos de las Instituciones son los encargados de emitir un consolidado a la DREC (Dirección Regional de Educación del Callao) el mismo que en muchas ocasiones es modificado debido a muchos factores tales como estrechas relaciones de amistad con algunos de los personales entre otros. Motivados por la problemática que el uso del control de asistencia del personal en forma manual en la Institución Educativa trae como consecuencia el registro ineficiente del mismo y acarrea perdidas económicas al estado y repercute en el desarrollo académico de las horas efectivas de clase, como se observa en el anexo correspondiente.

Con el propósito de contribuir a un nuevo conocimiento, se propone realizar un estudio, mediante el desarrollo de la presente tesina: En que medida los métodos de control de asistencia del personal docente y administrativo, utilizadas por las instituciones educativas escolares son altamente vulnerables; ocasionando costos económicos y sociales para el estado peruano.

1.2.2. FORMULACIÒN DEL PROBLEMA

¿En qué medida los métodos de control de asistencia del personal docente y administrativo, utilizadas por las instituciones educativas escolares son altamente vulnerables; ocasionando costos económicos y sociales para el estado peruano?

1.3. IMPORTANCIA Y ALCANCES DE LA INVESTIGACIÒN

1.3.1. IMPORTANCIA

La política actual en materia de educación busca entre otros aspectos mejorar la calidad educativa y como una de las medidas que ayudan a este propósito es el control estricto de la asistencia del personal docente y administrativo; sin embargo los métodos de control vigentes son altamente vulnerables.

Tanto los docentes como el personal administrativo registra su hora de ingreso , hora de salida en la mayoría de los casos en forma manual en una hoja de papel , estos datos se guardan diariamente para finalmente realizar un consolidado cada fin de mes y ser enviado a la DREC respectiva , órgano responsable de realizar el pago de los trabajadores ;este sistema presenta una serie de inconvenientes tales como la hora de entrada y salida consignadas son alteradas, existe suplantación de un personal por otro para que firme su asistencia respectiva , desaparece la hoja de registro , al momento de hacer el consolidado existe preferencias y no se informa

con exactitud las tardanzas, faltas , evasiones, ocasionando perdidas económicas ya que se pagan horas no trabajadas y lo más preocupante daño social debido a que se pierden horas de clase necesarias para alcanzar la soñada calidad educativa. Como una alternativa de solución a la problemática expuesta se plantea implementar un sistema biométrico de identificación dactilar. Es evidente que para que las Instituciones Educativas Públicas en el Perú pasan por una crisis en todos los niveles como lo demuestran los indicadores oficiales que se registran a partir de evaluaciones nacionales que ha desarrollado el ministerio de educación y otros organismos internacionales. Al respecto podemos citar algunos indicadores que reflejan la lamentable realidad de la educación secundaria en nuestro país:

"Niveles de desempeño en MATEMATICAS[1] evaluaciones nacionales 2004 en el tercer grado de secundaria: el 6 % de alumnos se hallaba en el nivel suficiente; 19.9% en el nivel básico; 19.0% en el previo y el 55.1 debajo del previo. Los estudiantes de 5° de secundaria: 2.9% en el suficiente; 11.0% en el básico; 17.7 % en el previo y el 68.5 % debajo del previo.En el año 2001 se midió los rendimientos de 4° grado de secundaria, obteniéndose los siguientes resultados: Suficiente 5.2 %; Básico 8.6 % y Bajo 86%".

Asimismo los costos económicos que son afectados al estado es aproximadamente de S/.940,40 al mes, como muestra en la factibilidad.

Estas cifras son sin duda la mejor respuesta a la necesidad de contribuir a que exista un mejor control de asistencia del personal que es uno de los muchos factores que puedan permitir que la educación en el Perú mejore. Por tanto, la presente investigación es importante porque:

[1] Fuente : Evaluación Nacional en Matemática
Recuperado de: www.grade.org.pe

- Tanto los docentes como el personal administrativo registrara su hora de ingreso, hora de salida en forma personal sin suplantaciones.
- Permite que el personal directivo monitoree el movimiento del personal de su institución para la toma de decisiones.

La encuesta realizada en la Institución Educativa refleja una preocupación de la comunidad educativa por mejorar el sistema de control de asistencia vigente por ser vulnerable. (Ver anexos)

1.3.2. ALCANCES

La presente tesina trata sobre el reconocimiento biométrico mediante identificación dactilar aplicado al control de asistencia del personal docente y administrativo de una Institución Educativa, solo involucra el proceso de control de asistencia por lo tanto los resultados que se obtiene están relacionados con este proceso tales como reporte de faltas, tardanzas, permisos , licencias del personal, no abarca la parte correspondiente a los descuentos, sanciones , etc. que se derivan como consecuencia de las faltas o tardanzas , actividades que corresponden al área de recursos humanos del respectivo órgano de control de las Instituciones Educativas como es la DREC.

1.4. LIMITACIONES EN LA INVESTIGACIÒN

La organización en estudio será la Institución Educativa “General Prado” de la Región Callao para la cual se implementará una solución informática al problema de control de asistencia del personal docente y administrativo usando metodología biométrica.

Siendo esta solución a desarrollar un Sistema de Identificación de Personas que mediante el uso de dispositivos lectores de Huellas Dactilares será capaz de validar el acceso al sistema de las personas

autorizadas y además contará con la funcionalidad de mantener un control de asistencia del personal administrativo y docentes.
La investigación será implementado hasta la fase de diseño y elaboración de interfaces del sistema.

1.5. OBJETIVOS: PRINCIPAL Y ESPECÌFICO

1.5.1. OBJETIVO PRINCIPAL

La presente tesina tiene como objetivo brindar una solución informática mediante el uso de tecnología biométrica para controlar la asistencia del personal docente y administrativo y así evitar su vulnerabilidad que actualmente se da mediante el uso de tarjeteros o fichas de control en las Instituciones Educativas públicas de nivel Secundario usando tecnología biométrica.

1.5.2. OBJETIVOS ESPECIFICOS

- Optimizar el control de la asistencia del personal administrativo y docente.
- Facilitar la labor de gestión de las I.E.
- Propiciar el uso de software basado en reconocimiento biométrico en las Instituciones.

1.6. HIPÓTESIS

"El uso de la tecnología biométrica como método de control de asistencia del personal docente y administrativo por las Instituciones Educativas Escolares evitarán su vulnerabilidad, lo cual facilitará la gestión y disminución de los costos económicos y sociales para el Estado Peruano"

1.7. VARIABLES E INDICADORES

1.7.1. VARIABLES

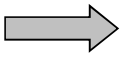
1.7.1.1. VARIABLE INDEPENDIENTE: "Uso de la tecnología biométrica mediante la huella dactilar". (X)

La biometría, es la ciencia aplicada al reconocimiento de las personas por sus características físicas, fisonómicas, dactilares, oculares y cada día se especializa más en distintos parámetros únicos del cuerpo humano**.** Donde la huella dactilar es un patrón para autenticar la identidad de un individuo de forma univoca. Y los datos capturados con los distintos modelos de lectores necesitan ser procesados para recién entonces llegar a convertirse en información (tardanzas, inasistencias, permisos, licencias, etc.)

1.7.1.2. VARIABLE DEPENDIENTE

"Vulnerabilidad del control de la asistencia del personal docente y administrativo de las Instituciones Educativas Escolares" (Y)

La Asistencia del personal es la presencia física en la Institución Educativa para realizar su labor académica y/o administrativa.

X  **Y**

1.7.2. INDICADORES

VARIABLE INDEPENDIENTE: "Uso de la tecnología biométrica mediante la huella dactilar":

- Grado de confiabilidad.
- Nivel de aceptación del dispositivo de identificación dactilar

VARIABLE DEPENDIENTE: “Vulnerabilidad del control de la asistencia del personal docente y administrativo de las Instituciones Educativas Escolares”:

- Nivel de asistencia del personal
- Nivel de horas dictadas del personal docente.
- Grado de Puntualidad del personal.

1.8. POBLACIÒN, MUESTRA

La población y muestra de la investigación, es el alumno, personal administrativo y académico de la Institución Educativa General Prado del Distrito de Bellavista de la Región Callao el cual está distribuido con 160 Docentes y 20 Administrativos.

1.9. PROPUESTA

Mediante este sistema el personal docente y administrativo hará uso de un Terminal provisto de un lector de huella dactilar para luego este dato ser comparado con la base de datos donde se almacenan las muestras de las huellas dactilares de todos los trabajadores y mediante un algoritmo verificar la identificación del trabajador para luego consignar su hora de ingreso o de salida , finalmente el sistema deberá emitir reportes tales como de asistencia de todo el personal , reporte de las tardanzas con la cantidad respectiva de minutos u horas de ser el caso , reporte de faltas entre otros.

1.10. ORGANIZACIÓN DE LA TESINA

La presente tesina presenta la siguiente organización: el primer capitulo denominado introducción nos permite tener un conocimiento del problema planteado y la propuesta de la solución, el segundo capítulo trata sobre el marco teórico, el siguiente capitulo trata sobre el estado del

arte , en este capitulo se hace énfasis a la identificación dactilar y sus diferentes técnicas, a continuación se presenta un caso de estudio cuya estructura consta del análisis y diseño del software respectivo , en seguida se plantea las conclusiones y recomendaciones para finalmente terminar con la bibliografía utilizada .

2. MARCO TEÒRICO CONCEPTUAL

2.1. BIOMETRÌA

El concepto de 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.

"Conjunto de métodos automatizados de identificación y verificación de la identidad de una persona viva, basados en una característica fisiológica. Analiza y mide ciertos rasgos unívocos de un individuo para crear un identificador biométrico**"** [3]. Este identificador puede ser almacenado en una base de datos y recuperado para su comprobación posterior. La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso del reconocimiento de la huella digital, se ha de tener en cuenta que en ningún caso se extrae la imagen de la huella, sino una secuencia de números que la representan. Sus aplicaciones abarcan un gran número de sectores: desde el acceso seguro a computadores, redes, protección de ficheros electrónicos, hasta el control horario y control de acceso físico a una sala de acceso restringido.

Por esta razón la definen como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamientos de enfermedades y otros por el estilo.

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. La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana. La identificación por medio de huellas digitales constituye una de la forma más representativa de la utilización de la biometría. Una huella digital está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados 'puntos de minucia'. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

2.2. TIPOS DE BIOMETRIA

Los tipos de biometría pueden agruparse teniendo en cuenta las características físicas y características del comportamiento de la persona a identificar, según este criterio tenemos:

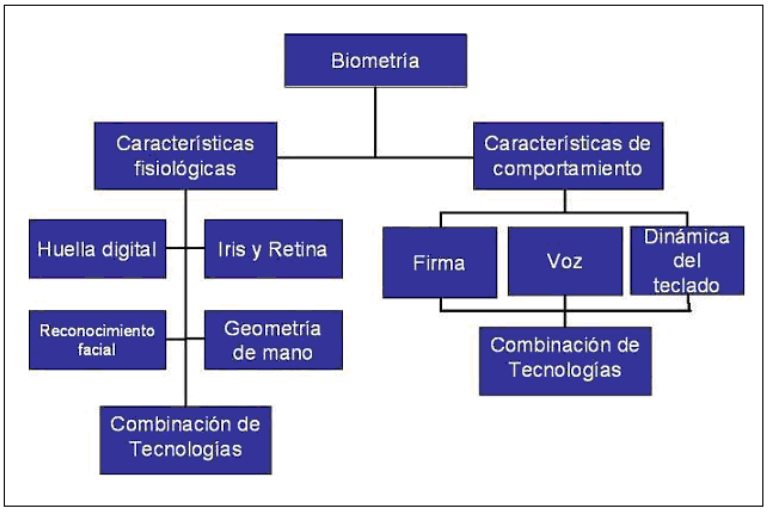


Figura 2.1 Tipos de biometría.

2.3. CONSTITUCIÓN DE UN SISTEMA BIOMÉTRICO

Los sistemas de identificación biométrica están compuestos de tres partes:

- Sistema de captura: Adquiere las características (imágenes o sonidos) a analizar.
- Sistema de proceso: Analiza las imágenes o sonidos y extrae una serie de características, generalmente numéricas.
- Sistema de clasificación: Compara las características extraídas por el sistema de proceso con las almacenadas en el sistema. Si la comparación es positiva (las características extraídas y las almacenadas se parecen suficientemente), se autoriza el acceso.

Dos son los tipos de errores que se pueden cometer en estos sistemas:

- Falso rechazo: Se produce cuando el sistema rechaza a un usuario autorizado. Se cuantifica mediante la probabilidad (o tanto por ciento) de falsos rechazos. Es un error molesto para los usuarios, pero no crítico para la seguridad.
- Falsa aceptación: Se produce cuando el sistema acepta a un usuario no autorizado, y le facilita el acceso. Se cuantifica mediante la probabilidad (o tanto por ciento) de falsas aceptaciones. Es un error crítico para la seguridad.

En términos generales, los sistemas de identificación de usuario se basan fundamentalmente en tres tipos de elementos:

- Algo que el usuario sabe: una contraseña.
- Algo que el usuario posee: una llave, una tarjeta.
- Algo que el usuario es: una característica corporal del mismo.

Los sistemas de identificación biométrica utilizan el tercer elemento para realizar la identificación, aunque pueden combinarse con los otros dos. Tienen la ventaja de que, al ser algo intrínseco al usuario, éste siempre lo lleva consigo (uno puede olvidar una tarjeta o su contraseña, pero no se puede olvidar su huella dactilar, o el timbre de su voz). Además, las posibilidades de falsificación se dificultan considerablemente.

Para que una característica biométrica resulte de utilidad debe cumplir algunas propiedades esenciales:

- Debe permanecer constante con el tiempo en un mismo individuo.
- Debe ser distinta para individuos distintos.
- Debe ser accesible y sencilla de obtener, y la verificación debe realizarse con rapidez. Por ejemplo, una muestra de ADN es perfectamente característica de los individuos, y cumple las dos condiciones anteriores, pero evidentemente la extracción de muestras de ADN y su posterior análisis no cumplen esta tercera condición.

Las características corporales que utilizan los sistemas de identificación biométrica son principalmente:

2.3.1. LA HUELLA DACTILAR

Es la tecnología más asequible, y si a eso añadimos que la probabilidad de igualdad de dos huellas dactilares de personas distintas es extremadamente baja, aproximadamente de 1 en 67 billones, se entiende que sea una de las más empleadas.

Se trata, de hecho, de uno de los procedimientos más antiguos que existen, y uno de los más populares policialmente, como todo el mundo sabe. El funcionamiento básico de un sistema de identificación de huellas dactilares es el siguiente: el usuario pone su dedo sobre un sensor, que captura una imagen de la huella. De dicha imagen se buscan y extraen las características, que son de dos tipos, patrones y minucias.

El patrón hace referencia a la posición de las líneas y valles, mientras que las minucias se refieren a la aparición de singularidades en las líneas, como puntos de bifurcación, cercado, unión, terminación, etc. Dos dedos diferentes nunca pueden poseer más de ocho minucias iguales, y cada uno tiene más de 30 ó 40 minucias.

Los detalles relativos a las líneas (curvatura, separación, etc.), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten componer un índice numérico correspondiente a esa huella. Este índice numérico de la huella es guardado en la base de datos del programa, en una tarjeta u otro tipo de soporte. Es imposible reconstruir la huella a partir del índice registrado en el fichero ya que la información guardada es información numérica (patrones), extraída a partir de la imagen de la huella, no la propia imagen.

Figura 2.2 Huellas dactilares.

Cuando el usuario solicita acceso al sistema, pone su dedo sobre el lector, y su huella dactilar es digitalizada y analizada a fin de extraer los elementos característicos y tras el análisis de las líneas y las minucias se compara el nuevo índice obtenido con el anteriormente almacenado.

Se trata de un tipo de sistema muy fiable. Las tasas de falso rechazo se sitúan por debajo del 1%, y las de falsa aceptación, están alrededor del 0.0001%. Las velocidades de proceso e identificación están por debajo del segundo en sistemas actuales.

2.3.2. LA FORMA DE LA MANO

Estos sistemas obtienen una imagen del perfil de la mano completa, de dos dedos o de un solo dedo, con una cámara convencional o con una cámara infrarroja. Una vez tomada la imagen se extraen una serie de características de la mano y los dedos, como pueden ser longitudes, anchuras, alturas, posiciones relativas de dedos, articulaciones, disposición de venas, etc. Esas características se transforman en una serie de patrones

numéricos, que luego se comparan con los patrones previamente almacenados.

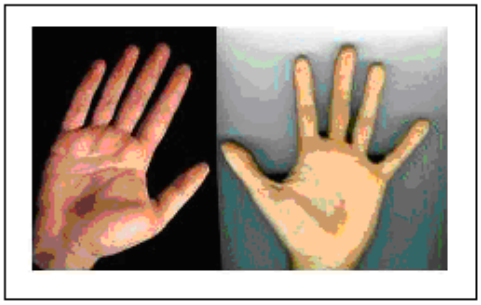


Figura 2.3 Palma de la mano

Uno de los primeros usos de este sistema fue en los juegos olímpicos de 1996. También se está empezando a utilizar como alternativa al número de identificación personal en operaciones con tarjetas de crédito.

Los sistemas comerciales presentan tasas típicas de falso rechazo en torno al 0.1 % y de falsa aceptación en torno al 1%.

Una variante de este sistema toma una imagen de la palma de la mano, y sus líneas y detalles se analizan con procedimientos semejantes a los sistemas de identificación de huellas dactilares.

2.3.3. EL PATRÓN DEL IRIS

El iris es la franja de tejido coloreado que rodea nuestra pupila. Aunque lo que más resalta es su color, un estudio cercano de la misma muestra un conjunto de rasgos característicos, como pueden ser estrías, anillos, surcos, texturas, etc. Este patrón es diferente de un individuo a otro pero en un mismo individuo no cambia con el tiempo.

El sistema adquiere una imagen del iris y transforma las características anteriormente mencionadas en patrones numéricos, que se contrastan con los previamente almacenados. Concretamente, una cámara de reconocimiento de iris toma una fotografía del mismo. Las cámaras

cumplen los estándares internacionales de iluminación segura, y utilizan un método de iluminación de longitud de onda cercana al infrarrojo que es escasamente visible y muy seguro. La imagen del ojo es primeramente procesada por un programa que localiza el iris. Luego, un programa codifica los patrones del ojo creando un código para la secuencia de texturas y rasgos característicos del iris.

Figura 2.4 .Patrón iris.

2.3.4. PATRONES DE VENAS DE LA RETINA

En esta técnica se examina el fondo del ojo y se detectan los patrones de venas que se extienden por la retina. Son también característicos y estables en cada individuo, y permiten diferenciar unos individuos de otros.

En los sistemas biométricos basados en patrones de vasos de la retina, el usuario mira a través de unos binoculares, realiza algunos ajustes, mira a un punto determinado y por último pulsa un botón. El sistema toma una imagen de la retina con una radiación infrarroja segura, de baja intensidad, detectando la estructura de vasos sanguíneos de la retina y transformándola en una serie de características numéricas para compararlas con las almacenadas.

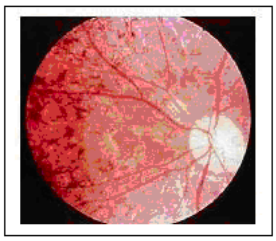


Figura 2.5. Patrones de venas de retina.

Uno de los inconvenientes de esta técnica es que el individuo la siente como más invasiva (debe iluminarse con luz el fondo del ojo), lo cual puede acentuar la prevención por parte de los usuarios.

Se trata de un sistema bastante fiable. La probabilidad de falso rechazo está en torno al 1%, y la de falsa aceptación, por debajo del 0,001%.

2.3.5. RECONOCIMIENTO DE VOZ

En este sistema se adquiere la voz del usuario utilizando un micrófono, y seguidamente se analiza mediante un ordenador. Se buscan principalmente patrones de intensidad y frecuencia.

Existen dos tipos principales:

- De texto dependiente, en los que el reconocimiento se basa en un conjunto muy limitado de frases estándar.
- De texto independiente, en los que la variedad de frases es mucho más amplia. De hecho el sistema va proponiendo al usuario que diga varias palabras extraídas de un conjunto bastante grande.

Se trata de un sistema poco costoso de implementar, por lo que se encuentra muy extendido. Sin embargo, uno de los problemas que frenan su difusión es que se trata de una tecnología todavía propensa a errores. La probabilidad de falso rechazo está en torno al 3%, y la de falsa aceptación, en valores algo superiores al 1%. Podemos citar algunas de sus aplicaciones concretas:

- La empresa General Motors utiliza estos sistemas para el acceso a sus centros de cómputo.
- El hospital de Chicago lo utiliza para el acceso a la sala de recién nacidos.

- El control de inmigraciones en la frontera de EEUU y México utiliza este sistema para el reconocimiento de pasajeros frecuentes.
- Se utiliza en aplicaciones de seguridad telefónica.

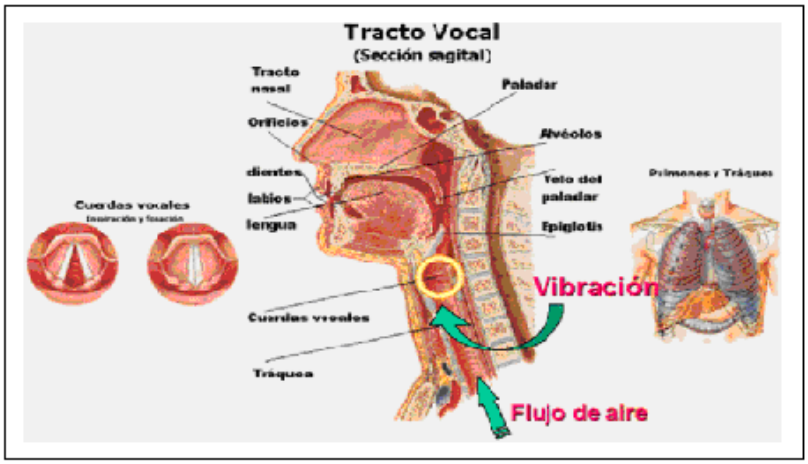


Figura 2.6 .Reconocimiento de voz.

2.3.6. RECONOCIMIENTO FACIAL

Se trata de un sistema de desarrollo relativamente reciente. Se toma una imagen de la cara de una persona (a veces se pueden tomar varias, de frente y de perfil), y se analizan las imágenes para extraer determinados parámetros, como forma general de la cara, curvaturas, situación absoluta y relativa de ojos, nariz y boca, marcas notables, etc. Esos parámetros se comparan con los almacenados en una base de fotografías o imágenes de usuarios autorizados (o no autorizados).

, "Las características de la cara, como una nariz grande o las cejas marcadas, no cambian fácilmente con el envejecimiento... el sistema registra y lee las características únicas de una cara, usando una tecnología similar a la del reconocimiento de billetes y monedas". El sistema funciona comparando la imagen de la cara con fotos almacenadas, y, según ha anunciado Hitachi estará disponible comercialmente Japón en el año 2005.

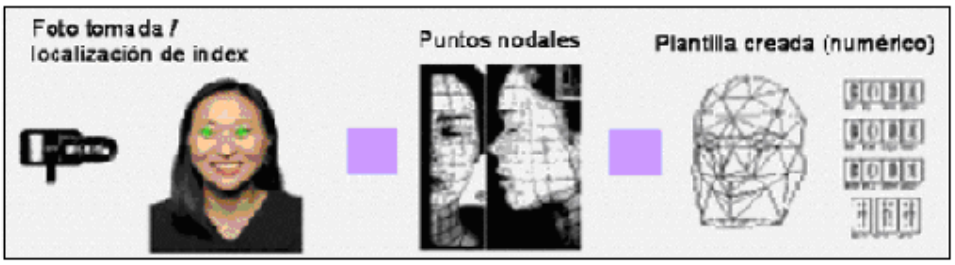


Figura 2.7 .Reconocimiento facial.

2.3.7. VERIFICACIÓN DE ESCRITURA

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 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. 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.

2.3.8. RECONOCIMIENTO DE FIRMA

Esta tecnología biométrica se puede dividir en dos grandes áreas: métodos estáticos (algunas veces llamados no en línea) y métodos dinámicos (algunas veces llamado en línea). Los métodos estáticos verifican características de la firma que no varían con el tiempo, en esta caso es una tarea de reconocimiento de patrones y los métodos dinámicos verifican características dinámicas en el proceso de la firma.

El proceso de la firma se origina en unas propiedades intrínsecas del sistema neuromuscular del ser humano, que produce los movimientos rápidos.

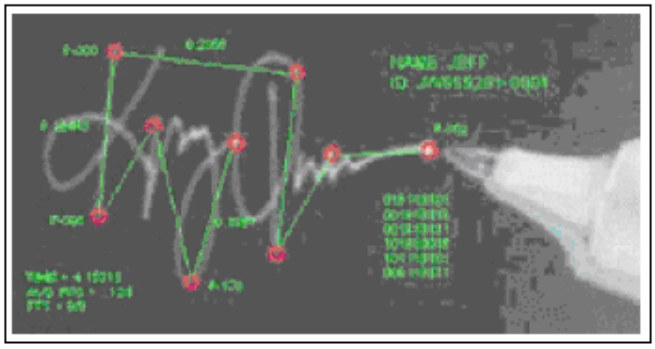


Figura 2.8 .Reconocimiento de firma.

2.3.9. RECONOCIMIENTO VASCULAR

Esta tecnología biométrica es de reciente desarrollo y también se conoce como reconocimiento del patrón de venas de la mano. Al igual que el reconocimiento de retina esta tecnología usa luz infrarroja a corta distancia para detectar los patrones de la red vascular, actualmente también se esta extrayendo patrones vasculares de otras partes del cuerpo y están estandarizados en la norma ISO/IEC 19794-9 los patrones vasculares de la palma de la mano, reverso de la mano y dedo.

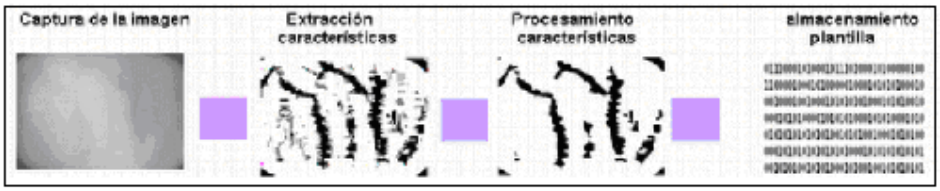


Figura 2.9 .Reconocimiento vascular.

2.3.10. RECONOCIMIENTO HUELLA DEL PABELLÓN AURICULAR

Esta tecnología biométrica se ha desarrollado para la medicina legal y forense especialmente, es una reproducción bidimensional del pabellón auricular y se maneja de manera similar a la huella digital o huella palmar. Para su desarrollo la Unión Europea creo un grupo de investigación (FEARID) que tenia como fin el desarrollo de esta tecnología en un periodo de 40 meses.

