UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMATICA

TESIS DE GRADO

"BIOMETRIA DE TECLEO DE LA CONTRASEÑA DEL USUARIO PARA LA SEGURIDAD DE ACCESO EN APLICACIONES DE INTERNET"

PARA OPTAR EL TITULO DE LICENCIATURA EN INFORMATICA
MENCION A INGENIERIA EN SISTEMAS INFORMATICOS

POSTULANTE: Ehyci Lincey Laurani Lima
TUTOR: Lic. Efraín Silva Sánchez
REVISOR: Lic. Javier Reyes Pacheco

LA PAZ – BOLIVIA
2011

DEDICATORIA

Este trabajo va dedicado a mi madre Eugenia por darme ánimos; a mi padre Juan que nunca dejo de apoyarme; a mis hermanas Kenia y Emely por confiar en mí. mi amor por estar conmigo en las buenas y en las malas.

Con mucho amor para todos ellos.

AGRADECIMIENTOS

A Dios por darme la sabiduría y las fuerzas necesarias para la culminación de este trabajo.

A mis padres por estar en todos y cada una de las batallas de la vida, por ayudarme en todo momento para lograr mis objetivos y por ser un verdadero ejemplo de vida.

A mi Tutor Lic. Efraín Silva Sánchez por su gran paciencia y aportes en el desarrollo del presente trabajo.

De igual manera a mi Revisor Lic. Javier Reyes Pacheco, por su apoyo incondicional, por el tiempo dedicado a la revisión, por los aportes, correcciones, observaciones y valiosas sugerencias.

También deseo agradecer a todos los docentes de la Carrera de Informática por su aporte en mi formación universitaria, y a todos mis amigos que siempre me apoyaron.

RESUMEN

El presente trabajo se realizo con el objetivo de reconocer los patrones de tecleo mediante la biometría de tecleo de la contraseña del usuario y de esta manera mejorar la seguridad de acceso en aplicaciones de internet, para esto se hallaron indicadores de tasas de error que nos aseguren la aplicación de este método para el proceso de autenticación.

La principal problemática que se encontró para la realización del presente trabajo fue ¿Es posible desarrollar un prototipo que mediante el uso de biometría de tecleo aplicado a la contraseña del usuario pueda mejorar la seguridad de acceso en aplicaciones de internet? Para la realización se aplico el método estadístico por lo que se desarrollo un prototipo bajo la plataforma .NET posteriormente se realizo la fase de experimentación en dos oportunidades, en donde se puso a prueba a 40 estudiantes universitarios.

Los resultados obtenidos una vez realizada todas pruebas fueron satisfactorios, obteniendo indicadores para la primera prueba: Tasa de Falsa Aceptación 4.44%, Tasa de Falso Rechazo 6.67 % y Tasa de Error de Cruce 8%; Para la segunda prueba: Tasa de Falsa Aceptación 3.33%, Tasa de Falso Rechazo 10% y Tasa de Error de Cruce 8%. Posteriormente se aplico la confiabilidad mediante reaplicación de pruebas que nos dieron correlación “muy alta” entre las pruebas de la primera y segunda medición de r=0.91 y r=0-90 donde equivale a decir que el prototipo analizado es confiable, en cuanto a la estabilidad a través del tiempo, por lo tanto brinda mayor seguridad en las aplicaciones de internet.

ABSTRACT

This study was conducted with the aim of recognizing patterns of typing by typing biometrics user's password and thereby improve the security of Internet applications access to this are indicators of error rates that will ensure the application of this method for the authentication process.

The main problem that was found for the realization of this work was Is it possible to develop a prototype using typing biometrics applied to the user's password can enhance security in applications access the Internet?
To perform the statistical method was applied so that a prototype was developed under the platform. NET then completed the testing phase on two occasions, where it was tested at 40 university students.

The results obtained upon completion of all tests were satisfactory, get directions to the first test: False Acceptance Rate 4.44% False Rejection Rate of 6.67% and Crossover Error Rate 8% for the second test: False Acceptance Rate 3.33 % False Rejection rate of 10% and Crossover Error Rate 8%. Reliability is then applied by reapplication of correlation tests that we gave "very high" between the evidence of the first and second measurement of r = 0.91 and r = 0-90 which is to say that the prototype is tested reliable, in terms of stability over time, thus providing greater security in Internet applications.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

Capítulo I

1. INTRODUCCION

Hoy en día la evolución de la tecnología en particular de los dispositivos electrónicos, sistemas informáticos progresa de forma imparable, y nos rodea cada vez más en nuestro entorno diario de trabajo y de ocio. Nos vemos habitualmente inmersos en ambientes donde la presencia de elementos tecnológicos es constante, de manera que en nuestro entorno profesional ya no se concibe el desempeño de las tareas necesarias sin el empleo de ordenadores y redes de comunicaciones, como la red de Internet.

Dentro del amplio abanico de tecnologías cuyo desarrollo vivimos de cerca en nuestro día a día, uno de los tipos que han surgido con fuerza en los últimos tiempos son los sistemas *biométricos* aplicados a la seguridad, dichos sistemas permiten dar control de acceso a lugares o a información restringida.

Los sistemas biométricos pueden ser de tipo *estático* si se miden características físicas o *dinámicas* si lo que se mide es el comportamiento de los usuarios. Por ejemplo, la huella dactilar es una biométrica estática mientras que la dinámica de tecleo es una biométrica dinámica.

De manera particular la biometría de tecleo de un usuario, se centra en las técnicas necesarias para identificar en qué medida existe una cierta regularidad en el modo de teclear de un usuario en un sistema informático. En este tipo de tecnología no se hace necesario tener hardware adicional para el muestreo de patrones de tecleo, y esto lo hace ideal para aplicaciones sobre Internet, ya que todos los ordenadores comparten la capacidad de admitir el tecleo de los usuarios.

Gracias a las ventajas de la biometría de tecleo la presente tesis pretenderá el desarrollo de un prototipo que fortalecerá la seguridad de acceso en aplicaciones de internet basado en la contraseña aprovechando el hecho de que cada persona tiene un ritmo único al escribir.

1. ANTECENDENTES

A lo largo de la historia el ser humano desarrollo varios métodos con el fin de poder autentificarse, gracias a la biometría se tienen el timbre de voz, la forma del rostro, las huellas dactilares, entre otros. Así también el uso de contraseñas, tarjetas de acceso, etc. Son claros ejemplos de los intentos por encontrar métodos de identificación confiables. El objetivo de esta identificación es permitirle a una persona el acceso a un ambiente protegido o a algún recurso físico o informático, todo esto con el fin de evitar la suplantación de identidad de personal autorizado.

Ante la gran gama de biometrías existentes el de tecleo, ha sido objeto de estudio por parte de varios investigadores en años recientes. Por tal motivo el presente trabajo usara el mismo para aumentar la seguridad de acceso utilizando la contraseña del usuario en aplicaciones de internet.

A continuación citaremos las investigaciones más importantes:

Shepherd[1], publicó su investigación en donde se presento un esquema continuo de autenticación. El objetivo del estudio fue desarrollar un sistema que pudiera identificar un usuario en tan corto tiempo como sea posible.

Monrose y Rubin[2], presentaron su investigación donde estudian el reconocimiento de patrones de tecleo como un biométrico de autenticación para el acceso