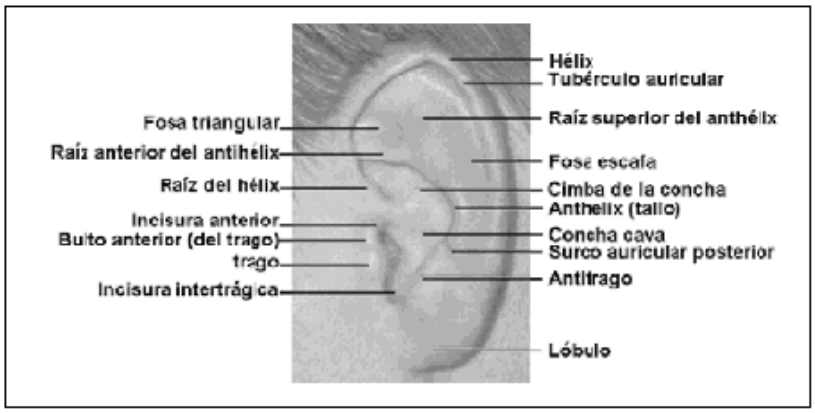


Figura 2.10 .Pabellón auricular.

2.3.11. RECONOCIMIENTO DE PATRONES DE TIPEO

Es un tipo de biométrico conductual usado para verificar la identidad de un individuo examinando sus patrones de tipeo en un teclado. Esta tecnología se sostiene sobre la premisa de que cada individuo exhibe un

patrón distintivo y una cadencia de tipeo. La mayoría de los estudios usan la duración entre tipeo (latencias) como característica de verificación de usuario, aunque hay otros que utilizan el tipo que permanece la tecla presionada. Esta tecnología no requiere de hardware adicional o dispositivo de captura, se soporta sobre un software de captura de la dinámica de tipeo del teclado. Esa tecnología usa clasificadores bayesianos, redes neuronales y sistemas fuzzy.

De acuerdo a los estudios realizados hay mejores resultados usando los tiempos de presión de la tecla que los tiempos de latencia, pero los mejores resultados se obtienen del uso simultáneo de ambas técnicas.

Figura 2.11. Patrones de tipeo.

2.3.12. RECONOCIMIENTO DE MARCHA

Es un tipo de biométrico conductual usado para verificar la identidad de un individuo examinando su patrón de marcha. La ventaja de este biométrico es que potencialmente puede realizar reconocimiento a distancia o a baja resolución. El reconocimiento puede basarse en la figura humana (estático) así como en su movimiento. El progreso en este tipo de biométricos ha sido bastante acelerado desde juegos de datos limitados hasta grandes bases de datos del mundo real con análisis de factores independientes.

Figura 2.12. Reconocimiento de marcha.

Hasta ahora, hemos comentado las características biométricas susceptibles de ser utilizadas en un sistema de reconocimiento, y hemos descrito brevemente algunos de estos sistemas. Pero, para que estos sistemas se implanten y se utilicen de forma regular, es necesario que cuenten con la confianza de los usuarios. Ello implica que el sistema debe considerar aspectos como:

- Probabilidad de fallos (falsos rechazos y falsas aceptaciones). Ya hemos hablado de cifras al considerar cada uno de los sistemas anteriores. Estabilidad, o robustez del sistema a cambios (normales) en la característica biométrica que mide. Nos referimos, por ejemplo, a cambios en el timbre de voz por un catarro, o a cambios en las características de las manos o de la cara debidas a heridas, etc.
- Comodidad y facilidad de uso del sistema por parte de los usuarios.
- Aceptación de los usuarios de que sus datos biométricos no serán accesibles por terceros.
- Posibilidad de engañar al sistema, obteniendo autorización suplantando una identidad verdadera, es decir, suplantando una característica biométrica.

La tabla que sigue resume de una forma cualitativa los parámetros que pueden resultar de interés en la aceptación, implantación y uso de los sistemas biométricos.

	Huellas Dactilares	Mano	Iris	Retina	Cara	Voz
Fiabilidad	+++	+++	++++	++++	+++	+++
Estabilidad	+++	++	+++	+++	++	++
Comodidad	+++	+++	++	+	+++	+++
Aceptación	++	+++	++	++	++	+++
Seguridad	+++	+++	++++	++++	+++	++

Tabla nº 1. Comparacion cualitativa de los sistemas biometrico.

Los dos últimos puntos mencionados anteriormente merecen un comentario especial. En los sistemas de identificación biométrica, no se almacenan las características biométricas de los usuarios directamente. Es decir, no se almacena directamente su huella dactilar, o una imagen de su iris, sino que lo que se almacena son las características numéricas necesarias para realizar la identificación, que se obtienen tras procesar las características biométricas directas. Por ejemplo, de una huella dactilar se almacena una serie de números con la posición absoluta y relativa de las minucias, códigos con el tipo de minucia, etc. Es imposible reconstruir, con sólo esa información numérica, la huella dactilar original. Cabe además la posibilidad de incluso cifrar esa información numérica. En cuanto a la seguridad, y a la posibilidad de "engañar" al sistema hoy en día cualquier sistema biométrico (exceptuando algunos modelos de reconocimiento de voz) es robusto frente a los ataques basados en suplantación (por ejemplo, utilizando partes del cuerpo amputadas al usuario legítimo). La mayor parte de los analizadores de huellas dactilares, de iris, de retina o de la geometría de la mano son capaces, además de decidir si la característica biométrica es de un usuario autorizado, de discriminar si éste está vivo. No obstante, no conviene bajar la guardia, puesto que cualquier sistema es, al final susceptible de ser burlado.

Las tecnologías biométricas de mayor uso hoy y con más apoyo por las industrias comerciales son: la huella digital, el reconocimiento facial, la geometría de la mano, el iris, la voz, la firma.

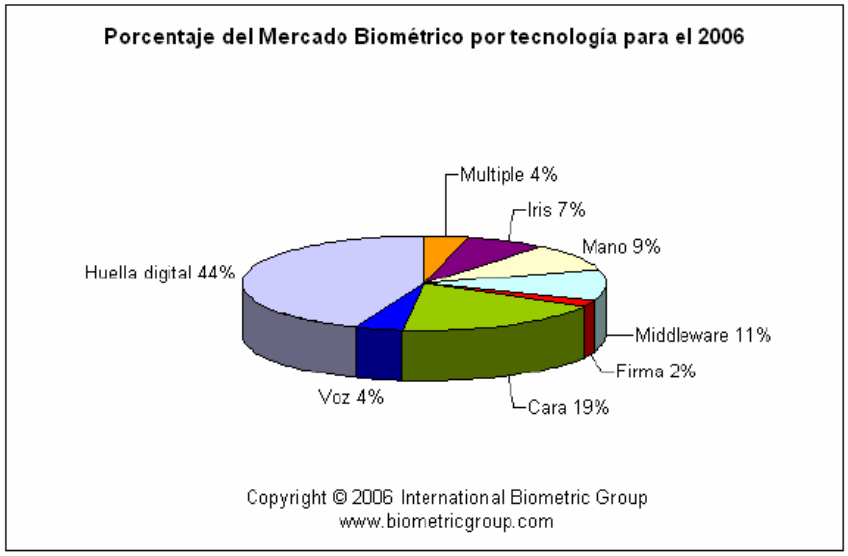


Figura 2.13 Cuadro comparativo del uso de las tecnologías biométricas.

.

.

3. ESTADO DEL ARTE

3.1. LAS HUELLAS DACTILARES EN LA IDENTIFICACIÓN BIOMÉTRICA

De todos las formas de identificación biométrica la huella dactilar es la más aceptada y a través de todo el tiempo de su uso se a podido comprobar que es un medio seguro de identificar a personas, ya que esta comprobado que dos dedos nunca tendrán huellas similares ni siquiera en gemelos y muchos menos una misma persona.

La huella dactilar es un buen patrón para determinar la identidad de un individuo de forma univoca.

"Toda huella presenta como característica principal, la presencia de un conjunto de crestas o partes donde la piel se eleva sobre las partes más bajas o valles existentes entre las crestas. Con respecto a estas crestas se definen dos características particulares que obedecen al término de minucias:

- Final de cresta (ridge ending). Característica definida como el punto donde la cresta acaba de forma abrupta.
- Bifurcación de la cresta (ridge bifurcación). Característica definida como el punto en el que la cresta se bifurca en dos o más crestas.

Estas dos características quedan unívocamente definidas a partir de su localización (coordenadas x, y respecto al sistema de coordenadas central de la imagen) y de su orientación"[11].

El número típico de minucias por huella oscila entre 30 y 45, siendo demostrado que el número máximo de minucias en común nunca sobrepasa las 8 minucias. [19]. (*Ver figura Nº 3.1*)

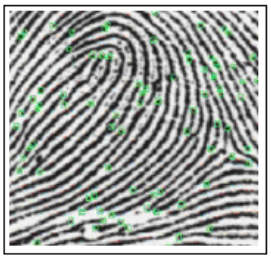


Figura 3.1 Huella digitalizada con minucias.

En la figura 3.1 “se muestra la imagen de una huella digitalizada con sus minucias, las cuales permiten la identificación biométrica a través de la huella” [7]

3.2. CLASIFICACION DE LAS HUELLAS DACTILARES.

Un sistema biométrico es aquel que puede medir las características de una persona y verificar su identidad el cual debe tener todos estos elementos:

- Universalidad: Cada persona registrada en el sistema debe poseer esta característica.
- Unicidad: Dos personas no pueden tener las mismas características en cuanto a la medición de ciertos parámetros dependiendo del sistema.
- Permanencia: Esta característica debe ser invariable en el tiempo.
- Cuantificación: Estas características pueden ser medidas de manera objetiva.

La huella dactilar posee todas las características anteriores; además ha sido usada a lo largo de la Historia y de la cual se han publicado diversos estudios sobre sus características y tipos, entre las más importantes están las publicadas por F. Galton y E. R. Henry al final del siglo XIX.

En el estudio de F. Galton las huellas dactilares son examinadas morfológicamente y los experimentos fueron hechos en grupos de

diferentes edades y diferentes razas .Dos conclusiones importantes fueron hechas:

- Las huellas dactilares son permanentes en forma y características desde el nacimiento hasta la muerte;
- Las huellas dactilares son únicas; es decir no existen dos individuos con las mismas huellas dactilares.

El estudio de E. R. Henry examinó la estructura global de la huella dactilar:

- Right Loop,vuelta derecha (R)
- Left Loop ,vuelta izquierda (L)
- Whorl , espiral (W)
- Arch, Arco (A)
- Tented Arch,Arco tendido (T)

Además existe la clasificación realizada por el FBI, según la figura 3.2

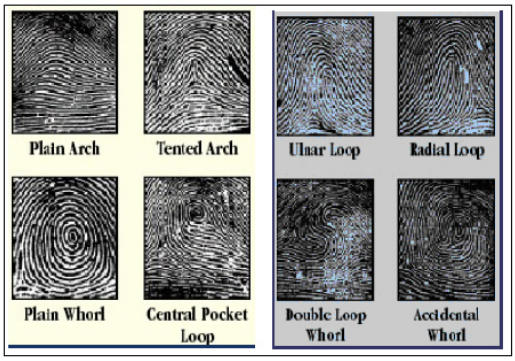


Figura 3.2.-Tipos de huellas digitales. Clasificación FBI

En la extracción de características de las huellas dactilares se utilizan ciertos puntos llamados ridges (crestas) , los cuales son como un segmento de curva simple.

Las huellas dactilares cuentan con otros puntos características llamados puntos core (central) y delta (Δ, letra griega) .El punto core es usado como una referencia en la codificación de otros puntos característicos de la huella dactilar llamados minucias .

3.3. EL PROCESO DE LA IDENTIFICACIÓN BIOMÉTRICA DACTILAR

El proceso general de identificación que sigue el sistema biométrico dactilar es: captura de los datos de la persona a identificar a través del dispositivo biométrico, extracción de minucias de la huella dactilar, comparación de las minucias extraídas contra las almacenadas en una base de datos a través de un algoritmo de comparación y la decisión de la comparación que dirá si la persona puede ser identificada o no.

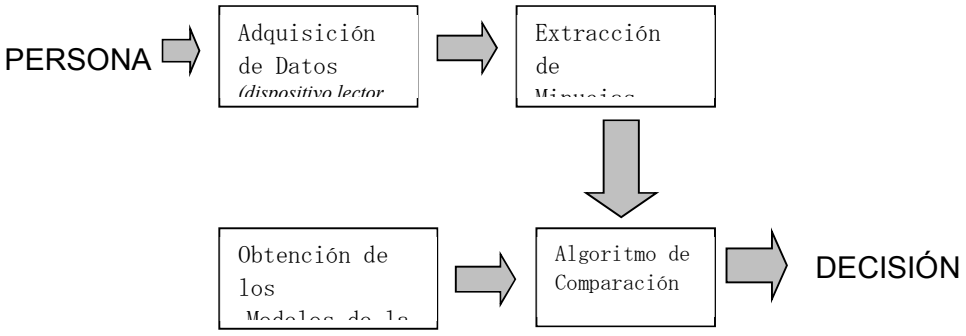


Figura 3.3 Proceso clásico de reconocimiento biométrico

En la figura 3.3 se muestra el proceso clásico que usa los sistemas de reconocimiento biométrico dactilar.

En este proceso de identificación cabe la posibilidad de tener errores, siendo los más probables a error, la captura y la toma de decisión, ya sea porque no puede llevar acabo una captura limpia de la huella por encontrase esta con imperfecciones u porque el dispositivo se encuentra deteriorado o porque rechaza a una persona que debió haber sido identificada o por identificar a una persona a la cual no debió.

"Es en la decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico: las tasas de falso rechazo y de falsa aceptación" [12].

3.4. TIPOS DE SISTEMAS EXISTENTES DE IDENTIFICACIÓN MEDIANTE HUELLAS DACTILARES

Básicamente los sistemas biométricos basados en huellas dactilares son de dos tipos [6]:

3.4.1. AUTOMATIC FINGERPRINT AUTHENTIFICATION SYSTEM (AFAS).

En un sistema AFAS la entrada es la huella dactilar y la información del individuo, la salida es la respuesta “si” o “no”, indicando si la imagen de entrada (huella dactilar) pertenece o no al individuo cuya información ha sido dada la cual esta almacenada en la base de datos. Ver figura 3.4

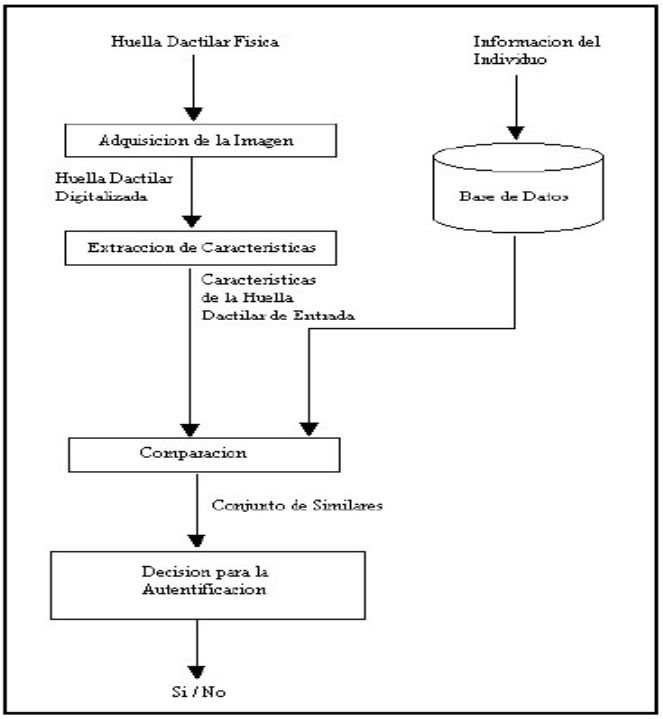


Figura 3.4 Diagrama de bloques de un sistema AFAS.

3.4.2. AUTOMATIC FINGERPRINT IDENTIFICATION SYSTEM (AFIS).

En un sistema AFIS la entrada es una huella dactilar y la salida es una lista de identificadores de personas que pueden tener la huella dactilar

dada , dependiendo de la puntuación en cuanto a similitud de la huella de la entrada con la almacenada en la base de datos , como se puede observar en la figura 3.5

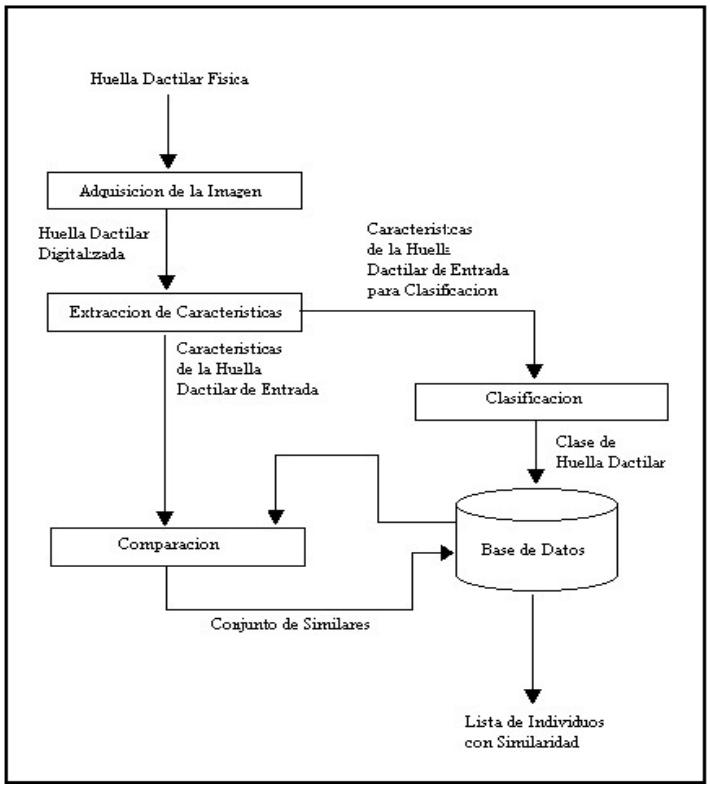


Figura 3.5 Diagrama de bloques de un sistema AFIS.

3.5. CARACTERISTICAS DE LAS HUELLAS DACTILARES

La representación mas comúnmente usada en la identificación de las huelas dactilares son las características de Galton. Una cresta está definida como un segmento de curva y un valle es la región entre dos crestas adyacentes.

Las discontinuidades locales tienen el nombre de minucias que es un término utilizado en la Medicina Forense y que significa “punto característico”, las cuales podemos observar en la figura 3.6

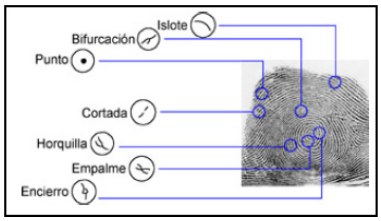


Figura 3.6 Tipos de minucias en una huella dactilar.

En una huella dactilar existe un aproximado de 50 a 150 minucias y dependiendo de la cantidad de registros en una base de datos con 10 comparaciones de minucias puede ser suficiente para comprobar la identidad de un individuo; pero solo en bases de datos pequeñas.

Habiendo detectado las minucias, se procede a crear un modelo con los puntos en coordenadas cartesianas bidimensionales (Ver figura 3.7) de la localización de las minucias , los cuales sirven para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible .

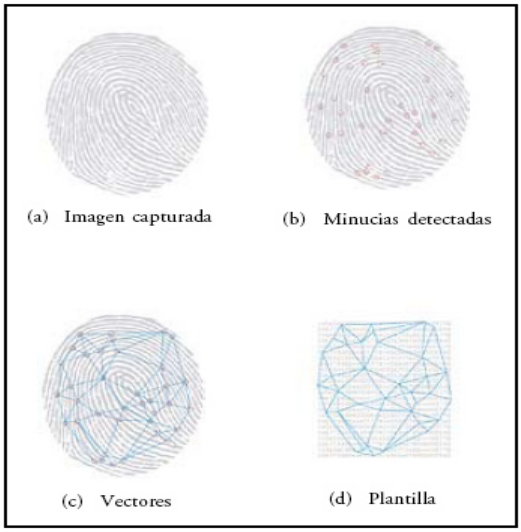


Figura 3.7 Proceso de modelado de coordenadas cartesianas.

3.6. APLICACIONES QUE SE LES PUEDE DAR A LOS SISTEMAS DE IDENTIFICACIÓN MEDIANTE HUELLA DACTILAR.

En las aplicaciones de cómputo actuales y en muchas de las actividades cotidianas, como puede ser el registro de personal, en donde las personas requieren interactuar entre ellas o confirmar su identidad a través de la computadora, usualmente no se tiene medios de identificación completamente seguros, ya que en muchos casos estos se reducen a contraseñas, números o datos personales que son riesgosos de manejar o que puedan olvidarse, o a credenciales que pueden extraviarse, duplicarse o transferirse a terceros para tener acceso a beneficios, instalaciones, etc.

La tecnología biométrica ha traspasado los laboratorios de espionaje, recintos militares y gubernamentales para extender sus aplicaciones al mercado empresarial y de consumo.

En el mercado tecnológico se pueden encontrar gran cantidad de productos biométricos los cuales pueden ser utilizados para proporcionar seguridad, reemplazando a los sistemas tradicionales de seguridad. Muchas empresas implementan sus sistemas con seguridad biométrica ya sea por medio de la voz, reconocimiento del iris, el tacto, la huella dactilar u otra forma de reconocimiento biométrico.

En vista que algunos de estos productos biométricos son relativamente muy costosos, son pocas las empresas que los adquieren.

Los biométricos Dactilares gracias a sus prestaciones y capacidades, son los biométricos actualmente mas usados, los cuales por su uso se agrupan en dos áreas:

- Seguridad, para la identificación de personas.
- Criminalística, como método de identificación.

Además de los anteriores tenemos:

ACCESO FÍSICO:

Por varias décadas, instalaciones de seguridad han utilizado la tecnología biométrica dactilar para los accesos de entrada. Actualmente, su uso principal es: acceso a recintos privados como edificios, oficinas, etc. Los biométricos permiten accesos seguros sin la presencia de un guardia

de seguridad, permitiendo una automatización tanto de software y hardware.

ACCESO VIRTUAL:

Actualmente, el método de seguridad más usado para el acceso a PCs y redes es la introducción de la contraseña. Sin embargo, la contraseña brinda una seguridad mínima para la protección de la información., los biométricos de reconocimiento dactilar están logrando un gran auge brindando una mayor seguridad a los datos, porque la seguridad no está basada en lo que usted sabe, sino en quién es.

ENCRIPTACIÓN Y SEGURIDAD DE ARCHIVOS:

Cada día se necesitan nuevas técnicas para dar seguridad a nuestros datos almacenados y enviados por la red, para ello, la Biometría Dactilar nos permite aumentar la seguridad del proceso de encriptación y desencriptación de los mismos. [2]

APLICACIONES DE COMERCIO ELECTRÓNICO

Las tecnologías ampliaron los mercados a la Web, realizándose transacciones en la cual es necesario que la persona se identifique, pero ¿cómo sabemos que alguien al cual no vemos es quien dice ser?, es aquí donde la biometría interviene, ayudando a identificar a las personas por medio de su huella dactilar.

CONTROL DE ASISTENCIA

Los antiguos tarjeteros, fotochecks con códigos de barras, banda magnéticas o tarjetas de proximidad, todos aquellos que se basan en algo que el empleado posee, pero que puede ser prestado, olvidado, robado o perdido y sin tener la certeza que la persona que lo presenta es el usuario auténtico, siendo por tales motivos el sistema burlado, es que se ha

integrado a estos sistemas la biometría dactilar la cual nos permite solucionar dichos problemas.

OTRAS APLICACIONES:

- Control de Votaciones.
- Procesos de Admisión.
- Sistemas de prevención en los aeropuertos.
- Exámenes (para evitar suplantaciones)
- Cobros y Tramites Documentarios
- Seguridad de dispositivos de uso privado (teléfonos, computadoras, etc.)
- Votación Electoral
- Entre otros

3.7. VENTAJAS DE LA IDENTIFICACIÓN DE PERSONAS MEDIANTE EL RECONOCIMIENTO DACTILAR

De todos los biométricos disponibles, incluyendo el escaneo de la cara, el iris y la retina, o la identificación de voz entre otros, la huella dactilar es uno de los más convenientes y seguros.

Las ventajas del biométrico de huella dactilar para la identificación de personas incluyen:

- Se tiene una cantidad significante de información en cada huella como para poder basarnos en ésta y asegurar la unicidad y autenticidad de cada huella.
- Todas y cada una de nuestras diez huellas digitales es única, diferente una de otra y a su vez distinta de las huellas de cualquier otra persona.
- A diferencia de las contraseñas, números de identificación (utilizados en tarjetas de crédito) y smart cards, de las que dependemos en estos días para identificarnos, nuestras huellas

dactilares no se pueden perder u olvidar y nunca pueden ser robadas.

- Tenemos diez huellas, pero solo una voz, una cara o dos ojos.
- Las personas que lo utilizan, no le tienen temor alguno como a otros biométricos que piensan que les puede causar algún daño futuro por su constante uso.

"Aunque existen diversos términos en el manejo de huellas dactilares, lo importante es saber que existe la suficiente información en cada huella para certificar la identidad de una persona" [15].

3.8. MÉTODOS DE RECONOCIMIENTO DE HUELLA DACTILAR

Los métodos existentes para almacenar y posteriormente comparar las plantillas de las huellas dactilares almacenadas en un repositorio de datos contra la capturada in-situ de la persona a identificar, son: el método basado en patrones y el método basado en minucias.

Actualmente, el reconocimiento de huellas dactilares, es la técnica biométrica más popular usada en la identificación y verificación automática de personas. Estos sistemas están siendo usados en diversas aplicaciones, tales como: control de acceso a instalaciones de alta seguridad, identificación de criminales por varios departamentos forenses alrededor del mundo, verificación de tarjetas de crédito, identificación de empleados, etc. [16].

Un sistema de reconocimiento de huellas dactilares consta de 4 etapas: Adquisición de la Imagen, Pre-procesamiento de la Imagen, Extracción de características y Matching o Reconocimiento [9].

La extracción de características es la etapa primordial en el reconocimiento de huellas dactilares, por lo tanto mientras más confiable sea el método utilizado en esta etapa, obtendremos un mejor rendimiento del sistema. Existen 2 enfoques para la extracción de características: enfoque basado en minucias y el enfoque basado en la imagen [9].

Se denominan minucias a las características locales de una huella dactilar, denominadas terminaciones de las crestas (ridge ending) y bifurcaciones de las crestas (ridge bifurcación), las cuales forman un único patrón para cada huella dactilar. Los enfoques basados en minucias son los más populares y los que implementan la mayoría de los sistemas automáticos de identificación y verificación de personas en la actualidad. Estos enfoques requieren extensivas operaciones de pre-procesamiento con la finalidad de extraer las minucias. Las operaciones de pre-procesamiento incluyen: realce de la imagen, estimación del flujo de orientación, segmentación y adelgazamiento de crestas [8]. Además, se requiere una etapa de postprocesamiento con el objetivo de reducir el número de minucias falsas erróneamente detectadas por la presencia de ruido en las imágenes de huellas dactilares [13].

Actualmente, existen diversos métodos basados en minucias y la mayoría de ellos siguen el proceso descrito anteriormente. Así tenemos que el método clásico basado en la extracción de minucias es el modelo más utilizado por la mayoría de sistemas de reconocimiento de huellas dactilares, sin embargo este método presenta una serie de deficiencias. En primer lugar antes de extraer las características de la huella dactilar, se requiere de un pre-procesamiento de la imagen, el cual consiste en mejorar la calidad de la misma. Por otro lado, luego de extraer las características, se debe realizar un post-procesamiento, el cual consiste en eliminar minucias falsas [9].

Sin embargo, existen métodos más robustos para extraer las minucias de una huella dactilar.

Así tenemos el método basado en agentes. Se ha demostrado que es una buena política seguir las crestas de una huella dactilar hasta que una minucia es hallada. Maio y Maltoni [14] presentaron un agente que toma pequeños pasos a lo largo de la cresta. Jiang et al. [4] mejoró el agente usando un paso de tamaño variable y un filtro direccional para la eliminación de ruido. Una solución mucho más simple es utilizar un agente

que aprende la tarea previo entrenamiento usando aprendizaje por refuerzo [1].

Los métodos basados en agentes buscan reducir el tiempo de procesamiento de la extracción de minucias así como el número de minucias falsas detectadas. Uno de los métodos más recientes basados en agentes es aquel dónde se utilizan agentes reactivos, los cuales son usados sobre la imagen de la huella digital ya adelgazada. Ellos detectan locaciones de interés que podrían ser minucias usando un coeficiente muy eficaz. Luego, varios agentes corren a través de la imagen, empezando por las locaciones de interés, para determinar si ellas son minucias reales o no. El método anteriormente descrito permite disminuir el tiempo de identificación o verificación de un sistema biométrico basado en huellas dactilares.

Se debe tener en cuenta que aunque los sistemas de reconocimiento de huellas dactilares son los sistemas biométricos más populares y que como consecuencia de esto es una de las áreas más estudiadas, todavía existe mucho por investigar así como diversos métodos que perfeccionar, por lo que se le considera un campo abierto en la actualidad y de gran impacto en la sociedad.

3.8.1. MÉTODO BASADO EN PATRONES O IMAGENES

Un dispositivo lector toma una imagen gráfica de la huella dactilar. La imagen gráfica recién obtenida del lector es conocida como una lectura en vivo (live scan) para distinguirla de una plantilla o huella almacenada en una base de datos. Un software de procesamiento examina la imagen de la huella digital y ubica el centro de la imagen, el cual podría ser distinto al centro de la huella digital. Luego se recorta la imagen a una distancia definida alrededor de ese centro de la imagen. El rectángulo de la figura adjunta muestra esta región recortada. La región recortada se comprime, se almacena y es clasificada para posteriores comparaciones.

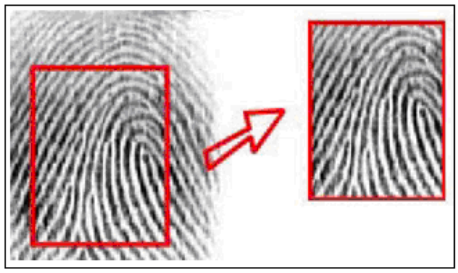


Figura 3.8.-Plantilla basada en patrones

Este proceso consiste en ubicar una huella dentro de los varios tipos existentes, los cuales son clasificados de acuerdo al número y dirección de crestas presentes en: Anillo de crestas, Lado derecho, Lado izquierdo, Arco, Arco de capa.

Las comparaciones de huellas digitales con plantillas basadas en patrones implican realizar una comparación gráfica de las dos plantillas y determinar una medición de la diferencia. Mientras más grande es la diferencia, menos concuerdan las huellas, es decir, consiste en ubicar una huella dentro de las varias plantillas existentes.

3.8.2. MÉTODO BASADO EN MINUCIAS

Tal como en el método basado en patrones, en el método basado en minucias un dispositivo lector toma una imagen gráfica de la huella dactilar (lectura en vivo). Un software especial analiza la imagen para determinar si realmente contiene la imagen de una huella dactilar, luego determina la ubicación del centro de la huella, el tipo de patrón (por ejemplo, de arco a la izquierda, de remolino u otro), estima la calidad de las crestas y finalmente extrae las minucias.

Vistas desde una perspectiva sencilla, las minucias indican dónde ocurre una variación relevante en la huella. Estas variaciones se muestran en la figura siguiente: [17]

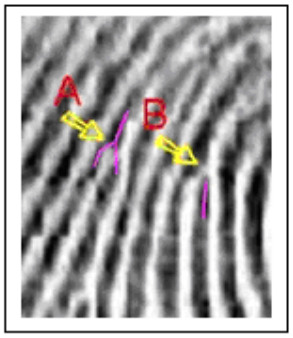


Figura 3.9 Cambios en la huella dactilar

Entendiéndose que las líneas oscuras de la imagen representan las crestas y las líneas claras representan los surcos, la flecha A muestra una región donde una cresta se divide en dos crestas (conocida como una bifurcación) y la flecha B muestra dónde termina una cresta.

Luego de reconocer estas variaciones en la huella digital, el software de extracción de minucias determina una orientación de estas variaciones (usando la flecha B como ejemplo, la orientación comienza al final de la cresta y se mueve hacia abajo).

Las minucias resultantes, en su forma más sencilla, son una colección de todas las bifurcaciones y finales de crestas, teniendo en cuenta su ubicación y su orientación.

La figura siguiente muestra un conjunto de minucias.

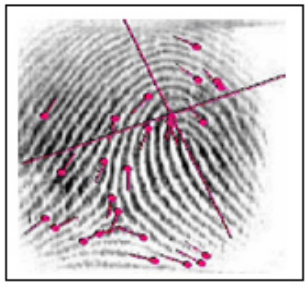


Figura 3.10.- Eje y minucias extraídas

Adicionalmente, el software de extracción de minucias coloca un eje de coordenadas sobre la huella, posicionándolo de tal forma que el centro del eje esté sobre el núcleo de la huella y que se alinee con la orientación de la huella.

Para que dos plantillas basadas en minucias concuerden no es necesario que concuerden todas las minucias que se han extraído de las huellas. De por sí se pueden obtener resultados muy precisos con que tan solo concuerde un tercio del total de minucias.

La extracción de características es la etapa primordial en el reconocimiento de huellas dactilares, por lo tanto, mientras más confiable sea el método utilizado en esta etapa, se obtendrá un mejor rendimiento del sistema. Uno de los principales problemas en la extracción de características de huellas dactilares es la presencia de ruido en la imagen.

Los métodos usados comúnmente toman las impresiones de la huella dactilar aplicando una capa uniforme de tinta sobre el dedo y presionando el dedo sobre un papel. Este procedimiento de captura causa una serie de problemas: áreas entintadas del dedo crean manchas en la imagen; se crean rupturas en las crestas de la imagen de la huella dactilar; y debido a la naturaleza elástica de la piel, las características de la huella dactilar pueden cambiar su posición, dependiendo de la presión aplicada sobre los dedos.

Aunque los métodos basados en tinta usados para la captura están aún disponibles, estos métodos incluso sufren del problema de desplazamiento de posición causado por la elasticidad de la piel. Además, la actitud no cooperativa de un sospechoso o un criminal ocasiona impresiones poco óptimas de la huella dactilar.

El método clásico de extracción de características utiliza la posición, orientación y número de minucias para la fase de comparación (matching). El campo de orientación de la imagen de la huella dactilar en escala de grises juega un rol importante en este método para diseñar los

filtros y la proyección de la imagen en dirección al campo de orientación se utiliza para segmentar la imagen de la huella dactilar [9].

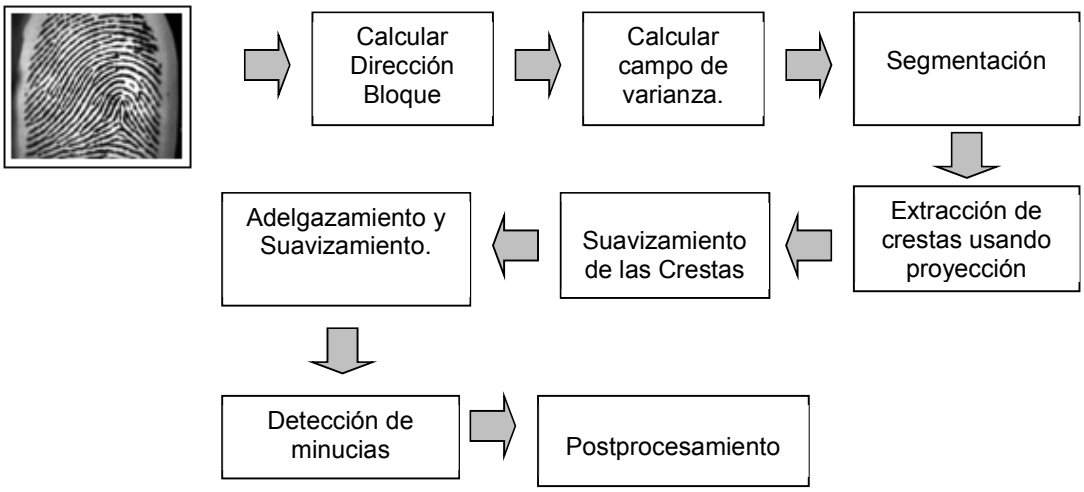


Figura 3.11. Fases del algoritmo clásico de extracción de características

En la figura anterior se muestra los pasos que sigue el algoritmo clásico de extracción de minucias de huellas dactilares [9]: la imagen de la huella dactilar es vista como un patrón de flujo con una textura definida. Se calcula un campo de orientación para el flujo de textura.

Con el objetivo de determinar eficientemente el campo de orientación local, la imagen de entrada es dividida en bloques de igual tamaño (ventanas de 16 x 16 píxeles) y cada bloque es procesado independientemente.

La proyección a nivel de tonos de grises con una línea perpendicular al campo de orientación local provee la máxima varianza. Las crestas son localizadas usando los picos y la varianza de la proyección. Las crestas son adelgazadas y el esqueleto de la imagen resultante es mejorado usando un filtro morfológico. La fase de extracción de características aplica una serie de máscaras a la imagen adelgazada y mejorada y por último la fase de postprocesamiento elimina las minucias falsas generadas.

.

.

4. CASO DE ESTUDIO I.E. GENERAL PRADO - DREC - CALLAO

A continuación se expone a modo de orientación las fases que seguiremos para el desarrollo de nuestro trabajo, para lo cual, contemplaremos los lineamientos del Proceso Unificado a fin de materializar nuestra propuesta de solución al problema del reconocimiento biométrico mediante identificación de huella dactilar aplicado a la Institución Educativa General Prado objeto de estudio de nuestra aplicación.

Asimismo utilizaremos el Lenguaje Unificado de Modelado ("Unified Modeling Language", UML en lo sucesivo) para la construcción y documentación de los distintos entregables que demandará el proceso de desarrollo, así como para la elaboración de distintos diagramas que servirán de mucho en el análisis y diseño del sistema.

La finalidad de este proyecto es dar una solución al problema del control de asistencia, dicha implementación se desarrollará teniendo en cuenta no sólo el desarrollo de un sistema que mediante un dispositivo lector de huellas nos permita identificar a la persona, sino además, gestionar lo relacionado al control de la hora de ingreso y salida del personal docente y administrativo así como también nos servirá para registrar los meritos y deméritos del personal docente así como también llevar el control de la presentación de sesiones de clases por los docentes documento indispensable que garantiza un mejor desempeño de sus funciones.

Para tal objetivo, la propuesta que presentamos será la implementación de un sistema que permita la autenticación los trabajadores del área administrativa y el personal docente que laboran presentando las siguientes características:

- Reconocimiento e Identificación de la huella mediante un lector de huellas.

- Autenticación de la persona mediante la captura de su huella y comparación de la misma en una Base de Datos de Personal.
- Registro de personas que laboran en la institución (docentes y administrativos).
- Registro de la fecha y hora del ingreso y salida del personal.

De esta forma el sistema podrá mostrarnos detalles como:

- Listado de Asistencia del Personal Administrativo y Docente (semanal, mensual, etc.)
- Listado de Personal con tardanzas registradas.
- Listado del Personal con las faltas registradas.
- Día más frecuente para faltas y/o tardanzas.
- Tiempo promedio de tardanza del personal.

4.1. MODELO DEL NEGOCIO.

Es política del Estado mejorar la calidad de los servicios educativos y uno de los procesos involucrados en esta mejora es el control estricto del cumplimiento de las horas efectivas de clase establecidas por el MED; sin embargo existen factores que hacen que no se cumpla a cabalidad. Uno de estos factores es el control de asistencia al personal docente y administrativo de las Instituciones Educativas.

4.1.1. PROCESOS DEL NEGOCIO

Los procesos que se desarrollan para llevar a cabo el control de asistencia en la I.E. materia de Studio son los siguientes:

REGISTRO DE ASISTENCIA.- Tanto el personal docente como el personal administrativo registran su hora de ingreso mediante el marcado de una tarjeta.

Deficiencias que se presentan:

- El caso mas frecuente es las suplantaciones, existen docentes que entran tarde o salen antes de la hora ; sin embargo las horas tanto de entrada como de salida consignadas en sus respectivas tarjetas es la correcta ya que otra persona realiza el marcado por ellos .
- No existe seguridad alguna en el resguardo de la información registrada, la misma que esta expuesta al alcance de cualquier persona por lo que en muchos casos es extraviada.

REALIZAR CONSOLIDADO DE ASISTENCIA.- Este proceso es desarrollado por el Sub Director de formación general quien se encarga de hacer un consolidado cada fin de mes, dicho consolidado contiene las faltas y tardanzas del personal tanto docente como administrativo, el consolidado es remitido a la Dirección Regional de Educación del Callao , específicamente al área de pagos y planillas que es el órgano responsable de ordenar el pago con los respectivos descuentos ya sea por tardanzas o faltas cometidas por los docentes o el personal administrativo . La principal deficiencia de este proceso es que al momento de hacer el consolidado cada fin de mes prima en muchos casos el aspecto personal, en muchos casos no se realizan los descuentos debidos por faltas y/o tardanzas.

ENVIAR CONSOLIDADO DE ASISTENCIA.-Lo realiza la Sub Dirección de la I.E., el consolidado es enviado en archivos impresos, sin tener en cuenta los riesgos de alteración de la información a que puede ser sometido a favor de algún personal.

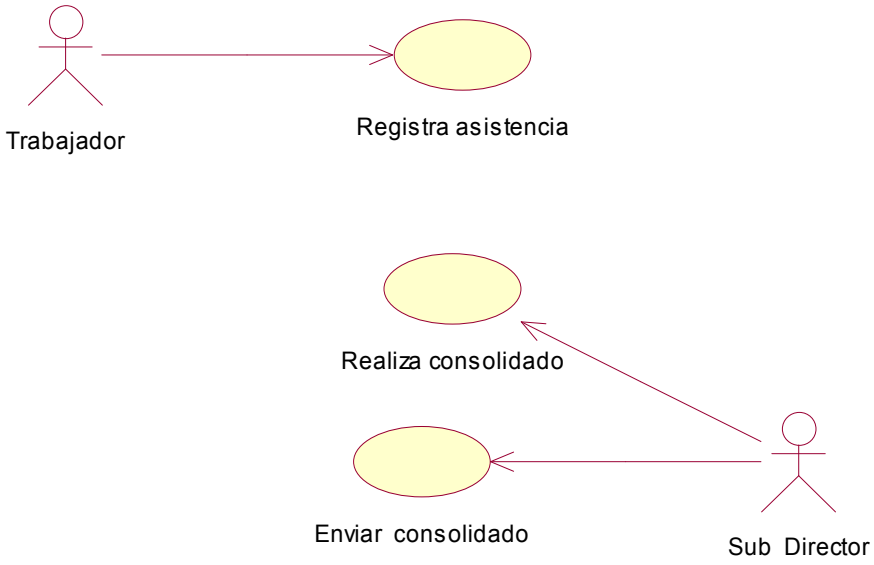
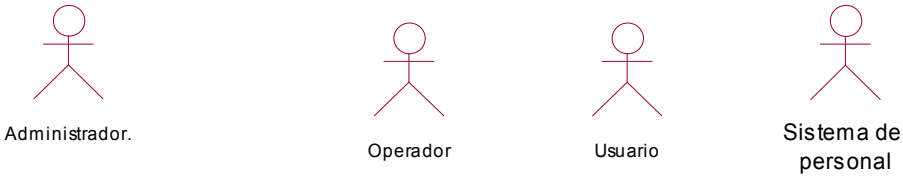


Diagrama Nº 4.1.- Casos de uso del negocio

4.1.2.- ACTORES DEL SISTEMA.

El sistema de Control de Personal cuenta con 4 actores:



ACTOR ADMINISTRADOR:

Representa al encargado del mantenimiento de la base de datos. Su trabajo consiste en dar altas, bajas y modificaciones del personal. Todo su trabajo podrá ser realizado a través de la aplicación, previa autenticación biométrica.

ACTOR OPERADOR:

Representa la persona que se encargará de iniciar la Sesión y el de verificar que las personas antes de ingresar deban poner su huella sobre el lector para que el sistema proceda con la autenticación. Se encargará de realizar las operaciones de consultas resumidas o consolidadas referente a la información que se registra en la base de datos.

ACTOR USUARIO:

Representa la persona que va a ingresar y debe de poner su huella sobre el lector para que el sistema proceda con la autenticación, están involucrados entre ellos el personal docente y administrativo.

ACTOR SISTEMA DE PERSONAL:

Representa la Base de Datos que contiene información del personal que labora en la I.E.

4.1.3. ESTUDIO DE LOS CASOS DE USO

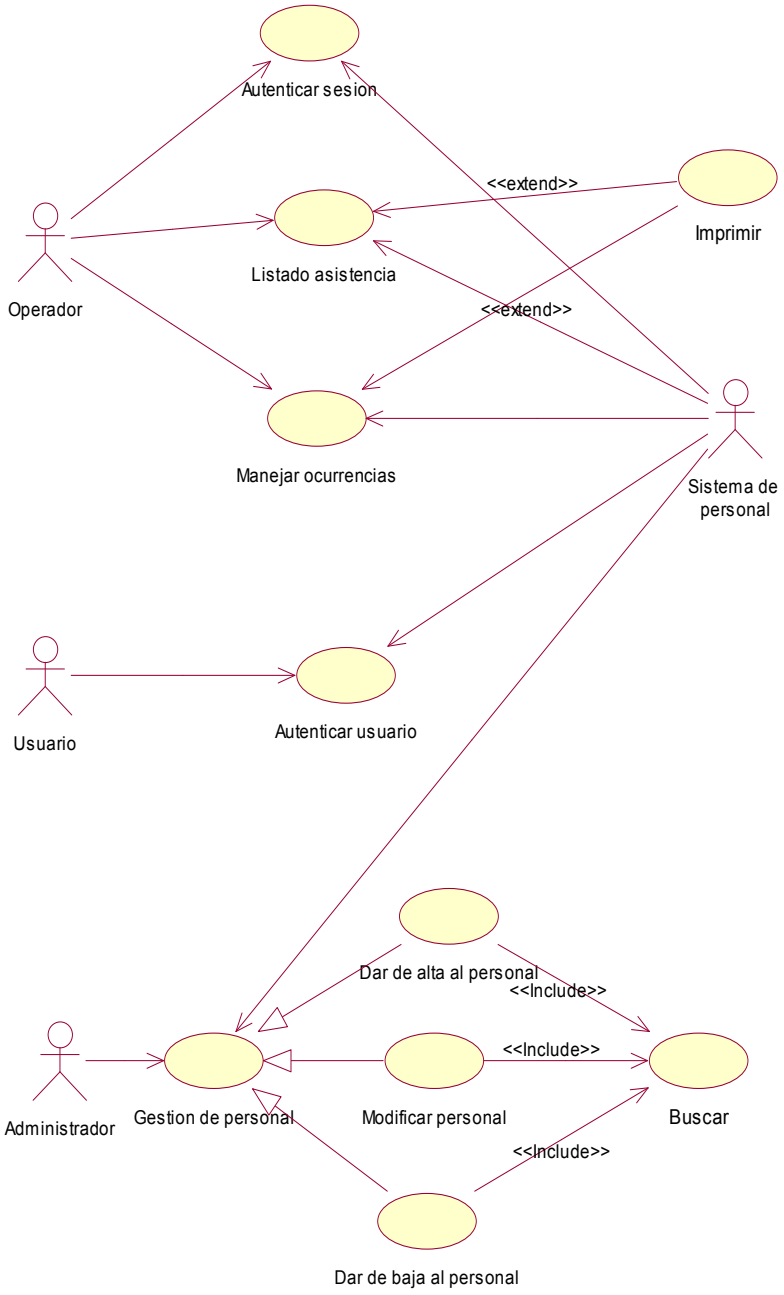


Diagrama Nº 4.2.- Casos de uso

ESPECIFICACIÓN DE CASO DE USO: AUTENTICAR SESIÓN

Caso de Uso	Autenticar Sesión
Objetivo	Iniciar el funcionamiento del sistema de personal.
Actores	Operador del Sistema, Sistema de personal
Precondiciones	El operador tiene que tener su huella dactilar en buen estado para su entrada en el sistema.
Pasos	1. El operador inicia la ventana de la aplicación, apertura una ventana que le solicitará ingreso de su huella y clave personal 2. El operador ingresa los datos para iniciar la sesión. 3. El operador envía los datos para que el sistema lo valide. 4. El sistema procesa la información, realizando una búsqueda de operadores autorizados. 5. El sistema muestra un mensaje con la pantalla de la sesión de trabajo (pantalla principal).
Variaciones	Paso 2: El operador puede elegir salir del sistema, debido a problemas con la huella dactilar o el sistema le solicitará un usuario y contraseña válidos. Paso 3: El operador puede decidir no enviar los datos para la validación y salir del sistema. Paso 4: Problemas con la conexión con la Base de datos. Operador no existe. Paso 5: Los datos del operador no son válidos.
Poscondiciones	El sistema dará como resultado un mensaje de éxito, que le solicitará su confirmación para el acceso al sistema.
Extensiones	Este caso de uso no cuenta con extensiones.

Requisitos Especiales	El operador debe al menos tener conocimiento de informática, de entorno de ventanas gráficas

ESPECIFICACIÓN DE CASO DE USO: LISTAR ASISTENCIA.

Caso de Uso	Listar Asistencia.
Objetivo	Tener un listado sobre la asistencia, permisos y licencias del personal docente y administrativo de la I.E. (Hora de entrada, hora de salida).
Actores	Operador del Sistema, Sistema de personal
Precondiciones	El operador debe haberse validado al entrar al sistema con su huella o login y password (medida de contingencia) y además debe estar de alta en el sistema. El operador debe haber seleccionado de su pantalla actual la opción de Listar Asistencia.
Pasos	1. El operador solicita listado de asistencia de personal. 2. El operador, selecciona ciertos parámetros para la solicitud. 3. El operador envía la solicitud. 4. El Sistema atiende la solicitud y realiza una búsqueda en la base de datos de la información solicitada por el operador. 5. Se envía los resultados de la búsqueda al operador en forma de reporte.
Variaciones	Paso 2: El operador envía la solicitud con los parámetros por defecto para su búsqueda en el sistema. Paso 4: El Sistema retorna el mensaje de que no se pudo establecer conexión con la base de datos.

Poscondiciones	El sistema dará como resultado una pantalla de informe con opción de imprimir el reporte.
Extensiones	Este caso de uso cuenta con el caso de uso “imprimir”, el cual da la opción de enviar la información para imprimir.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASO DE USO: MANEJAR OCURRENCIAS

Caso de Uso	Manejar ocurrencias.
Objetivo	Controlar permisos, licencias y días con suspensión de labores en forma imprevista durante el año lectivo.
Actores	Operador del Sistema, Sistema de personal
Precondiciones	El operador debe haberse validado al entrar al sistema con su huella o login y password (medida de contingencia) y además debe estar de alta en el sistema. El operador deberá contar con un documento que acredite esta acción. (Fichas de desplazamiento, boletas de permiso, resoluciones de licencias, días no laborables). El operador debe haber seleccionado de su pantalla actual la opción de Manejar ocurrencias.
Pasos	1. El operador ingresa las fechas y horas con permiso, licencia o días no laborables a favor del personal. 2. El operador , selecciona ciertos Parámetros para el ingreso de información.

	3. El operador envía la información. 4. El sistema actualiza los datos.
Variaciones	Línea 2.: El operador envía la solicitud con los parámetros por defecto para su búsqueda en el sistema.
Poscondiciones	El sistema dará como resultado un reporte de aceptación de la información ingresada.
Extensiones	Este caso de uso cuenta con el caso de uso "imprimir", el cual da la opción de enviar la información para imprimir.
Requisitos Especiales	El operador debe al menos tener conocimiento de informática, de entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASO DE USO: AUTENTICAR USUARIO.

Caso de Uso	Autenticar Usuario.
Objetivo	Validar al usuario.
Actores	Usuario (Personal docente o Administrativo); Sistema de personal.
Precondiciones	Para realizar este caso de uso, el operador del sistema debe haber iniciado con éxito la sesión de control de personal. El usuario (personal docente o Administrativo) tiene que estar dado de alta en el Sistema.
Pasos	1. El Sistema esta a la espera de una huella de un usuario. 2. Un usuario pone su huella en el lector de huellas. 3. El Sistema captura esa huella la procesa y la envía para la comparación con otras huellas de la base de datos.

	4. La huella buscada es válida, entonces comunicará que el usuario es válido.
Variaciones	Paso 2: El usuario puede tener la huella en mal estado (cortes, heridas, etc.) Paso 3: El sistema no establece conexión con la base de datos, por errores del sistema. Paso 4: La huella no fue encontrada en la base de datos, entonces se retorna el mensaje de que el usuario no es válido.
Poscondiciones	El sistema dará como resultado los datos del usuario (fotografía y otros datos personales).
Extensiones	Este caso de uso no cuenta con casos de uso extendidos, por tanto no tiene puntos de extensión.
Requisitos Especiales	. El operador debe al menos tener conocimiento de informática, de entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASO DE USO: IMPRIMIR.

Caso de Uso	Imprimir
Objetivo	Impresión de reportes.
Actores	Operador del Sistema; Sistema de personal
Precondiciones	El operador debe haberse validado al entrar al sistema con su huella o login y password (medida de contingencia) y además debe estar de alta en el sistema. El operador debe haber seleccionado de su menú principal cualquier opción de consulta de información (resumen de asistencia de personal, resumen de avance académico, etc.) para visualizar esta información.

Pasos	1. El operador solicita la impresión del reporte. 2. El Sistema atiende la solicitud y envía la solicitud a la impresora. 3. El sistema comunica que la impresión terminó con éxito.
Variaciones	Paso 2: El sistema comunica al operador que la impresora está desconectada o le falta papel. Paso 3: El Sistema retorna el mensaje de que no se pudo establecer conexión con la impresora o hubo problemas.
Poscondiciones	El sistema dará como resultado una pantalla que le informará que se imprimió con éxito el reporte.
Extensiones	Este caso de uso no cuenta con casos de uso extendidos, por tanto no tiene puntos de extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASO DE USO: GESTIÓN DE PERSONAL.

Caso de Uso	Gestión de Personal.
Objetivo	Gestionar la información referente al personal que forma parte del Sistema (nuevos ingresos de personal, modificación, dar de baja, dar de alta, etc.).
Actores	Administrador del Sistema
Precondiciones	El Administrador debe haberse validado con su huella dactilar y su Contraseña. El administrador debe haber seleccionado la opción de gestión de personal.
Pasos	1. El administrador solicita la opción de gestión de Personal.

	2. El Sistema muestra la pantalla de gestión de Personal con una serie de opciones referente al manejo del personal.
Variaciones	Paso 2: El sistema puede mostrar el mensaje de que el administrador no tiene acceso a estas opciones.
Poscondiciones	El sistema dará como resultado una pantalla con las opciones de dar de Alta Personal, Dar Baja de Personal, Modificar datos de Personal, etc.
Extensiones	No presenta ningún punto de Extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASOS DE USO: DAR DE ALTA PERSONAL.

Caso de Uso	Dar de Alta Personal.
Objetivo	Autorizar el acceso del usuario al sistema.,
Actores	Administrador del Sistema
Precondiciones	El Administrador debe haberse validado con su huella dactilar y contraseña. El administrador debe haber seleccionado la opción de gestión de personal. El Administrador debe haber seleccionado la opción de dar de alta personal. El Administrador solicita buscar datos del Personal en el sistema para poder darlo de alta.
Pasos	1. El Administrador solicita la opción de dar de Alta o Autorizar al Personal. 2. El Sistema le muestra una pantalla que le solicita los datos del personal a ingresar. 3. El Administrador digita los datos del Personal y acepta. UC: Buscar

	4. El Sistema muestra la información de Personal seleccionado. 5. El Administrador procede a modificar el estado del Personal a Dar de Alta y Confirma los cambios.
Variaciones	Paso 3: El Administrador busca al personal y se da cuenta que no lo tiene registrado. Paso 5: El Administrador decide cancelar la opción de Dar de Alta y sale de esta opción. Paso 6: El Sistema muestra un aviso al administrador donde le comunica que hubo problemas con el registro de dar Alta al Personal.
Poscondiciones	En el sistema se generará una orden de alta de Personal, entonces se dará de alta al personal, con disponibilidad de acceso al Sistema.
Extensiones	No existen puntos de extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

ESPECIFICACIÓN DEL CASO DE USO: MODIFICAR PERSONAL.

Caso de Uso	Modificar Personal.
Objetivo	Modificar datos del personal docente y administrativo de la I.E.
Actores	Administrador del Sistema
Precondiciones	El Administrador debe haberse validado con su huella y contraseña. El administrador debe haber seleccionado la opción de gestión de personal. El Administrador debe haber seleccionado la opción de modificar datos del personal.

	El Administrador solicita buscar datos al Personal en el sistema para poder modificar sus datos.
Pasos	1. El administrador solicita la opción de Modificar. 2. El Sistema le muestra una pantalla que le solicita los datos del personal a modificar. 3. El administrador digita los datos del Personal y acepta. UC: Buscar 4. El Sistema muestra la información de Personal seleccionado. 5. El administrador procede a modificar los datos del personal y confirma los cambios. 6. Muestra una pantalla de éxito en la operación.
Variaciones	Paso 3: El Administrador administrativo busca al personal y se da cuenta que no lo tiene registrado. Paso 5: El Administrador decide cancelar la opción de Modificar datos y sale de esta opción. Paso 6. : El Administrador muestra un aviso que hubo problemas con el registro de la Modificación del Personal.
Poscondiciones	En el sistema se generará una modificación del Personal, un nuevo cambio se guardará en el sistema.
Extensiones	No existen puntos de extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

ESPECIFICACIÓN DE CASO DE USO: DAR DE BAJA PERSONAL.

Caso de Uso	Dar de Baja Personal.
Objetivo	Desautorizar el acceso al Personal
Actores	Administrador del Sistema

Precondiciones	El Administrador debe haberse validado con su huella dactilar y contraseña. El administrador debe haber seleccionado la opción de gestión de personal. El Administrador debe haber seleccionado la opción de dar de baja personal. El Administrador solicita buscar datos del Personal en el sistema para poder darlo de baja. UC: Buscar.
Pasos	1. El administrador solicita la opción de dar de Baja al Personal. 2. El Sistema le muestra una pantalla que le solicita los datos del personal a modificar. 3. El administrador digita los datos del Personal y acepta. 4. El Sistema muestra la información de Personal seleccionado. 5. El administrador procede a modificar el estado del Personal a Dar de Baja y confirma los cambios. 6. Muestra una pantalla de éxito en la operación.
Variaciones	Paso 3: El administrador busca al personal y se da cuenta que no lo tiene registrado. Paso 5: El administrador decide cancelar la opción de Dar de Baja y sale de esta opción.
Poscondiciones	En el sistema se generará una orden de baja de Personal, entonces se dará de baja al personal, sin disponibilidad de acceso al Sistema
Extensiones	No existen puntos de extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

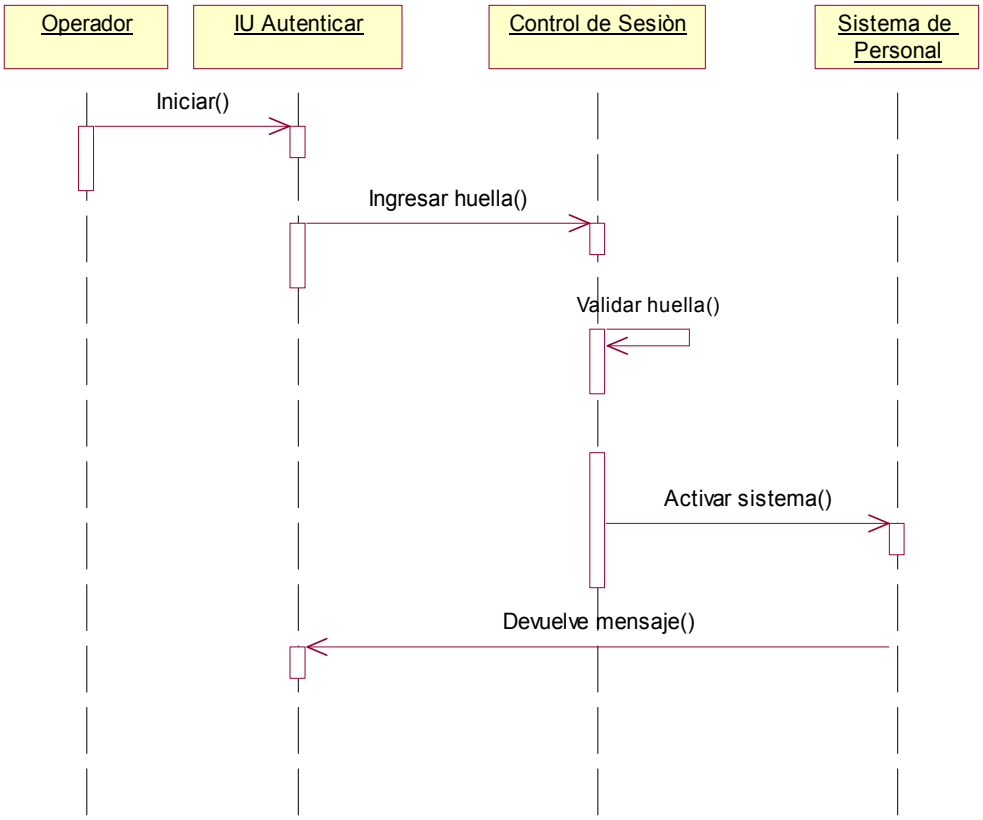
ESPECIFICACIÓN DE CASO DE USO: BUSCAR.

Caso de Uso	Buscar
Objetivo	Buscar al personal en la Base de Datos del sistema.
Actores	Administrador del Sistema
Precondiciones	El Administrador debe haberse validado con su huella dactilar y contraseña. El administrador debe haber seleccionado la opción de gestión de personal. El Administrador debe haber seleccionado la opción buscar.
Pasos	1. El administrador solicita la opción Buscar al Personal. 2. El Sistema le muestra una pantalla que le solicita los datos del personal a Buscar. 3. El administrador digita los datos del Personal y acepta. 4. El Sistema muestra la información de Personal seleccionado. 5. El administrador procede a manipular información del Personal y confirma los cambios. 6. Muestra una pantalla de éxito en la operación.
Variaciones	Paso 3: El administrador busca al personal y se da cuenta que no lo tiene registrado. Paso 5: El administrador decide cancelar la opción Buscar y sale de esta opción.
Poscondiciones	El sistema visualizara en pantalla los datos del personal seleccionado.
Extensiones	No existen puntos de extensión.
Requisitos Especiales	El usuario debe al menos tener conocimiento de informática (Windows), entorno de ventanas gráficas.

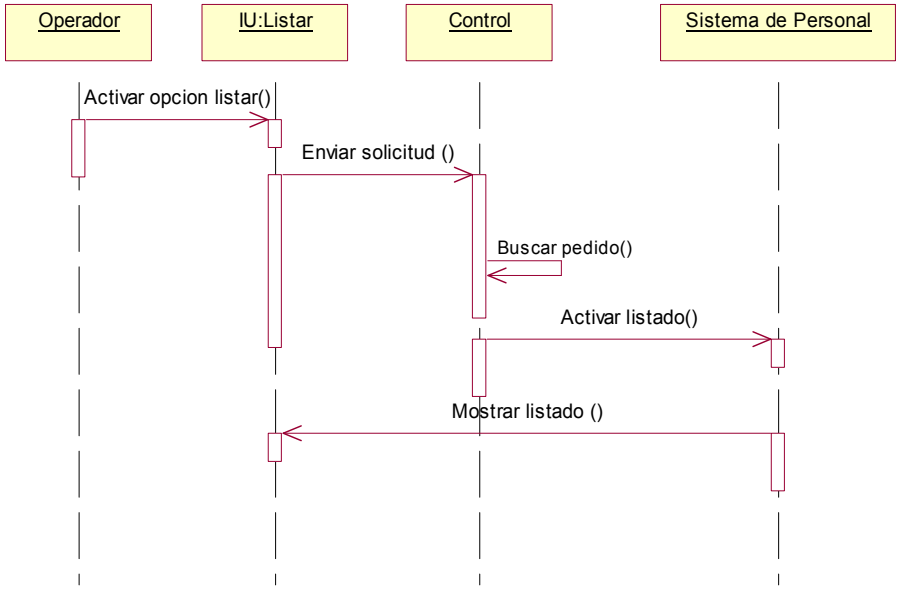
4.1.4. DIAGRAMAS DE SECUENCIA.

Diagrama Nº 4.3.- Diagramas de secuencias.

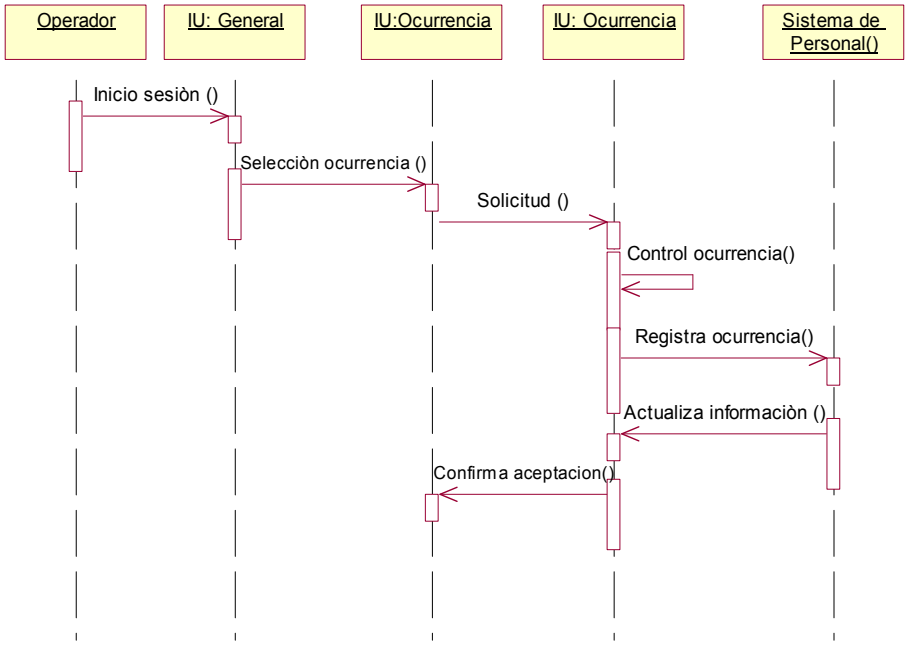
AUTENTICAR SESIÒN:



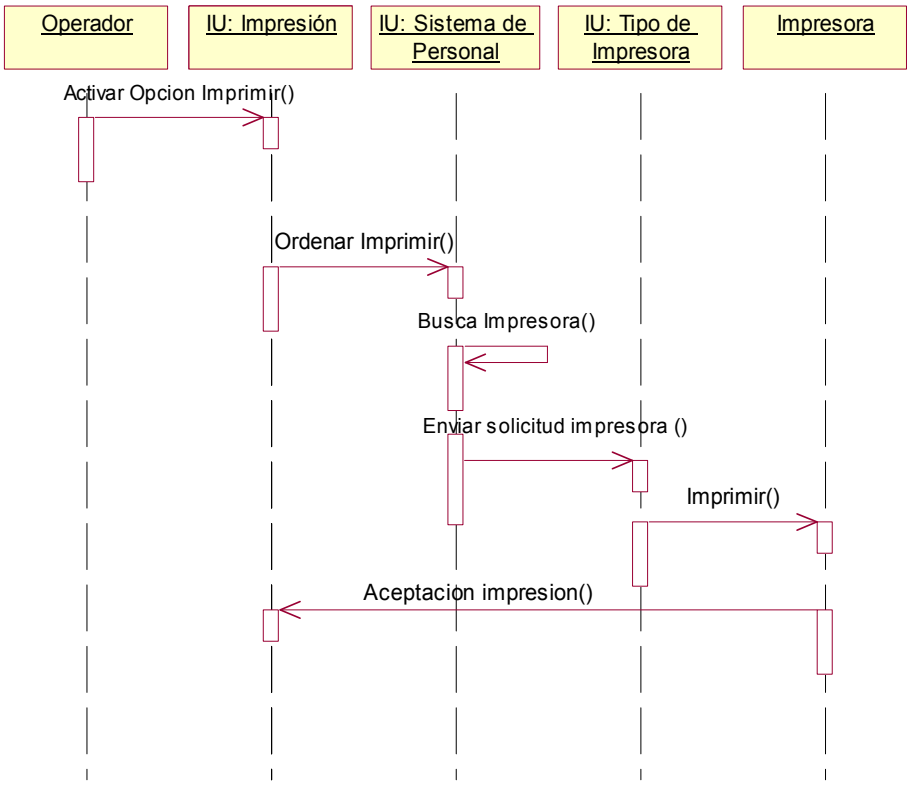
LISTADO DE ASISTENCIA:



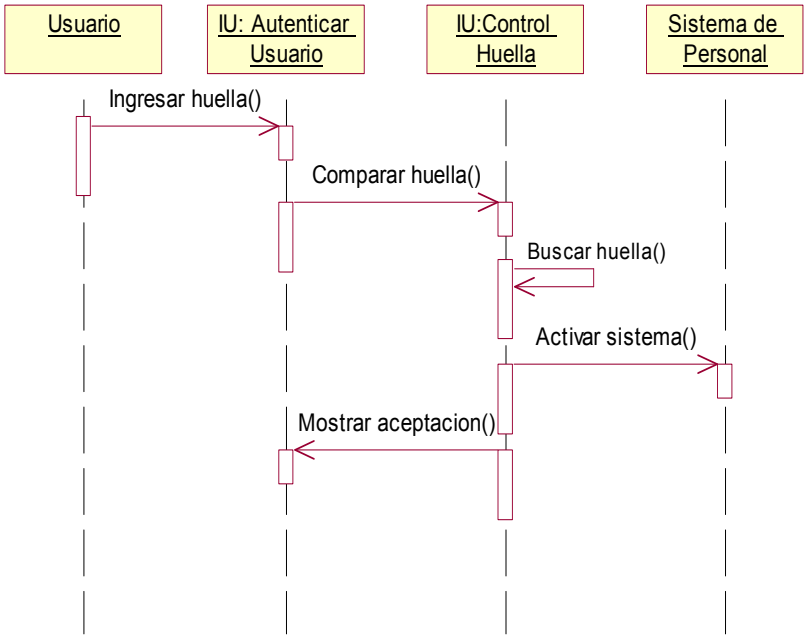
MANEJAR OCURRENCIAS:



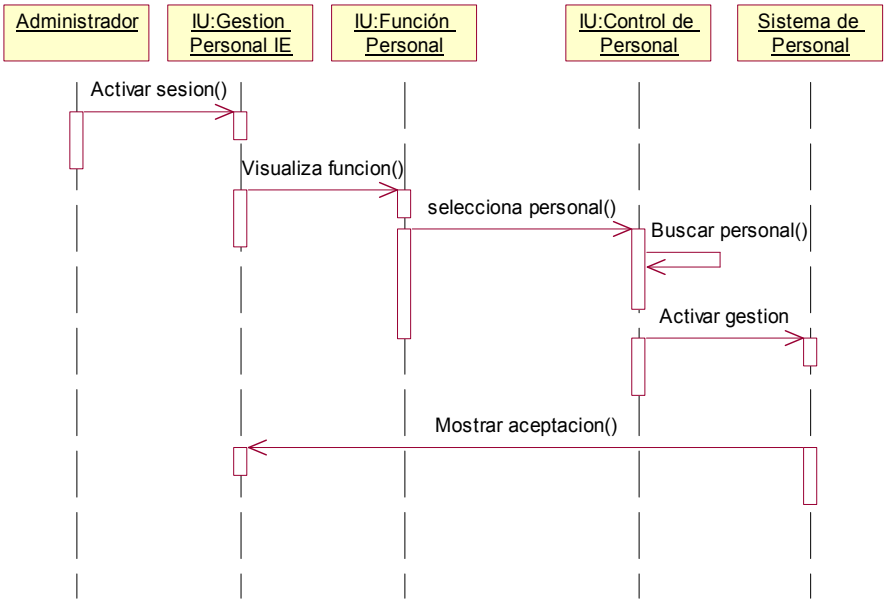
IMPRIMIR :


Operador
IU: Impresión
IU: Sistema de Personal
IU: Tipo de Impresora
Impresora
Activar Opcion Imprimir()
Ordenar Imprimir()
Busca Impresora()
Enviar solicitud impresora ()
Imprimir()
Aceptacion impresion()

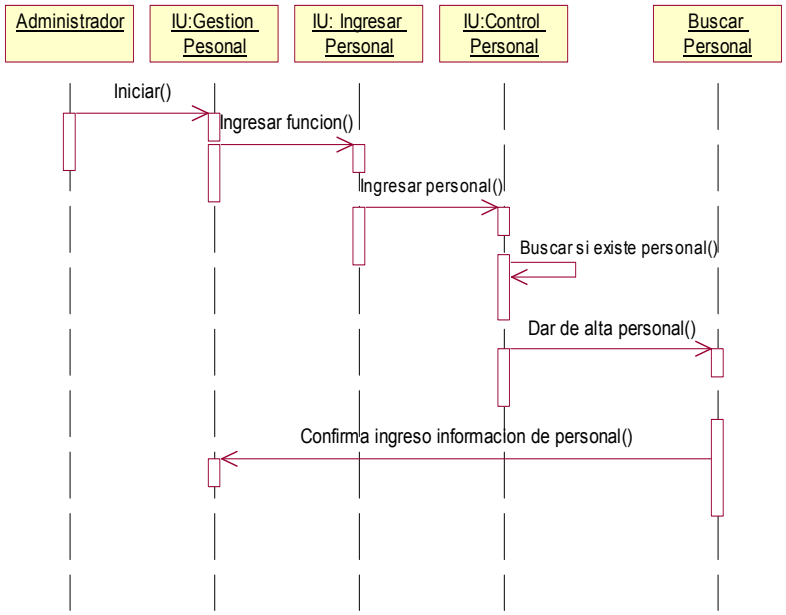
AUTENTICAR USUARIO:



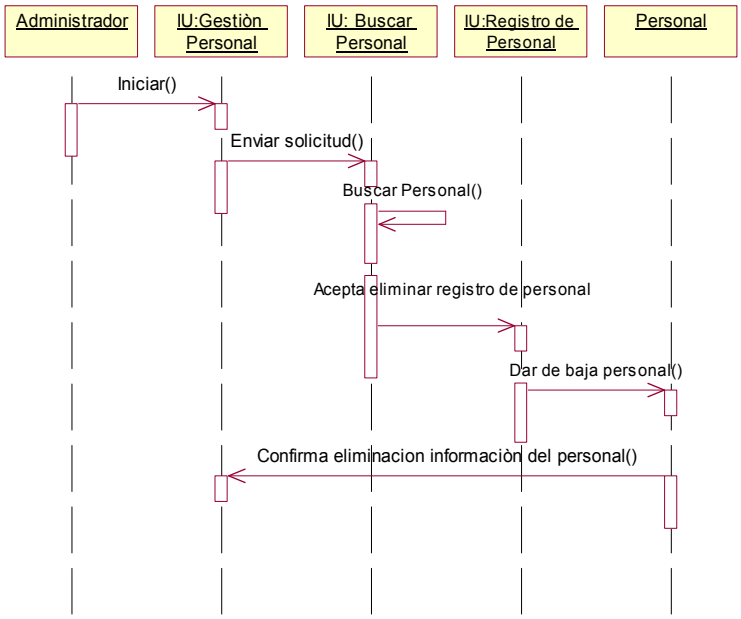
GESTIÒN DE PERSONAL:



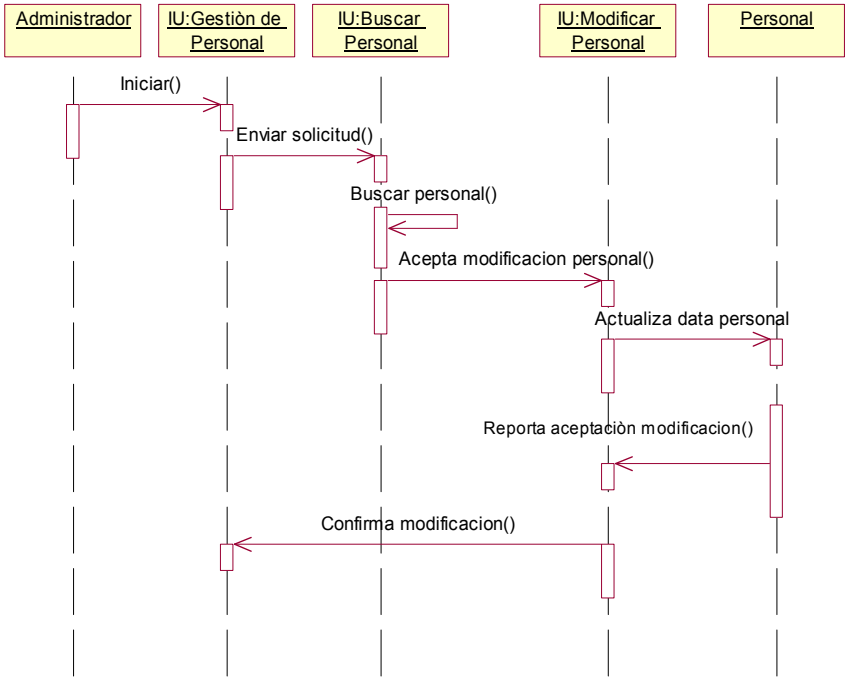
DAR DE ALTA AL PERSONAL:



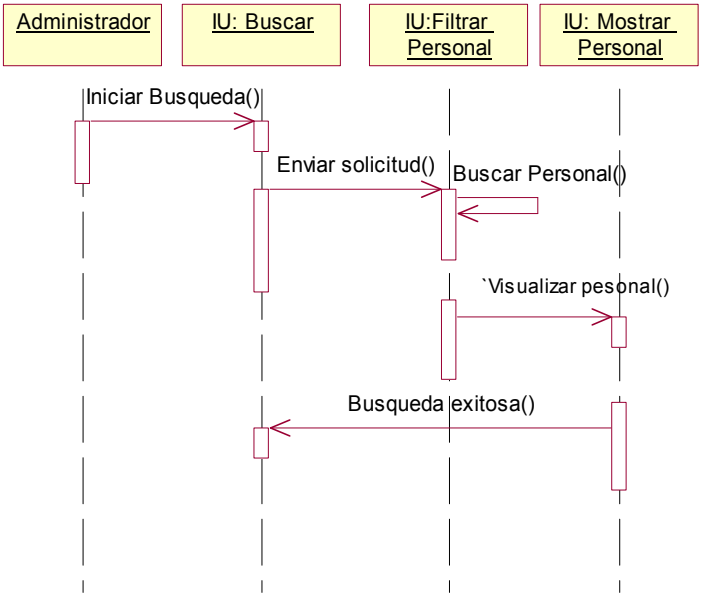
DAR DE BAJA AL PERSONAL:



MODIFICAR PERSONAL:



BUSCAR:



4.1.5.-DIAGRAMA DE CLASES

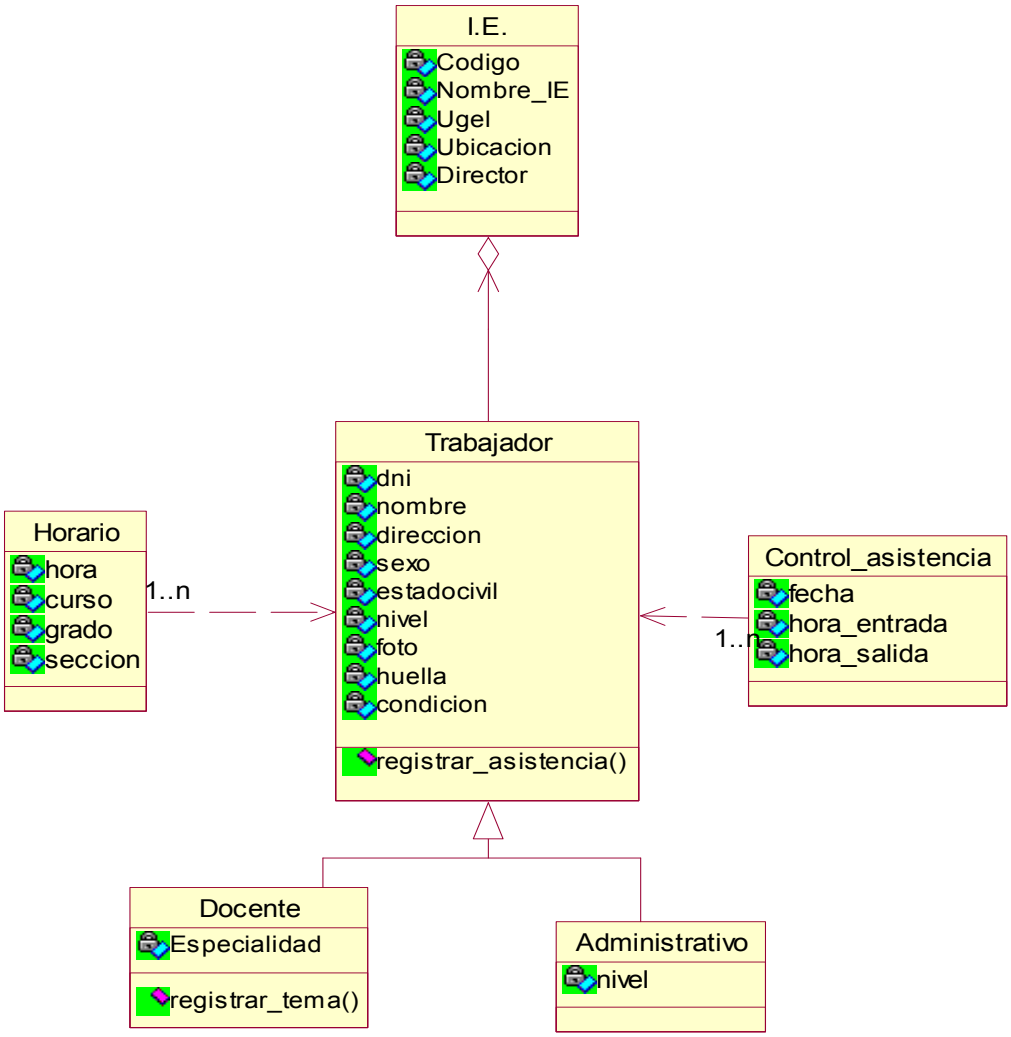


Diagrama Nº 4.4.- Diagrama de clases

4.2. ESTUDIO Y DESARROLLO DE LA BASE DE DATOS.

La base de datos de nuestro sistema será implementada en MySQL que es un sistema de gestión de base de datos open source, relacional multiusuario. La base de datos que implementaremos nos permitirá:

1. El registro de los datos de los trabajadores docentes y administrativos tales como DNI, apellidos y nombres entre otros.
2. Registrar los datos de la I.E. tales como el código modular, descripción y la dirección.
3. Guardar el turno del trabajador.
4. Registrar datos como el periodo lectivo, la hora de ingreso y salida del docente de acuerdo a su horario asignado por la Dirección de la I.E.
5. Registrar los días feriados y no laborables que pueden ocurrir durante el año lectivo.
6. Se podrá registrar el nivel en la que trabaja el docente o administrativo.
7. Permite registrar la hora de entrada y de salida del docente o trabajador.
8. Guarda los permisos y licencias que puede tener el personal.
9. Registrará la hora de ingreso y salida del docente que es la misma que figura en su horario, la hora real de entrada y salida del docente que viene a ser la hora en la que el docente se registra en el sistema ya sea a su entrada o salida mediante el biométrico, las tardanzas y la fecha. Estos datos nos permitirán obtener reportes de las inasistencias, tardanzas, permisos o licencias de los trabajadores.

4.2.1. MODELO LÒGICO.

.

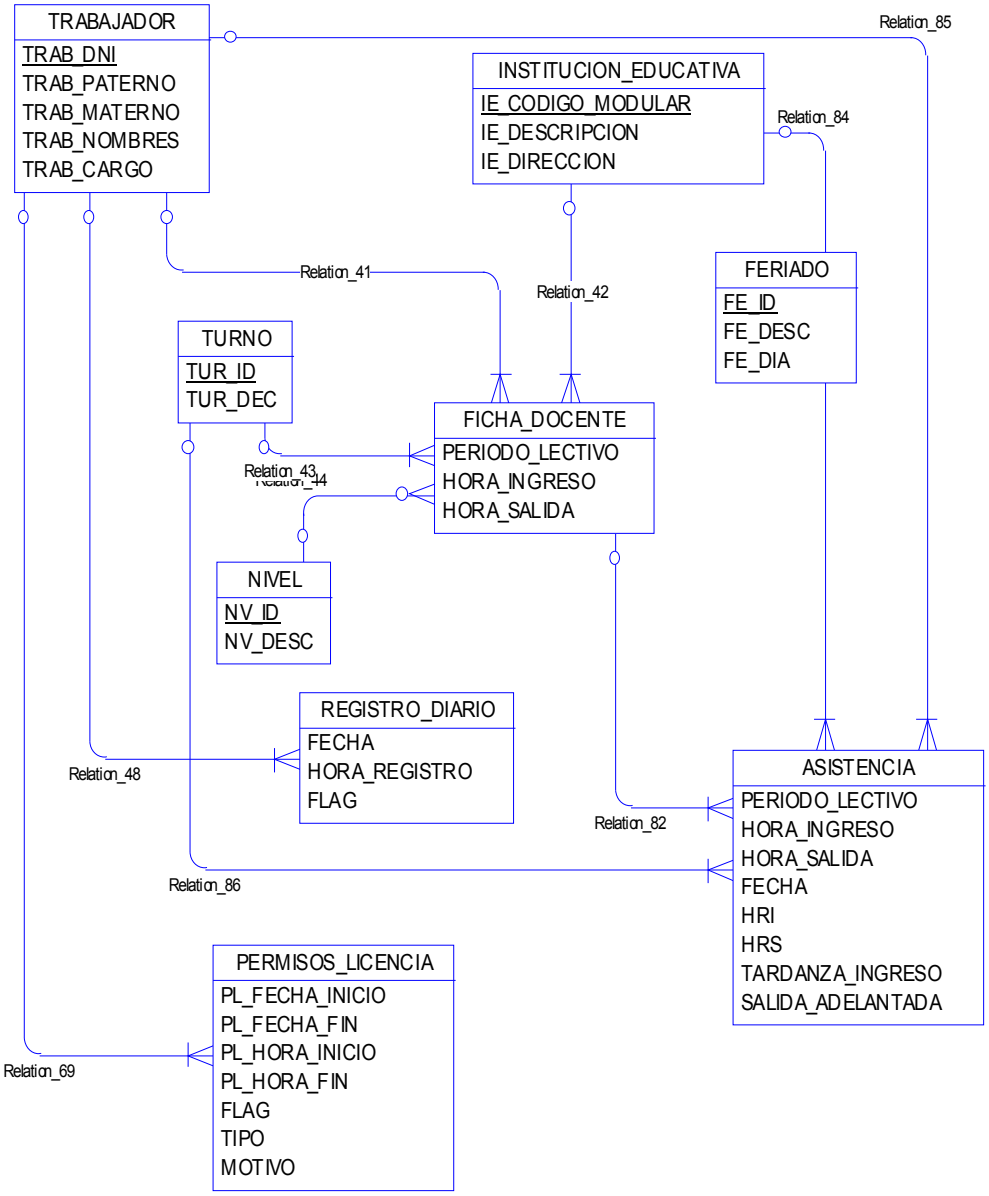

TRABAJADOR
TRAB_DNI
TRAB_PATERNO
TRAB_MATERNO
TRAB_NOMBRES
TRAB_CARGO
INSTITUCION_EDUCATIVA
IE_CODIGO_MODULAR
IE_DESCRIPCION
IE_DIRECCION
FERIADO
FE_ID
FE_DESC
FE_DIA
TURNO
TUR_ID
TUR_DEC
FICHA_DOCENTE
PERIODO_LECTIVO
HORA_INGRESO
HORA_SALIDA
NIVEL
NV_ID
NV_DESC
REGISTRO_DIARIO
FECHA
HORA_REGISTRO
FLAG
ASISTENCIA
PERIODO_LECTIVO
HORA_INGRESO
HORA_SALIDA
FECHA
HRI
HRS
TARDANZA_INGRESO
SALIDA_ADELANTADA
PERMISOS_LICENCIA
PL_FECHA_INICIO
PL_FECHA_FIN
PL_HORA_INICIO
PL_HORA_FIN
FLAG
TIPO
MOTIVO
Relation_85
Relation_84
Relation_41
Relation_42
Relation_43
Relation_48
Relation_82
Relation_86
Relation_69

Diagrama Nº 4.5 Modelo lógico de la base de dato

4.2.2.-MODELO FÌSICO.

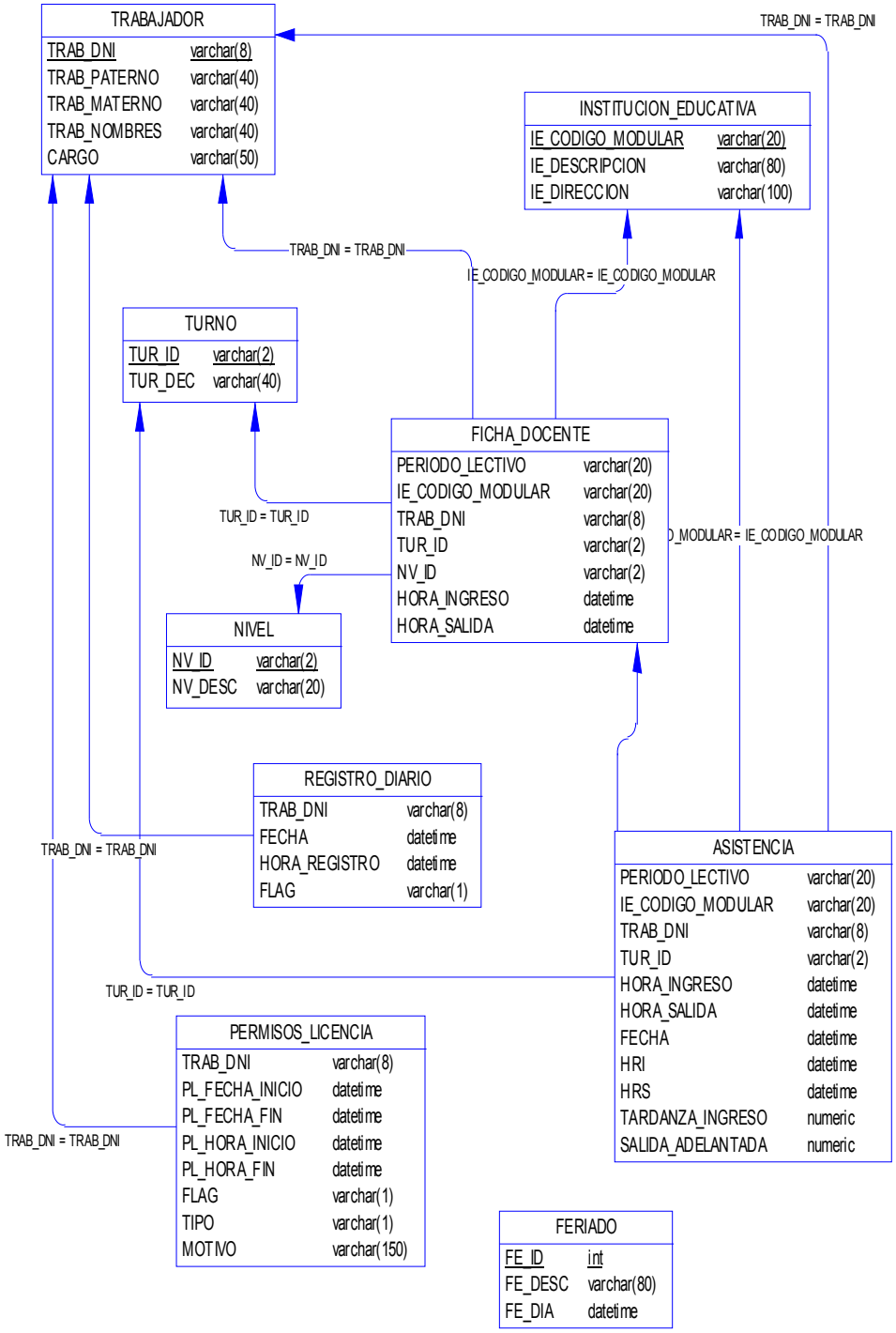


Diagrama Nº4.6 Modelo físico de la base de datos

4.3. DIAGRAMA DE COMPONENTES DEL SISTEMA.

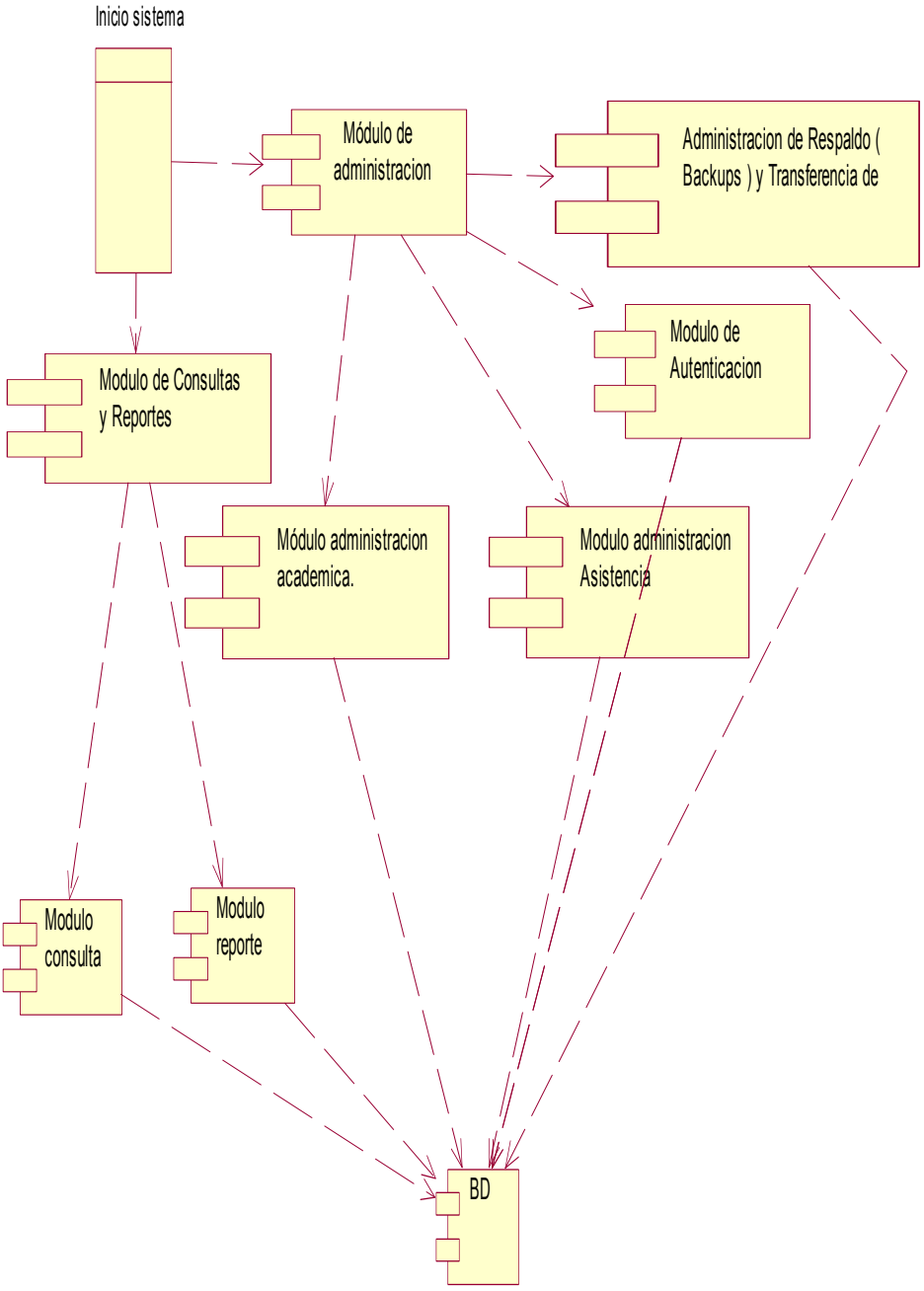


Diagrama Nº4.7-Componentes del sistema.

MÓDULO DE ADMINISTRACIÓN.-ESTE COMPONENTE PERMITE ACCEDER A LOS SIGUIENTES COMPONENTES:

- Módulo administración académica.-Permite administrar datos referentes a la I.E., datos del trabajador (Dar altas, modificar, dar bajas, etc.), manejo de nivel, turnos, etc.
- Modulo administración Asistencia.-Permite administrar datos de feriados, licencias, permisos, datos de la ficha del docente tales como horario que deberá cumplir.
- Administración de Respaldo (Backups) y Transferencia de Datos.- Permitirá administrar el respaldo, si éste se realizará por internet o por Cd (mensual), también permitirá verificar si la asistencia de cada día fue enviada a la DRE correctamente vía Internet.
- Modulo de Autenticación.-Este módulo permitirá decidir que usuarios serán administradores, operadores, se podrá registrar sus datos y asignarles un password para que puedan usar el sistema
- Modulo de Consultas y Reportes: Este módulo presenta los submodulos de consulta y reporte:
- Submodulo de Consulta.-Permitirá ver la asistencia de los trabajadores en un rango de fechas.
- Submodulo de Reporte.- Contendrá una ventana de Reporte Diario en el cual se imprime un listado que muestra la asistencia registrada por los trabajadores de un día especifico, en un rango de fechas , reporte mensual de los trabajadores con tardanzas ,etc.

.4.4. DIAGRAMA DE DESPLIEGUE.

El siguiente diagrama muestra los diferentes tipos de hardware, sobre los cuales operara nuestro sistema, se observa en primer lugar un capturador de huella digital que viene a ser el biométrico quien es el encargado de identificar y validar al usuario, seguidamente existe una PC que cumple el papel de servidor /cliente, en esta PC existe una aplicación que interactúa con la base de datos permitiendo registrar su asistencia de dicho usuario. También se observa una PC que será manejada por el Administrador, por medio de una IU y vía Web se podrá hacer la gestión

del sistema que incluye tareas como emisión de reportes diarios de asistencia, dar de alta a un usuario, dar de baja o modificar algunos datos de los usuarios entre otras tareas. Finalmente la PC que hace el papel de servidor se comunica vía Internet con una PC que se encuentra en la DRE, la finalidad de esta conexión es para enviar diariamente mediante el protocolo SSH la información generada.

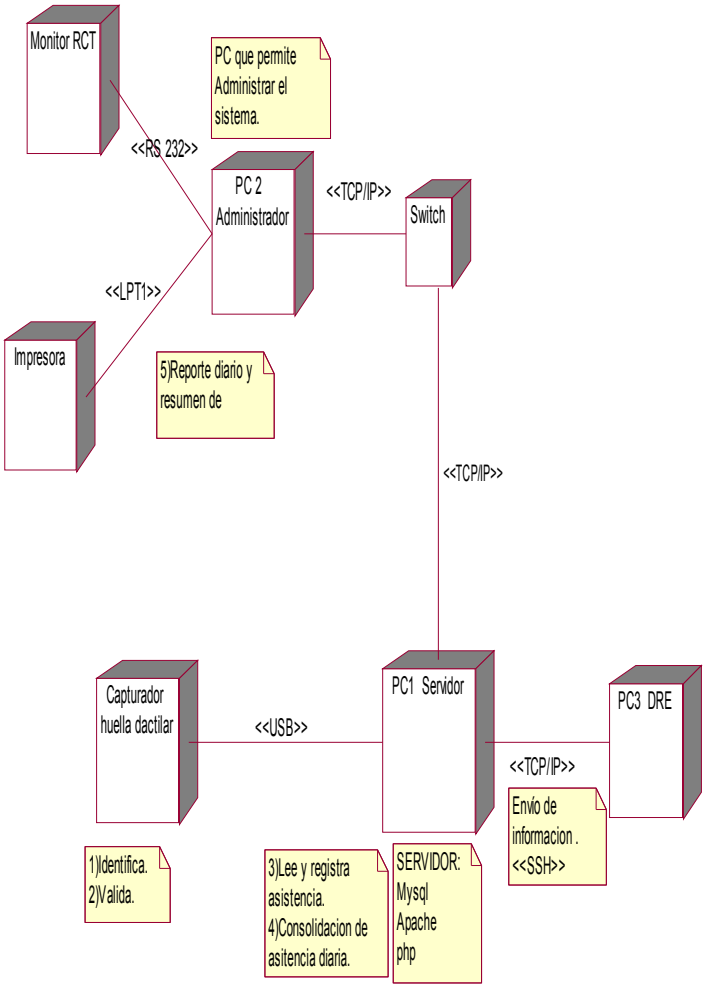


Diagrama Nº4.8 Despliegue del sistema

4.5. REQUERIMIENTO MÍNIMO DE SOFTWARE Y HARDWARE

4.5.1. SOFTWARE

Para el diseño y desarrollo de nuestra aplicación utilizaremos las siguientes herramientas de desarrollo:

- PHP: Acrónimo de Hipertext Preprocesor, lenguaje de programación de gran repercusión en la programación web unido a MySql, trabaja del lado del servidor con independencia de la plataforma. Se caracteriza por su rapidez y por disponer de una amplia gama de librerías de funciones y por ofrecer una extensa documentación.
- MySql: es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.
- Apache: Es un servidor.

4.5.2. HARDWARE

El hardware que utilizaremos para el funcionamiento de nuestra aplicación será:

- 1 PC que hará las veces de Servidor.
- 1 PC que permitirá la administración del sistema.
- 1 Dispositivo lector de huellas dactilares para la oficina donde se realiza el acceso y donde sea necesaria la identificación de la persona a ingresar.
- Un SAI (Sistema de Alimentación Ininterrumpida).

4.5.3. CARACTERÍSTICAS TÉCNICAS

PC SERVIDOR:

- Pentium IV a más.
- Sistema Operativo Linux.

- PHP.
- Mysql
- Apache.
- Memoria de 512 MB a más.
- Disco duro de 80 GB a más.

PC ADMINISTRACIÓN:

- Pentium IV a más.
- Sistema Operativo Microsoft Windows xp con sp 2.
- Monitor de 17 pulgadas a Colores (configuración 800X600).
- Memoria de 256 MB.
- Disco duro de 80 GB a más.

OTROS DISPOSITIVOS:

- Switch.
- Impresoras.

MEDIO DE COMUNICACIÓN:

- Protocolo TCP/IP: TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.
- Protocolo SSH: (o *S*ecure *Sh*ell) es un protocolo para crear conexiones seguras entre dos sistemas. Usando SSH, la máquina

del cliente inicia una conexión con una máquina del servidor. SSH proporciona los siguientes tipos de protección:

- .Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor durante sesiones ulteriores.
- El cliente puede transmitir su información de autenticación al servidor, como el nombre de usuario y la contraseña, en formato cifrado.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación fuerte, lo cual los hacen extremamente difícil de descifrar y leer.

4.6. ANÁLISIS DE FACTIBILIDAD

En este análisis, se toma en cuenta que el beneficiado será el alumnado y el personal de la Institución Educativa. Se hace una comparación entre el Sistema Actual y la implementación del nuevo Sistema usando Tecnología de Huella Dactilar.

PERSONAL	DOCENTE	ADMINISTRATIVO	TOTAL
Nombrados	135	16	151
Contratados	25	4	29
Total	160	20	180

Tabla Nº 2.Cantidad de docentes y administrativos de la I.E. General Prado.

	DOCENTES	ADMINISTRATIVOS
Promedio de tardanzas/ hora	156	16
Costo de descuento por hora en soles.	5,70	3,20

Total de descuentos por tardanzas en soles.	889,20	51,20	940,40

Tabla Nº3 .Descuentos en soles por tardanzas de la I.E. General Prado

Costo del reloj de asistencia	s/. 1620
Tarjetas(180 por mes)	s/. 45
Mantenimiento del reloj/mes	s/. 20
Costo de dispositivo huella dactilar	s/. 1260
Costo del desarrollo del software.	s/. 2200
Mantenimiento del sistema (mes)	s/. 20
Hardware + software	s/. 0

Tabla Nº4 .-Costos unitarios del sistema actual (Reloj tarjetero) y control de asistencia mediante implementación biométrica.

COSTO DE USO DEL TARJETERO (DURANTE 05 MESES)

COSTO	Marzo	Abril	Mayo	Junio	Julio
Descuento a todo el personal	940,4	940,4	940,4	940,4	940,4
Reloj de asistencia	1620				
Tarjetas	45	45	45	45	45
Mantenimiento del reloj	20	20	20	20	20
Total	2625,4	1005,4	1005,4	1005,4	1005,4

COSTO TOTAL: S/. 6647

Tabla Nº5 .Costo total del sistema de control de asistencia actual mediante reloj tarjetero.

COSTO DE LA IMPLEMENTACIÒN DEL SOFTWARE
(DURANTE 05 MESES)

COSTO	Marzo	Abril	Mayo	Junio	Julio
Dispositivo huella dactilar	1260				
Desarrollo software	2200				
Mantenimiento del sistema	20	20	20	20	20
Hardware + software	0	0	0	0	0
Total	3480	20	20	20	20

COSTOS TOTAL: S/. 3 560

Tabla Nº6 .Costo total del sistema de control de asistencia mediante reconocimiento biométrico de huella dactilar.

OBSERVACIONES:

- Si comparamos durante los cinco meses donde se incluye costos de implementación (marzo) concluimos que el desarrollo del nuevo sistema bajo la huella dactilar es rentable su implementación, existiendo un ahorro S/. 3087
- Será más rentable aún si se considera que el personal realizara el esfuerzo de llegar a la hora puntual a la Institución Educativa, como consecuencia los beneficiados será el alumnado al estar más tiempo con sus profesores.
- Además el costo fuerte de implementación será sólo en el primer mes del uso del sistema.
- Los descuentos son insensibles para todo el personal, ello conlleva a que el personal docente y administrativo sea puntual en asistir a la Institución y así evitar ser descontado.
- La Institución cuenta con equipo de cómputo cuyo mantenimiento esta garantizado por la DIGETE –MED. (Ex proyecto Huascarán).
- Si tenemos en cuenta el costo social que representa la pérdida de horas de clase efectivas que se ocasiona al faltar los docentes al no ser descontados económicamente, las faltas son frecuentes.

Teniendo en cuenta ésta observación la inversión estimada es mínima comparando con los beneficios que traerá el sistema.

4.7. INTERFASES DEL SISTEMA.

CONTROL DE ACCESO AL SISTEMA: En este mòdulo para acceder al sistema y realizar su respectivo mantenimiento es importante tener la clave, solamente las personas autorizadas tienen el acceso.

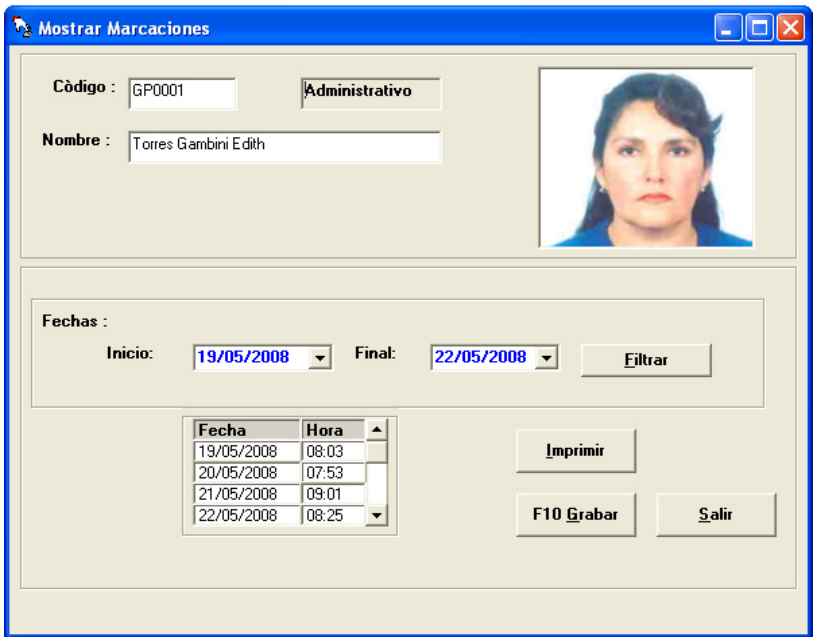
CONSULTAS DE PROGRAMACIÒN Y ASISTENCIA DEL PERSONAL:

La interface, que solo es manipulado por el administrador del sistema, es para realizar un seguimiento del personal ya sea administrativo o docente.

.

EDICIÒN DE ASISTENCIA DEL PERSONAL EN UN INTERVALO DE TIEMPO:

La interface permite listar escogiendo un intervalo de tiempo, la hora de ingreso/ salida de la Institución Educativa del personal docente o administrativo, es importante para realizar un seguimiento del mismo.

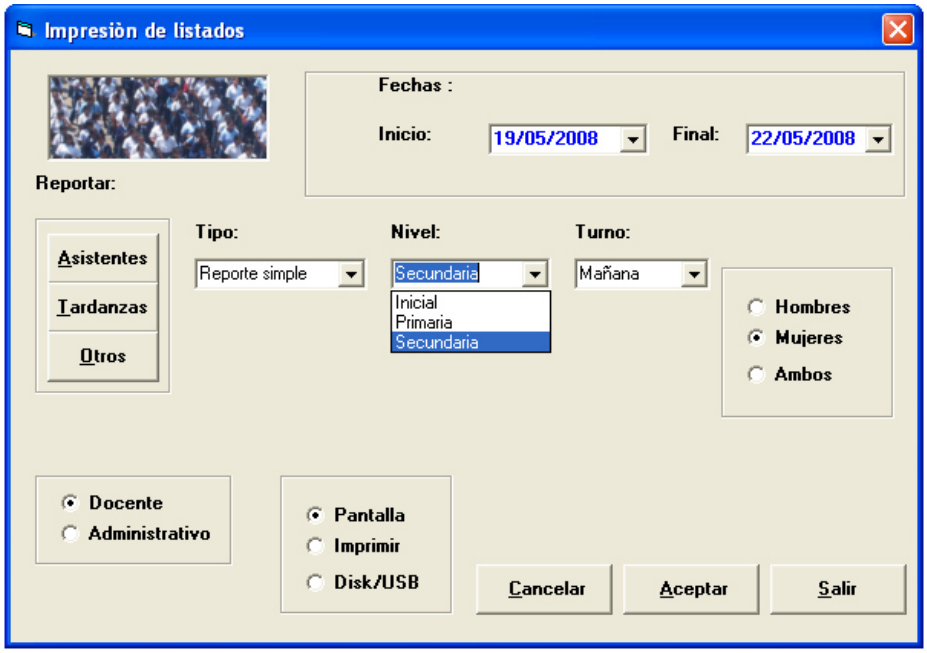


CONTROL DEL USO DE LAS OCURRENCIAS QUE PRESENTA EL PERSONAL:

La interface, permite listar las características de la inasistencia del personal de la Institución Educativa y los casos en que el docente o administrativo tienen opción de faltar, así como las posibilidades que tienen para ausentar del colegio como por ejemplo la licencia interna que por derecho le corresponde a los trabajadores.

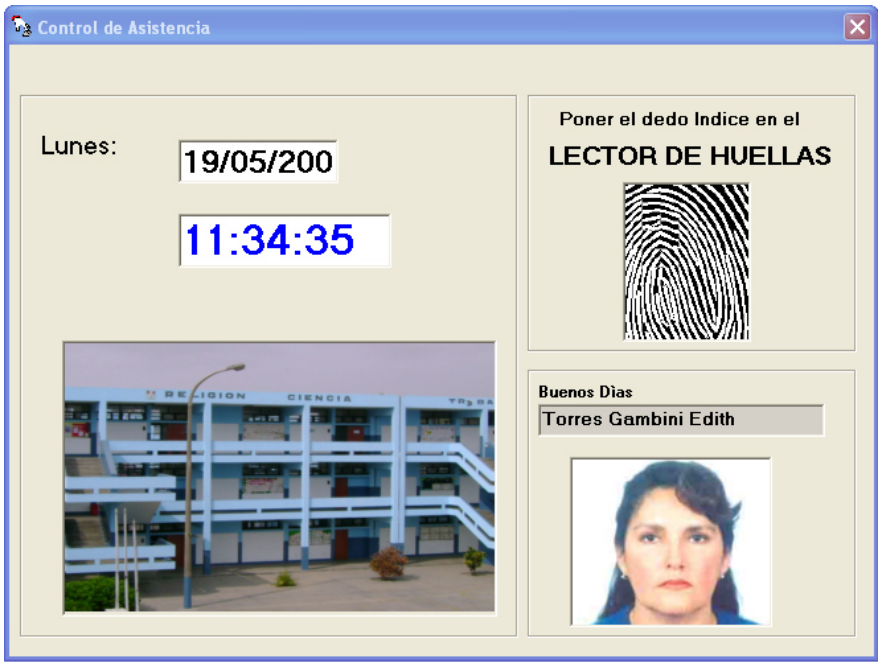
IMPRESIÒN DE LISTADOS DE ASISTENCIA DEL PERSONAL:

La interface permite generar un reporte del personal de la Institución educativa en un intervalo de tiempo, generalmente se utiliza para listar los consolidados de fin de mes.



INTERFACE DEL CONTROL DE ASISTENCIA DEL PERSONAL:

Es la interface en que muestra de manera positiva al personal docente o administrativo el día, su hora de ingreso/salida luego de haber interactuado con el dispositivo que captura la huella digital, mostrándose la foto en señal de haber realizado una operación exitosa



CONCLUSIONES

- El uso de la tecnología biométrica como método de control de asistencia del personal docente y administrativo por las Instituciones Educativas Escolares evita su vulnerabilidad, facilitando la gestión y reduciendo los costos económicos y sociales para el Estado Peruano
- La biometría mediante la identificación de la huella dactilar permite un mayor control de la asistencia del personal docente y administrativo de las Instituciones Educativas.
- La biometría ofrece una nueva forma de autenticarse basándose en lo que es la persona, utilizando algo que forma parte de su cuerpo, brindando seguridad, comodidad y rapidez como rasgos propios de la seguridad biométrica.
- Los sistemas biométricos de identificación dactilar se puede aplicar en distintos ámbitos, entre los que podemos mencionar: control de asistencia, acceso físico a recintos, acceso virtual a sistemas de aplicación, aplicaciones de comercio electrónico, voto electrónico, transacciones bancarias, entre otras.
- La identificación por medio de huellas dactilares constituye una de las formas más representativas y económicas de la utilización de la biometría; sin embargo su mayor desventaja es de no poder autenticar usuarios que hayan sufrido lesiones en los dedos y no pueden ser reconocidos, es por ello que se recomienda el uso adicional de claves.
- Los identificadores biométricos más sobresalientes son la Huella Dactilar y el patrón de Iris, los cuales presentan óptimos niveles de requerimientos como un elevado nivel de distinción, permanencia y rendimiento, garantizando aplicaciones de buena calidad.
- Los sistemas biométricos aplicados a la seguridad presentan una serie de posibilidades sin embargo su adopción es progresiva.
- La elección de un identificador biométrico depende en gran parte del tipo de aplicación que se desee implementar, sin embargo, es

recomendable el uso de identificadores biométricos fisiológicos antes que los de comportamiento, ya que estos últimos pueden ser muy inestables al estar supeditados al cambio de ánimo de la persona.

FUTUROS TRABAJOS

- En el futuro para evitar rechazo frente a la posibilidad de que una organización controle información biométrica de los ciudadanos se recomienda el uso de tarjetas inteligentes que almacenen los patrones biométricos de los usuarios de esta forma las entidades no se quedan con ningún tipo de información biométrica sino que únicamente valida que la persona que desea realizar una operación o acceder a un lugar es quien dice ser . Una de estas tarjetas son las denominadas Match Card.
- También se recomienda como un trabajo futuro la integración del sistema planteado en la presente Tesina con el sistema de recursos humanos que maneja la UGEL de tal manera que la información producida en las Instituciones Educativas sean exportados automáticamente por los sistemas de la UGEL de tal manera que ellos dispongan de la información en tiempo real y tener un mejor control de las Instituciones Educativas.
- Se recomienda implementar el sistema de control usando tecnología biométrica por medio de huella dactilar en las I.E. Públicas del Perú, para evitar la vulnerabilidad y contribuir a la mejora de la calidad educativa en el País.

RECOMENDACIONES

- Mantener como contingencia la manera tradicional en la que se venía realizando el control de asistencia en caso que la persona que se desea autentificar haya sufrido algún problema físico que lo indisponga ante el lector de huella dactilar.

REFERENCIAS BIBLIOGRÁFICAS

[1] Bazen A.M., Otterlo M., S.H. Gerez, M. Poel. "Un agente de refuerzo para el aprendizaje minucias extracción de huellas dactilares". En Krose B., M. de Rijke, G. y M. Schreiber van Someren, editores, Actas de la Bélgica - Países Bajos Artificial Conferencia de Inteligencia, páginas 329 - 336, 2001.

[2] Dorizzi Bernardette, Usages Des Techniques Biométriques Pour La Vérification Et L'identification Eléctronique, Groupe des Ecoles des Télécommunications / Direction scientifique, Francia, 2003

[3] Proceedings of the IEEE, An Identity-Authentication System Using Fingerprints, Vol 85, Nº 9, page 1365, September 1997.

[4] Jiang X., Ser W., Yau W., "Detecting the fingerprint mintiae by adaptive tracing the gray – level ridge". Pattern Recognition, 34(5):999 – 1013, Mayo 2001.

[5] Hong L., Jain A., Wan, "Fingerprint Image Enhancement Algorithms and Performance Evaluation", IEEE Transactions on Pattern Analysis and Machine.

Intelligence, vol. 20, no 8, pp., 777 – 789, 1998.

[6] Hoyos Juan Carlos, León Ramírez Jaime, Madrigal Carlos Andrés, Sistema De Reconocimiento Biométrico Por Medio De La Huella Dactilar, Universidad de Antioquia, Colombia, 2004

[7] Jiménez Sáenz Josu, Sistemas de Reconocimiento Biométrico: La Huella Dactilar, Facultad de Informática de San Sebastián, Seguridad de Informática, 2002

[8] Hong Y., Huang K., Zhang, "Clasificación de Huellas Digitales Sobre la base de Extracción y Análisis de las singularidades y Pseudoridges ", Qinzhi Escuela de Eléctrica y Información Ingeniería de la Universidad de Sidney, Australia, 2002.

[9] Jain K., Chen S., Ratha N., "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, No. 11, pp. 1657-1672, 1995.

[10] Jian A., D. Maio, D. Maltoni, Prabhakar S., "Manual de reconocimiento de huellas dactilares", Junio 2003 - New York Springer.

[11] Orgueira Pérez José Antonio, Sistema De Gestión De Huellas Dactilares En Formato Digital, pag. 12, Universidade Da Coruña Facultade De Informática, Departamento de Tecnoloxías da Información e as Comunicacións, Brasil, 2003. 1ra Edición.

[12] Kuosmamen P., Tico M., “An algorithm for Fingerprint Image PosProcessing.” Accepted to The 34-th Asilomar Conference on Signal, Systems and Computers. Pacific Grove. California. Oct.29- Nov.1, 2000.

[13] Jian A., D. Maio, D. Maltoni, Prabhakar S., "Manual de reconocimiento de huellas dactilares", Junio de 2003 - Nueva York Springer.

[14] Proceedings of the IEEE, An Identity-Authentication System Using Fingerprints, Vol 85, Nº 9, page 136, September 1997.

[15] Miller B., “Vital Signs of identity”. IEEE Spectrum, 31(2): 22-30, Febrero 1994.

[16] Sandström Marie, Liveness Detection in Fingerprint Recognition Systems, LinkÄoping Universitet, pág. 18, Suecia, 2004

[17] Villamizar J., “Procesamiento y Clasificación de Huellas Dactilares”, Pontificia Universidad Javeriana, Bogotá, noviembre 1993.

[18] Zorita Simón D., García Gomar M., Sánchez Asenjo M., Sánchez Bote JL., Ortega García J., pag. 1, Esquema Completo De Identificación Y Verificación De Patrones Biométricos De Huellas Dactilares, Dpto. Ingeniería Audiovisual y Comunicaciones, EUIT- Telecomunicación, Universidad Politécnica de Madrid, 2001

REFERENCIAS ELECTRÓNICAS

[19] Ángela Martín Méndez. La Biometría: el método de identificación más seguro. 25 de octubre de 2006.Obtenida en abril del 2008 de http://www.homini.com/index.htm.

[20] ¿Por qué huella digital ? (n.d). Obtenida en abril del 2008 de http://www.kimaldi.com/

[21] Identificación por huellas dactilares. (n.d). Obtenida en abril del 2008 de http://biometrics-on.com/es/identificacion-por-huellas-dactilares.asp

ANEXOS

CUESTIONARIO APLICADO A LOS ALUMNOS

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

Respetado alumno:

Se está realizando una investigación "RECONOCIMIENTO BIOMÉTRICO MEDIANTE IDENTIFICACIÓN DE HUELLA DACTILAR APLICADO A LAS INSTITUCIONES EDUCATIVAS ESCOLARES" A continuación se presentan preguntas. Trata de responder con absoluta sinceridad y seriedad marcando la alternativa que consideres como respuesta:

1. TUS PROFESORES ASISTEN PUNTUALMENTE AL DICTADO DE CLASES:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

2. LAS CLASES CORRESPONDIENTES A LA PRIMERA HORA, SE INICIAN EXACTAMENTE A LA HORA ESTABLECIDA:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

3. LA SALIDA DEL AULA EN LA ÚLTIMA HORA DE CLASES ES EXACTAMENTE A LA HORA ESTABLECIDA:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

4. LAS HORAS DE CLASE PERDIDAS POR LAS TARDANZAS O INASISTENCIAS DE TUS PROFESORES SON RECUPERADAS:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

5. CONSIDERAS QUE DEBERIA HABER UN MAYOR CONTROL EN LA ASISTENCIA DE LOS PROFESORES A LA INSTITUCIÒN EDUCATIVA:

A) Si B) No

6. LOS PROFESORES FALTAN A LA INSTITUCIÒN EDUCATIVA:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

7. ALGUNOS PROFESORES SE AUSENTAN EN HORAS DE CLASE:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

8. CUANDO ALGUNOS DE TUS PROFESORES NO ASISTEN, LA SUBDIRECCIÒN O EL AUXILIAR INGRESA A TU SALÒN A REEMPLAZAR A TU PROFESOR EN SU HORA CORRESPONDIENTE:

A) Si B) No

9. CONSIDERA UD. QUE EXISTE UN SEGUIMIENTO ADECUADO POR PARTE DE LA DIRECCIÒN O SUB DIRECCIÒN DE LA I.E. SOBRE LA ASISTENCIA DE DOCENTES:

A) Si B) No

10. ESTA UD. DE ACUERDO QUE SE IMPLEMENTE EN TU COLEGIO UN SISTEMA QUE CON LA AYUDA DE UN COMPUTADOR PERMITA UN MAYOR CONTROL DE ASISTENCIA PARA TUS PROFESORES:

    A) Si B) No

CUESTIONARIO APLICADO A LOS DOCENTES

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

Respetado Docente:

Se está realizando una investigación "RECONOCIMIENTO BIOMÉTRICO MEDIANTE IDENTIFICACIÓN DE HUELLA DACTILAR APLICADO A LAS INSTITUCIONES EDUCATIVAS ESCOLARES" A continuación se presentan preguntas. Trata de responder con absoluta sinceridad y seriedad marcando la alternativa que consideres como respuesta.

1. CONSIDERA QUE EL PROCESO DE CONTROL DE PERSONAL DOCENTE Y ADMINISTRATIVO DE LA I.E. ES EL APROPIADO:

A) Si B) No

2. EN EL PROCESO ACTUAL DE CONTROL DE ASISTENCIA QUE MANEJA LA INSTITUCIÒN EDUCATIVA. ¿CUÁLES DE LAS POSIBLES FALTAS SE COMETEN?

   A) No se registra los datos por olvido del personal.
   B) Alteración de la hora de ingreso o salida-
   C) Suplantación.
   D) No se Registra los datos con veracidad.

3. RESPECTO AL CONSOLIDADO DE TARDANZAS O FALTAS QUE SE ENVIA A LA UGEL/DREC CONSIDERA UD. QUE ES JUSTO:

   A) Es justo.
   B) No refleja la realidad.
   C) Existe favoritismo a algunos docentes.

4. ASISTE PUNTUALMENTE AL DICTADO DE SUS CLASE:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

5. LAS HORAS DE CLASE PERDIDAS POR TARDANZA O FALTAS DE UD. LOS RECUPERA:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

6. CUANDO UD. SALE DE LA I.E. EN HORAS DE CLASE , UTILIZA PAPELETA DE DESPLAZAMIENTO:

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

7. SU SALIDA DE LA I.E. ES DE ACUERDO A SU HORARIO ESTABLECIDO

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

8. AL MOMENTO DE HACER USO DEL ACTUAL PROCESO DE CONTROL DE ENTRADA/SALIDA. ¿UD. REGISTRA SU HORA REAL?

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

9. UNA VEZ REGISTRADO SU HORA DE INGRESO O SALIDA ¿UD. ACOSTUMBRA MODIFICARLO HACIENDO UNA CORRECCIÒN MANUALMENTE?

A) Siempre B) Casi Siempre C) Pocas veces D) Nunca

10. DE LOS TRES DIAS DE PERMISO POR MOTIVOS PERSONALES ¿DE CUÀNTOS DIAS HIZO USO?

A) Ninguno B) Uno C) Dos D) Tres

11. CONSIDERA UD. QUE EL PROCESO DE CONTROL ACTUAL DE ASISTENCIA DE SU I.E. DEBE:

A) Mantenerse B) Modificarse C) Cambiar por otro mejor

12. ESTA UD. DE ACUERDO QUE EN SU I.E. SE IMPLEMENTE UN SISTEMA DE CONTROL DE ASISTENCIA MEDIANTE LECTOR DE HUELLA DACTILAR CON LA YUDA DE UN COMPUTADOR:

A) Si B) No

13. DE SER AFIRMATIVA SU RESPUESTA EN LA PREGUNTA 12, CUAL ES LA PRINCIPAL RAZON PARA ELLO:

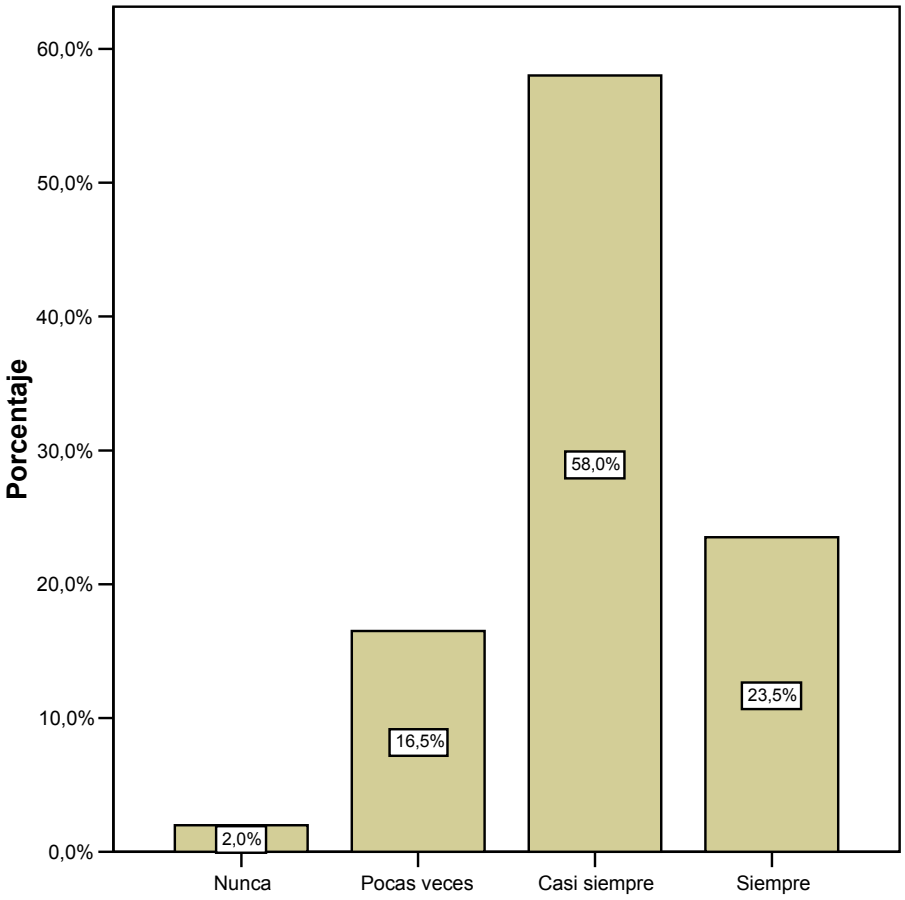
A) Para evitar horas de pérdida de clase.
B) Evitar favoritismo personal
C) Tener mejor control del personal docente y administrativo.

14. DE SER NEGATIVA SU RESPUESTA EN LA PREGUNTA 12. INDICAR LAS RAZONES QUE LO LLEVA A ELLO:

A) Temor al cambio.
B) Desconocimiento de la tecnología biométrica.
C) Evitar el control de las autoridades.

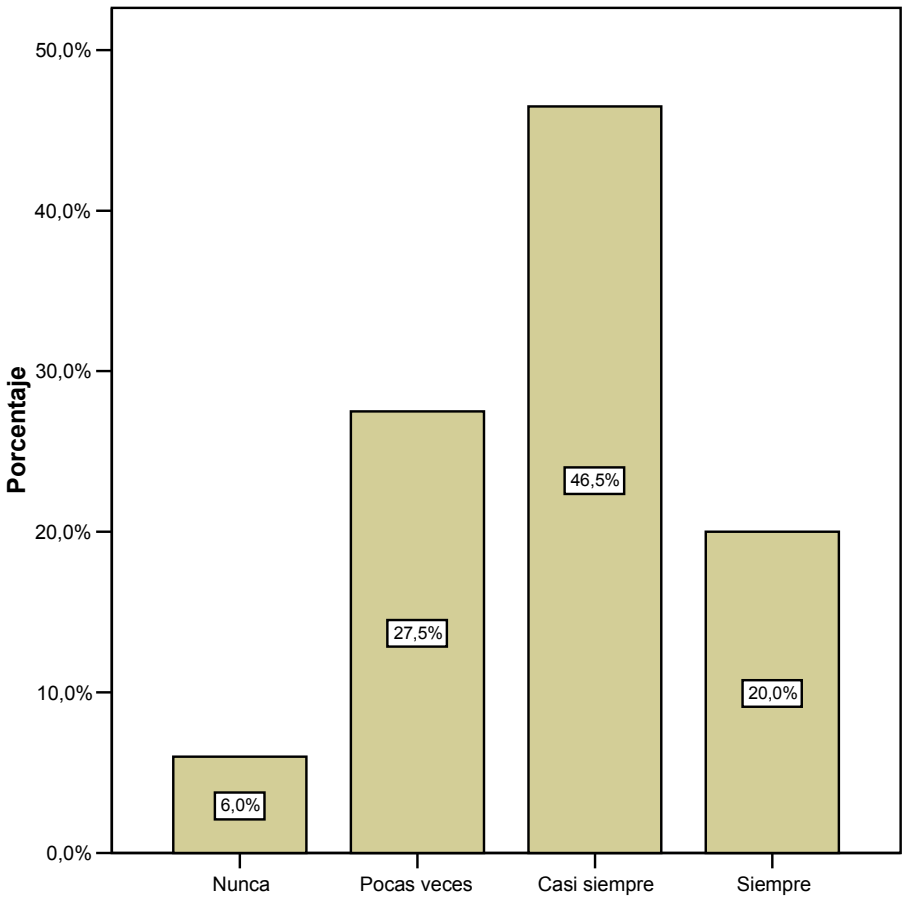
RESULTADOS E INTERPRETACIÓN DEL CUESTIONARIO APLICADO A LOS ALUMNOS

1. TUS PROFESORES ASISTEN PUNTUALMENTE AL DICTADO DE CLASES



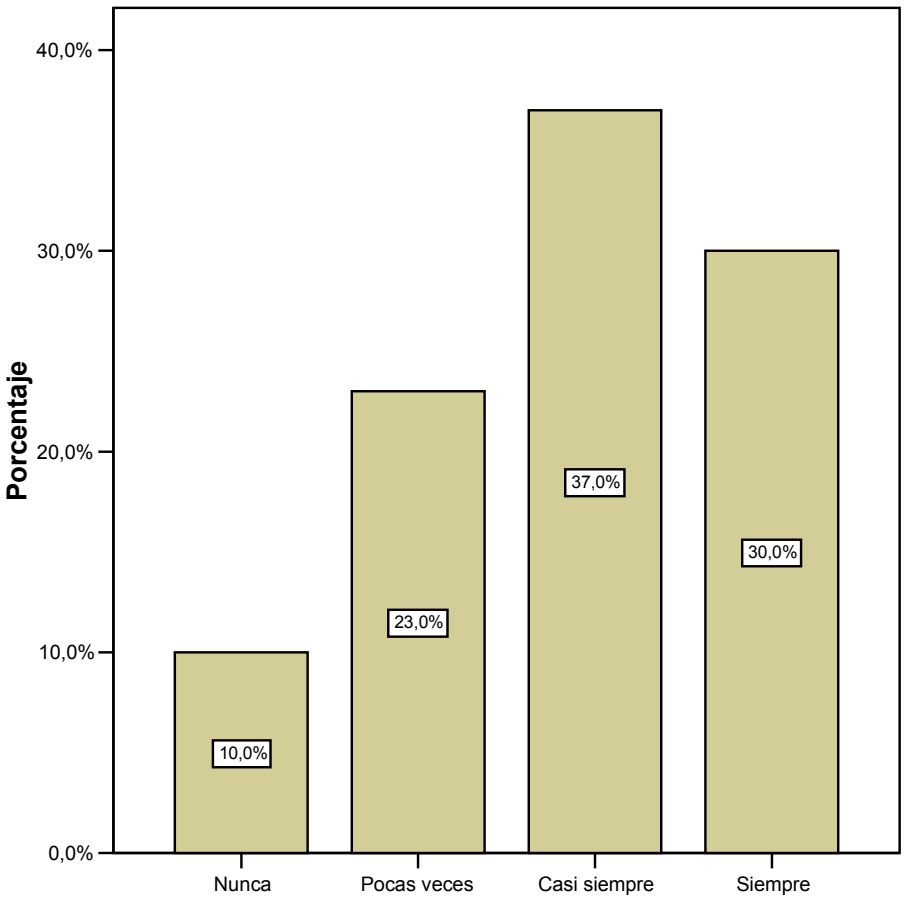
- Se puede afirmar que sólo el 23,5% de alumnos considera que los profesores asisten a clase puntualmente.

2. LAS CLASES CORRESPONDIENTES A LA PRIMERA HORA, SE INICIAN EXACTAMENTE A LA HORA ESTABLECIDA



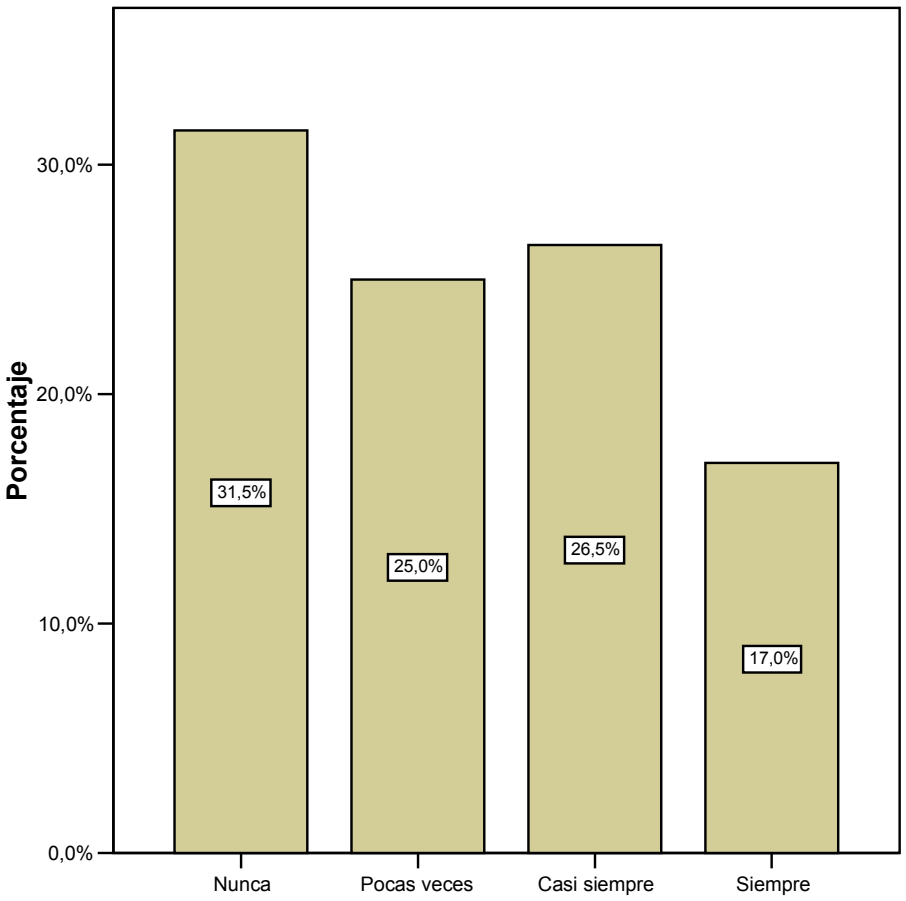
- Sólo el 20% afirma que los docentes asisten puntualmente a la primera hora de clases.

3. LA SALIDA DEL AULA EN LA ÚLTIMA HORA DE CLASES ES EXACTAMENTE A LA HORA ESTABLECIDA



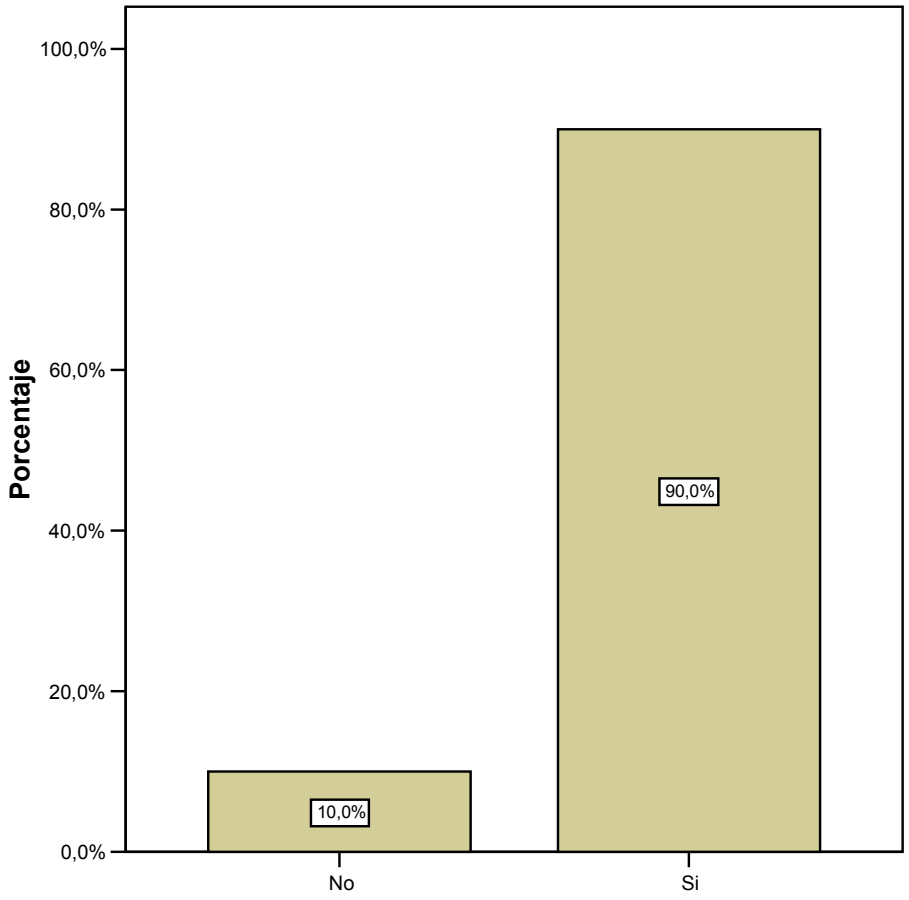
- De acuerdo al gráfico que solo el 30% del alumnado declara que la hora de clases respecto a la última hora se respeta.

4. LAS HORAS DE CLASE PERDIDAS POR LAS TARDANZAS O INASISTENCIAS DE TUS PROFESORES SON RECUPERADAS



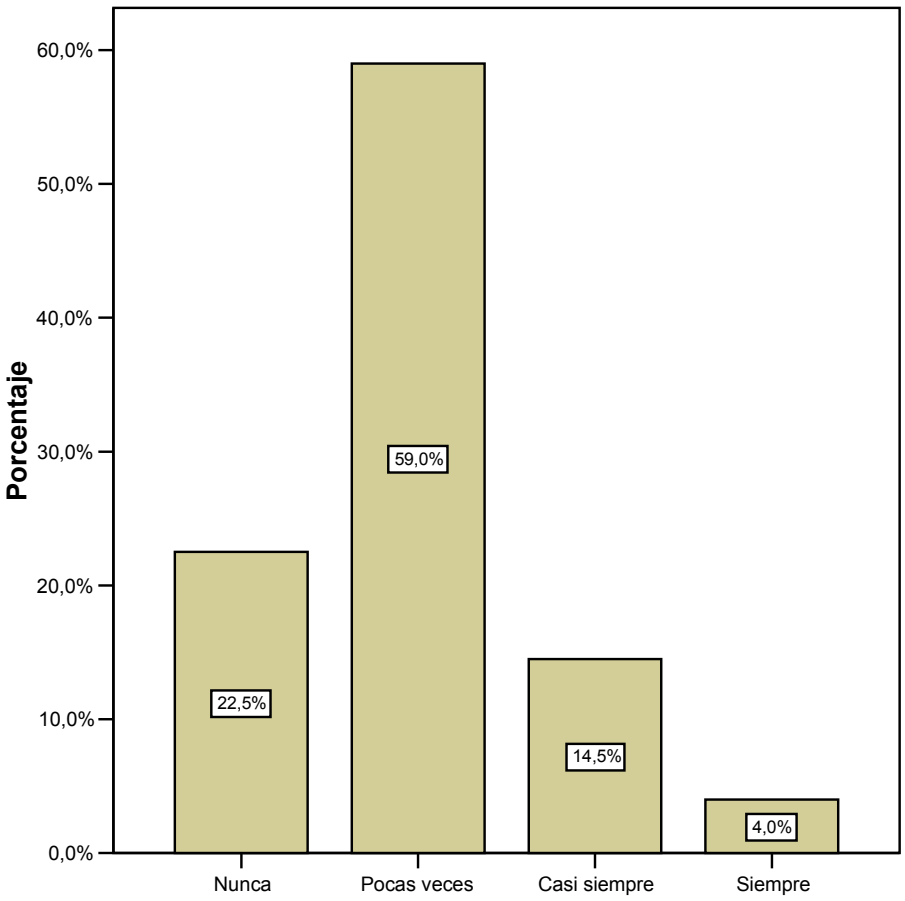
- El 17% del alumnado afirma que las clases perdidas son recuperadas, perjudicándose al alumnado en su proceso enseñanza - aprendizaje.

5. CONSIDERAS QUE DEBERIA HABER UN MAYOR CONTROL EN LA ASISTENCIA DE LOS PROFESORES A LA INSTITUCIÒN EDUCATIVA



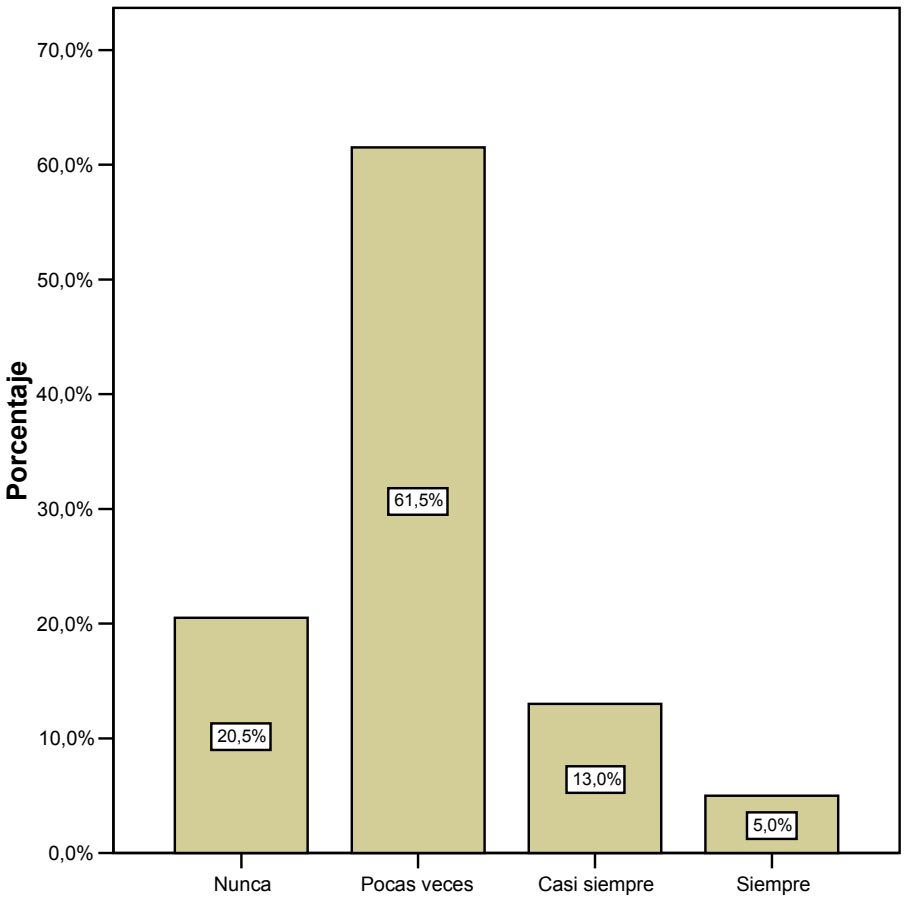
- El 90% del alumnado esta de acuerdo que debe haber mayor control en la asistencia de los profesores.

6. LOS PROFESORES FALTAN A LA INSTITUCIÒN EDUCATIVA



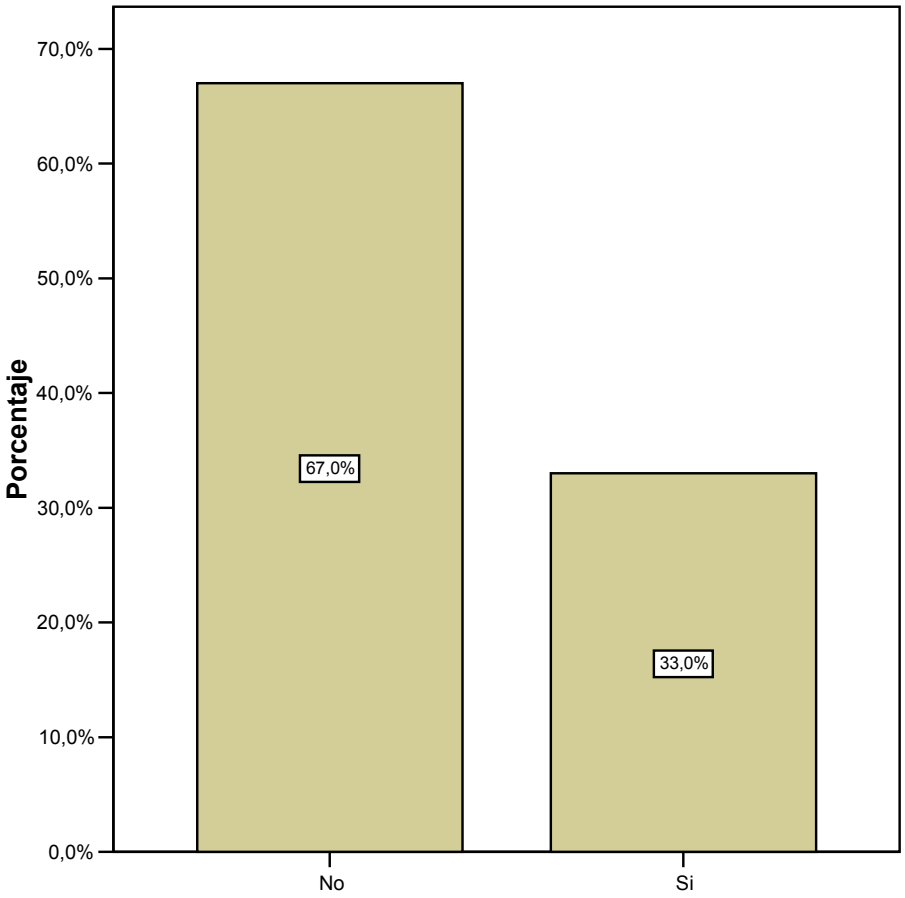
- El 4% del alumnado percibe que los profesores siempre faltan a la Institución Educativa.

7. ALGUNOS PROFESORES SE AUSENTAN EN HORAS DE CLASE



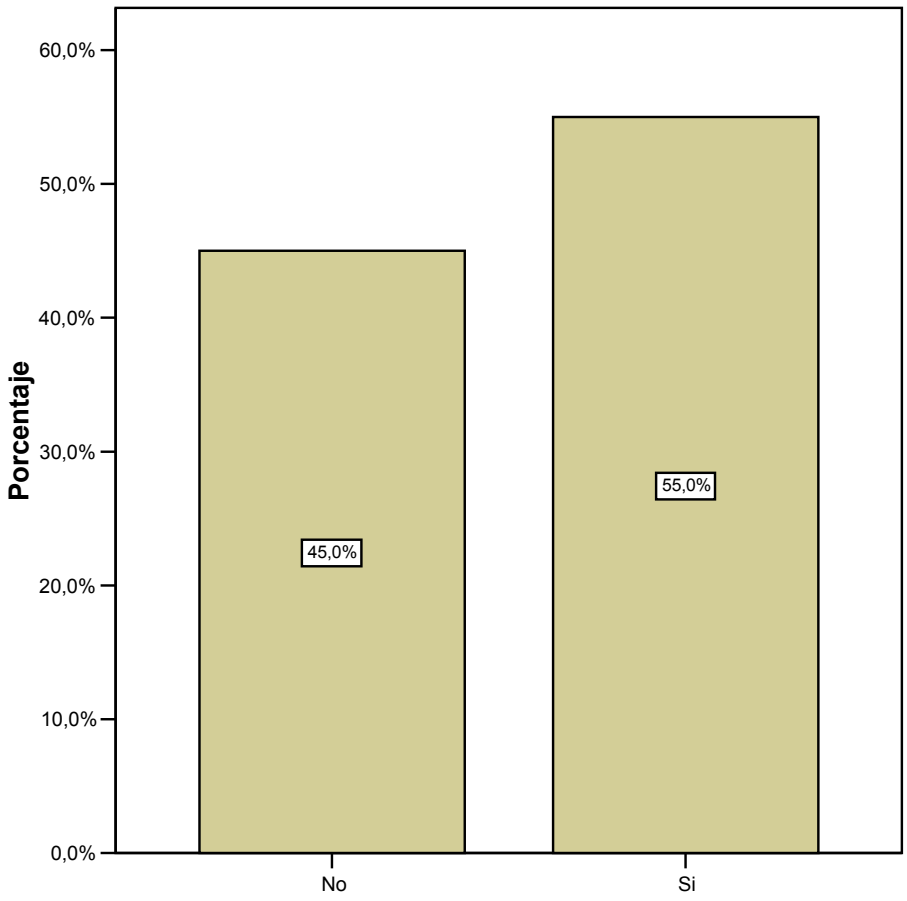
- Sòlo el 20,5% el alumnado afirma que los docentes no se ausentan durante el desarrollo de las lecciones en la institución Educativa.

8. CUANDO ALGUNOS DE TUS PROFESORES NO ASISTEN, LA SUBDIRECCIÒN O EL AUXILIAR INGRESA A TU SALÒN A REEMPLAZAR A TU PROFESOR EN SU HORA CORRESPONDIENTE.



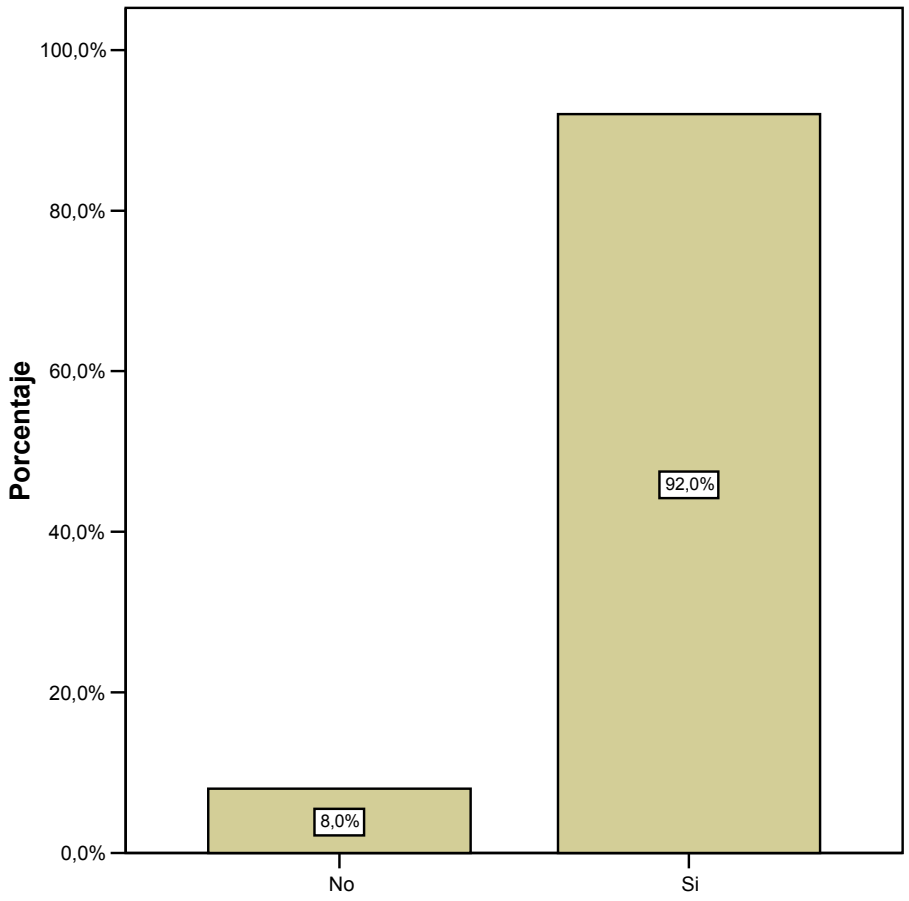
- El 67% del alumnado considera que las aulas sin profesor no son reemplazados por el auxiliar a cargo o por el Sub Director.

9. CONSIDERA UD. QUE EXISTE UN SEGUIMIENTO ADECUADO POR PARTE DE LA DIRECCIÒN O SUB DIRECCIÒN DE LA I.E. SOBRE LA ASISTENCIA DE DOCENTES.



- Se puede afirmar que el 55% de alumnos considera que no se hace seguimiento a la asistencia de los profesores.

10. ESTA UD. DE ACUERDO QUE SE IMPLEMENTE EN TU COLEGIO UN SISTEMA QUE CON LA AYUDA DE UN COMPUTADOR PERMITA UN MAYOR CONTROL DE ASISTENCIA PARA TUS PROFESORES.

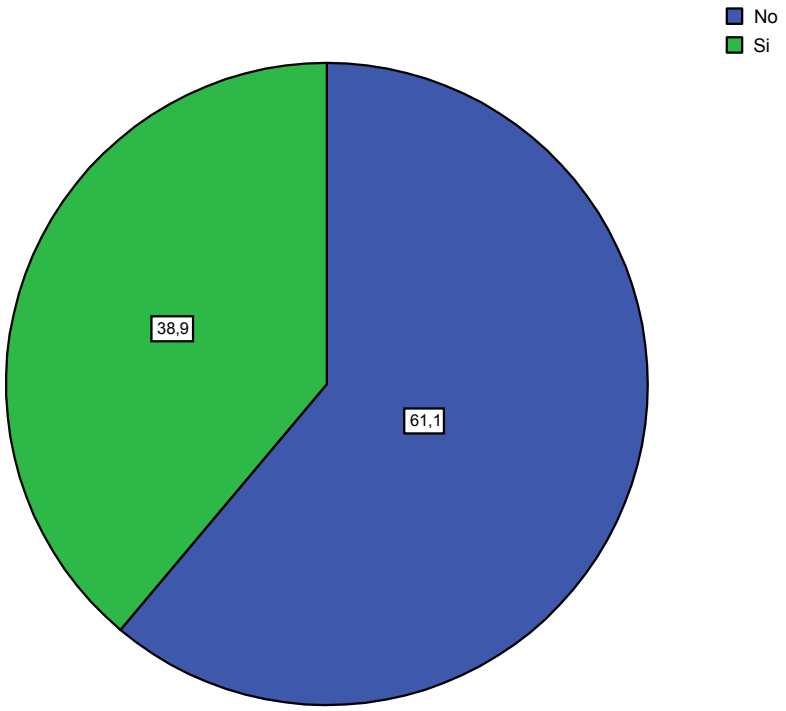


- El 92% del alumnado esta de acuerdo que se implemente un Software de control de asistencia del personal.

RESULTADOS E INTERPRETACIÓN DEL CUESTIONARIO APLICADO A LOS DOCENTES

1. CONSIDERA QUE EL PROCESO DE CONTROL DE PERSONAL DOCENTE Y ADMINISTRATIVO DE LA I.E. ES EL APROPIADO

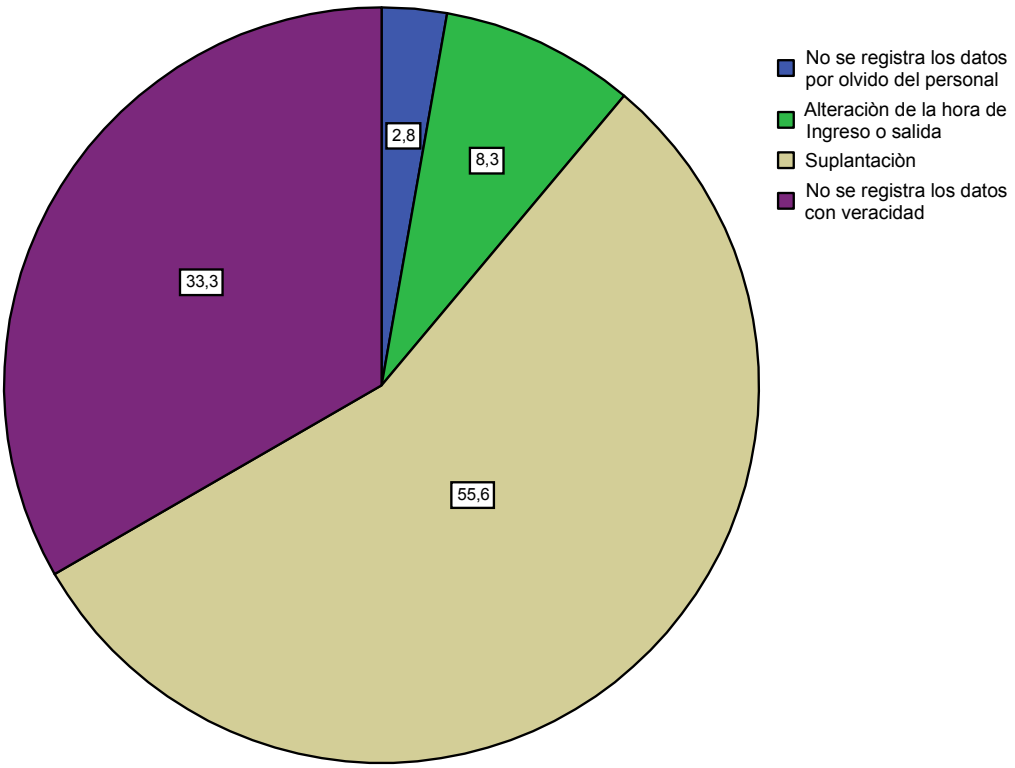
(PORCENTAJE)



- El 61,1% del personal de la Institución afirma que sistema de control actual esta desfasado e inapropiado.

2. EN EL PROCESO ACTUAL DE CONTROL DE ASISTENCIA QUE MANEJA LA INSTITUCIÒN EDUCATIVA. ¿CUÁLES DE LAS POSIBLES FALTAS SE COMETEN?

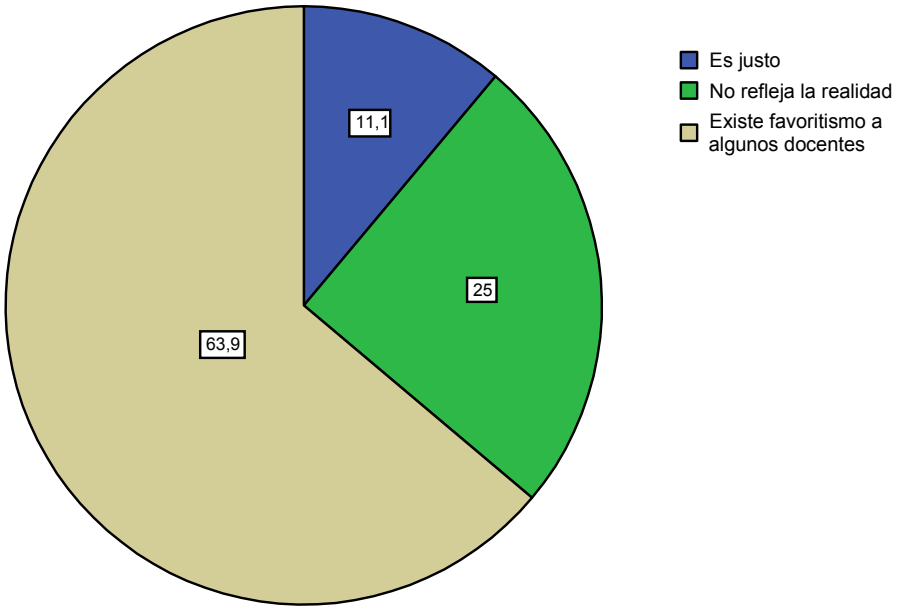
(PORCENTAJE)



- El 55,6% del personal considera que la suplantación es uno de los talones de Aquiles de la Institución Educativa en el momento de usar el proceso de control de asistencia.

3. RESPECTO AL CONSOLIDADO DE TARDANZAS O FALTAS QUE SE ENVIA A LA UGEL/DREC CONSIDERA UD. QUE ES JUSTO

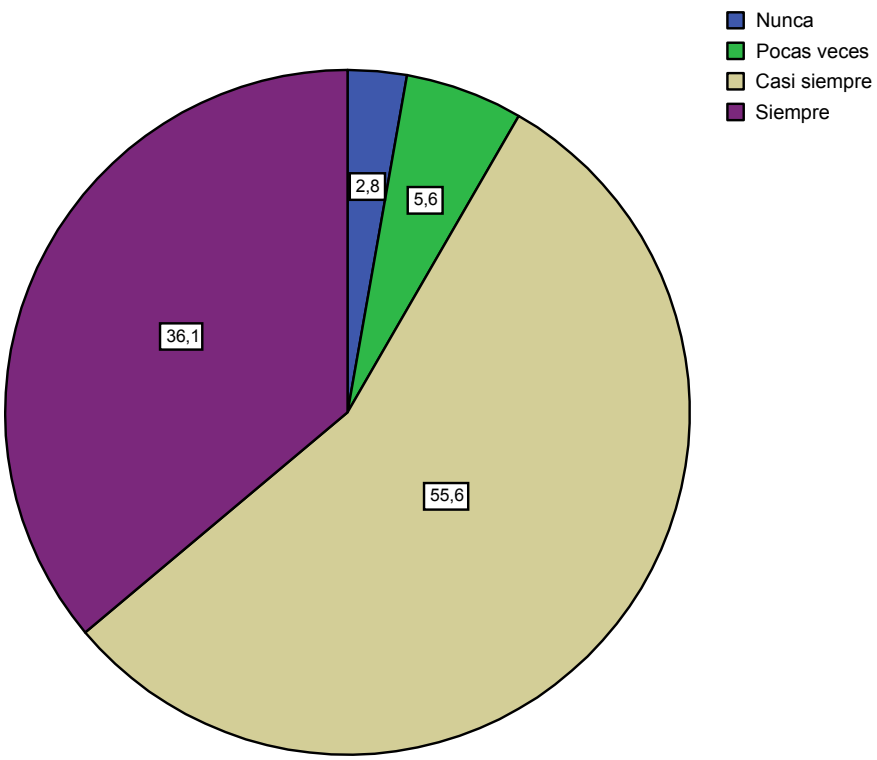
(PORCENTAJE)



- El 63,9% de docentes considera que al momento de realizar el consolidado de asistencia existe favoritismo a un grupo de docentes.

4. ASISTE PUNTUALMENTE AL DICTADO DE SUS CLASE

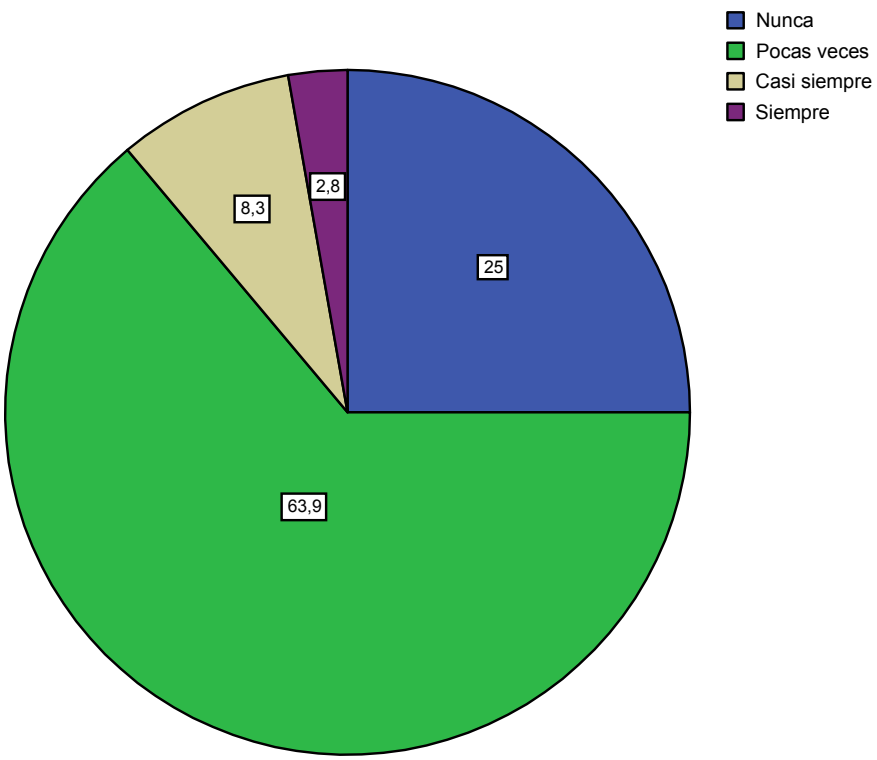
(PORCENTAJE)



- Sólo el 36,1% de los trabajadores de la Institución Educativa asisten puntualmente al dictado de su asignatura.

5. LAS HORAS DE CLASE PERDIDAS POR TARDANZA O FALTAS DE UD. LOS RECUPERA:

(PORCENTAJE)

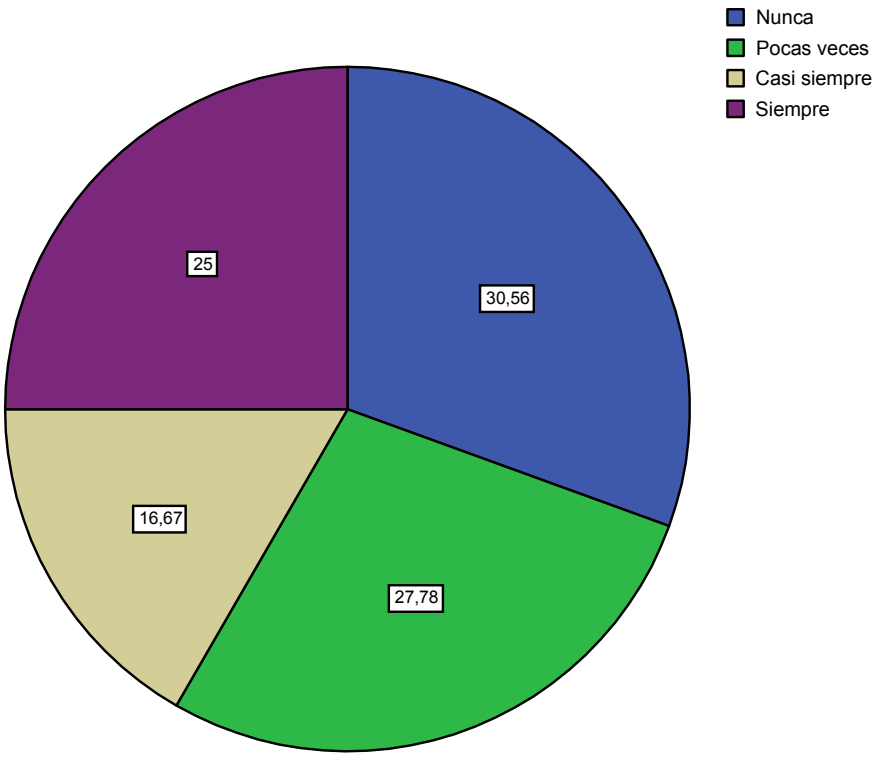


- Sólo el 2,8% de los docentes de la Institución Educativa afirma recuperar las clases perdidas.

6. CUANDO UD. SALE DE LA I.E. EN HORAS DE CLASE , UTILIZA PAPELETA DE DESPLAZAMIENTO

(PORCENTAJE)

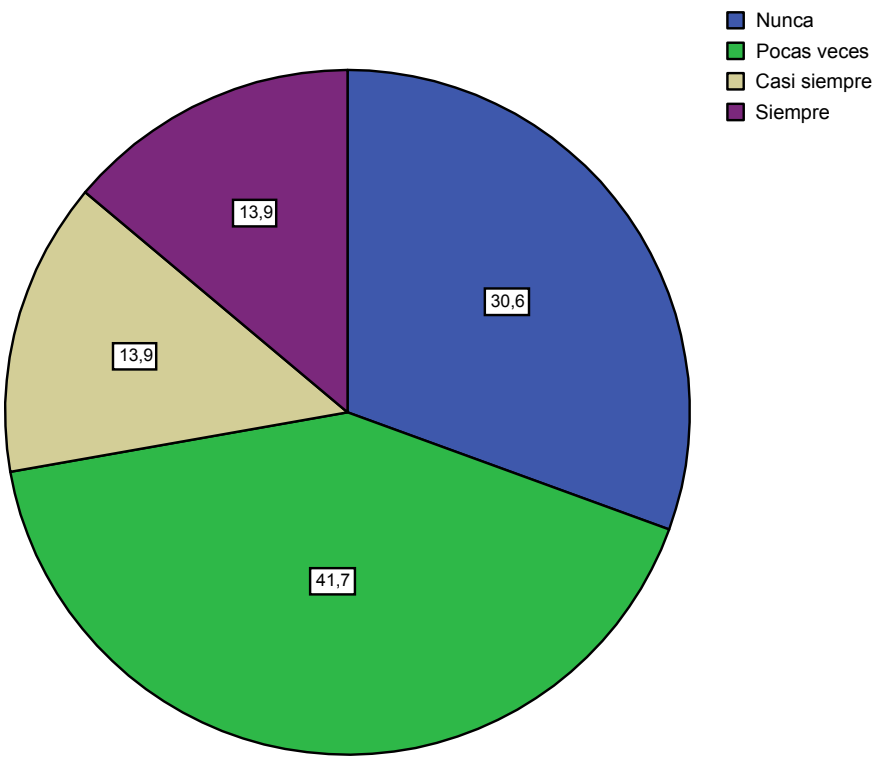
- Sólo el 36,1% de los trabajadores de la Institución Educativa asisten puntualmente al dictado de su asignatura.



- El 30,56% de los encuestados afirma que nunca recupera las clases perdidas.

7. SU SALIDA DE LA I.E. ES DE ACUERDO A SU HORARIO ESTABLECIDO.

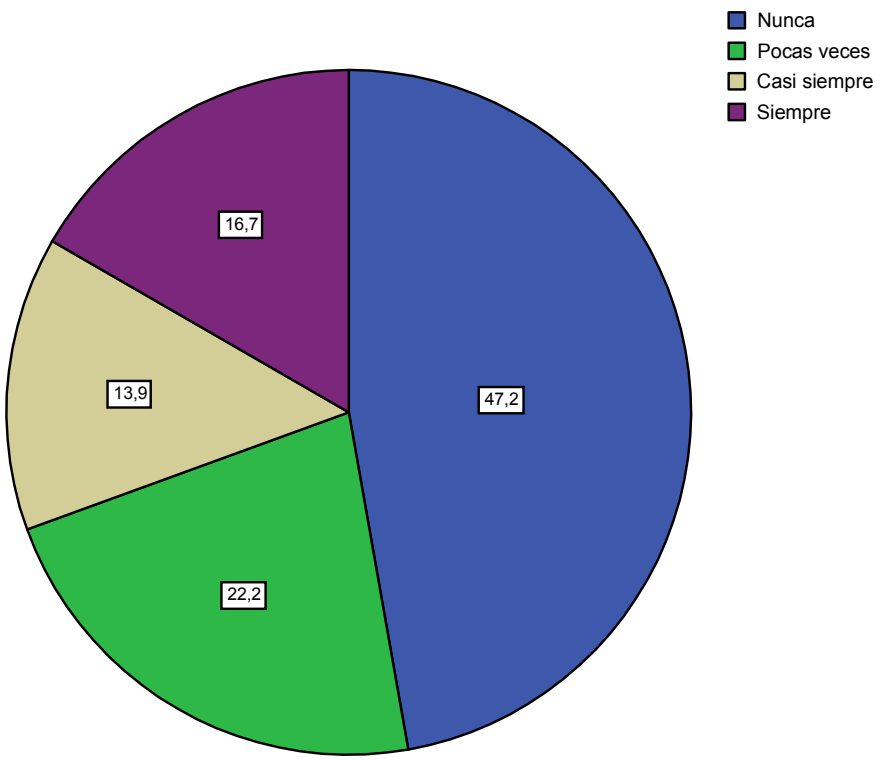
(PORCENTAJE)



- Sólo el 30,6% termina sus labores respetando su finalización de la misma.

8. AL MOMENTO DE HACER USO DEL ACTUAL PROCESO DE CONTROL DE ENTRADA/SALIDA. ¿UD. REGISTRA SU HORA REAL?

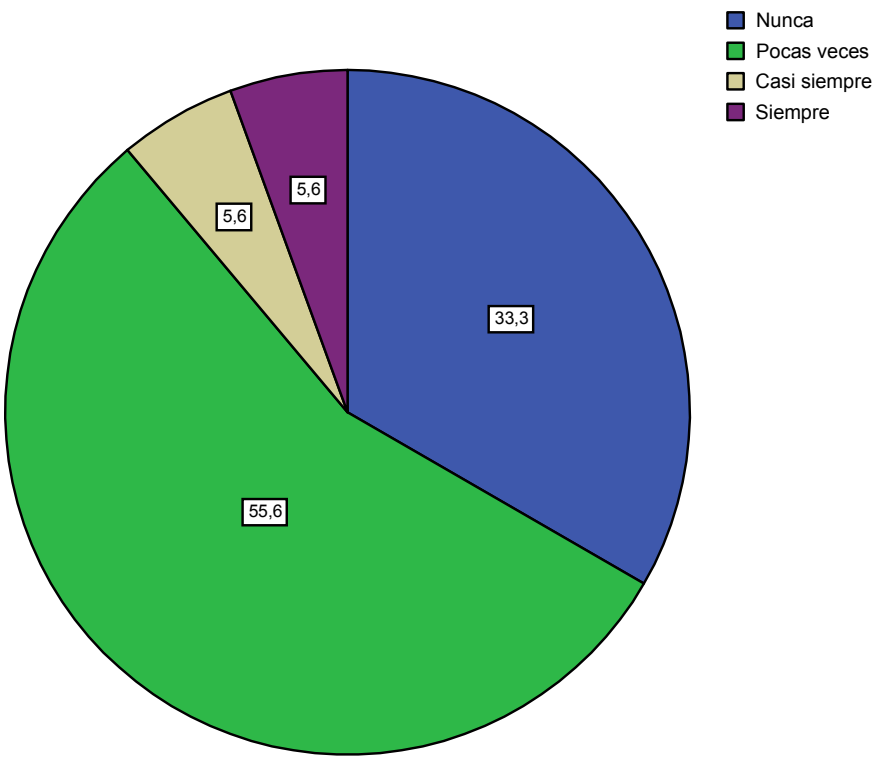
(PORCENTAJE)



- El 16,7% de los docentes afirman que siempre registran su hora real al ingresar a su Institución Educativa.

9. UNA VEZ REGISTRADO SU HORA DE INGRESO O SALIDA ¿UD. ACOSTUMBRA MODIFICARLO HACIENDO UNA CORRECCIÒN MANUALMENTE?

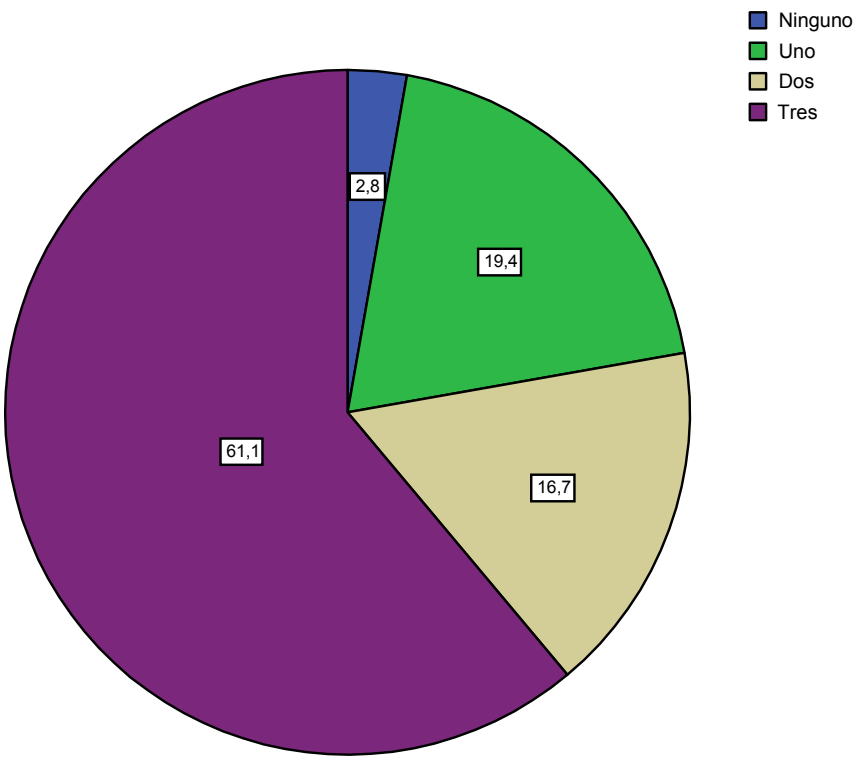
(PORCENTAJE)



- El 5,7% de los docentes afirman que siempre realizan corrección manualmente una vez ya registrado su asistencia.

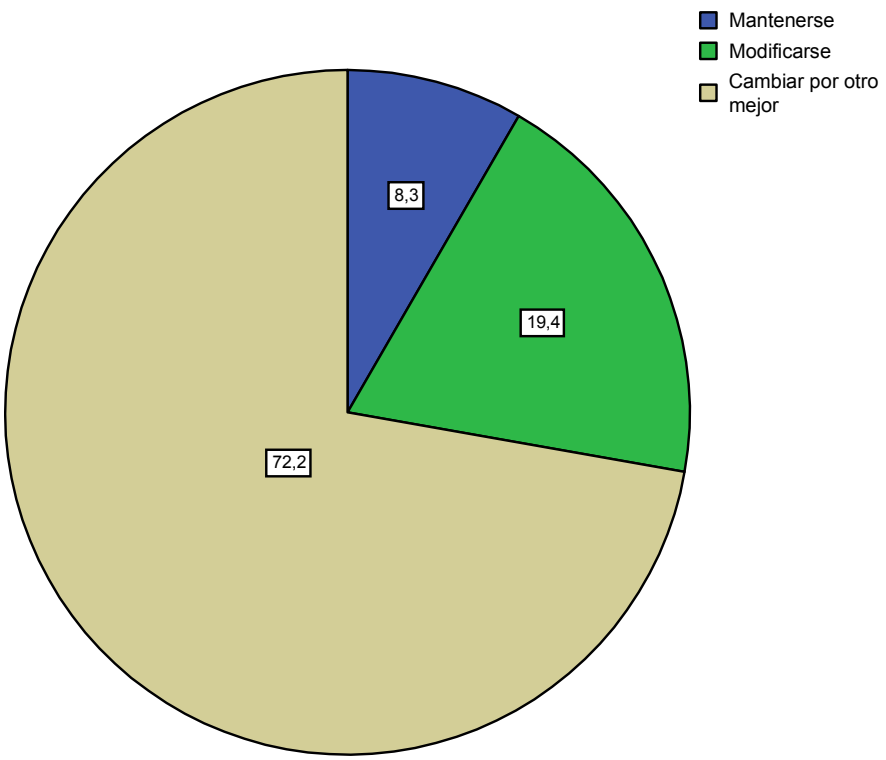
10. DE LOS TRES DIAS DE PERMISO POR MOTIVOS PERSONALES ¿ DE CUÀNTOS DIAS HIZO USO?

(PORCENTAJE)



- El 61,1 % de los trabajadores de la Institución Educativa consumen rápidamente de los 03 días de licencia interna.

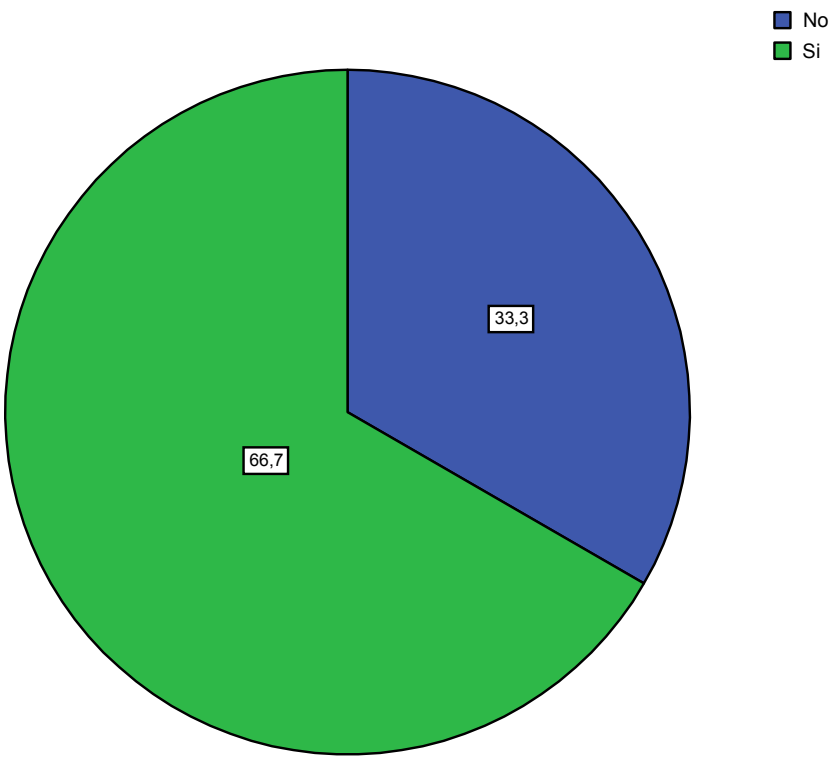
11. CONSIDERA UD. QUE EL PROCESO DE CONTROL ACTUAL DE ASISTENCIA DE SU I.E. DEBE :
(PORCENTAJE)



- El 72,2 de los encuestados afirma que el sistema de control de asistencia debe cambiarse por otro mejor para así evitar su vulnerabilidad.

12. ESTA UD. DE ACUERDO QUE EN SU I.E. SE IMPLEMENTE UN SISTEMA DE CONTROL DE ASISTENCIA MEDIANTE LECTOR DE HUELLA DACTILAR CON LA YUDA DE UN COMPUTADOR.

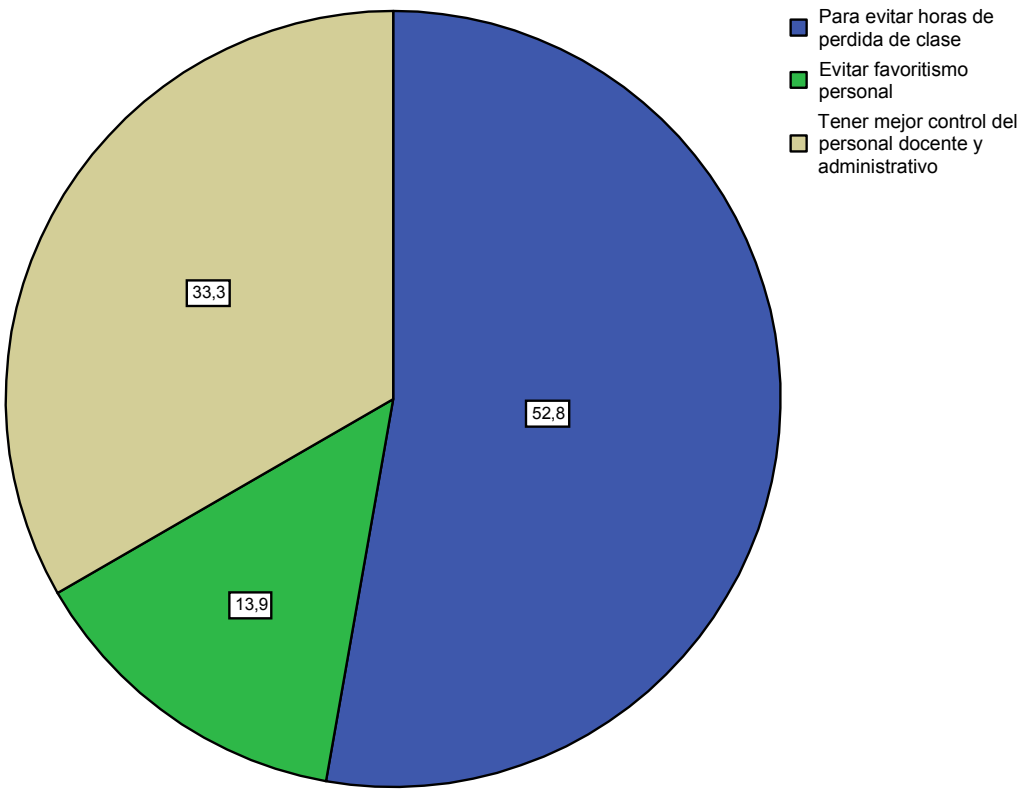
(PORCENTAJE)



- El 66,7% de los encuestados de la Institución Educativa están de acuerdo que se implemente un sistema de control de asistencia usando tecnología dactilar.

13. DE SER AFIRMATIVA SU RESPUESTA EN LA PREGUNTA 12, CUAL ES LA PRINCIPAL RAZON PARA ELLO.

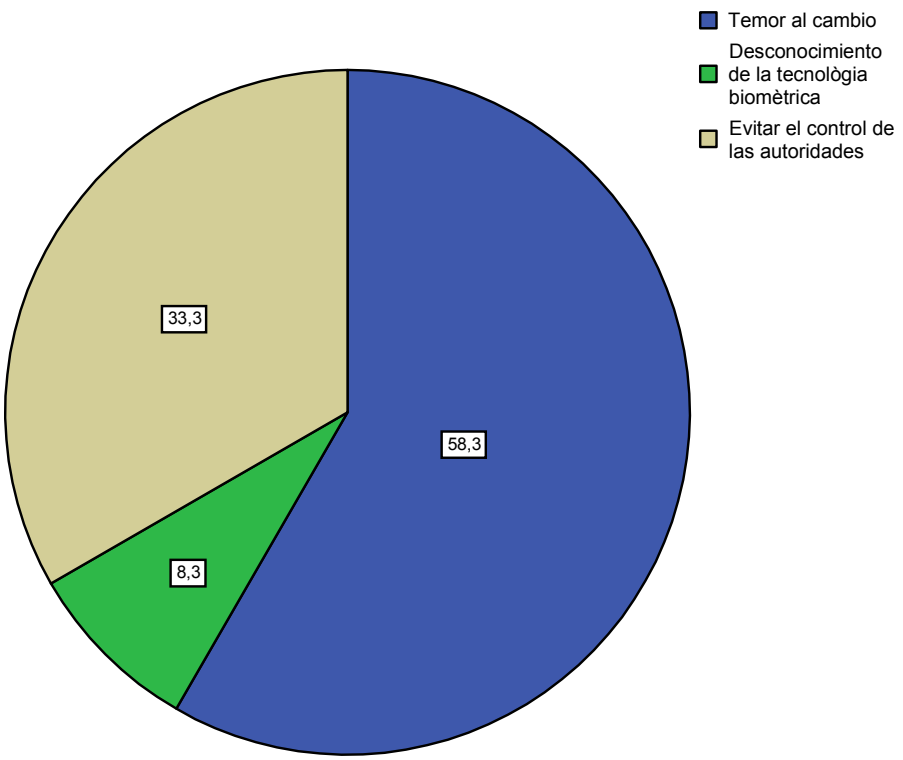
(PORCENTAJE)



- El 52,8 % de los encuestados que desean que se implemente un nuevo sistema de control es porque se quiere evitar la pérdida de clase en la Institución Educativa.

14. DE SER NEGATIVA SU RESPUESTA EN LA PREGUNTA 12. INDICAR LAS RAZONES QUE LO LLEVA A ELLO:

(PORCENTAJE)



- El 58,3% de los trabajadores de la Institución Educativa que no desean que se cambie el sistema de control es por temor al cambio.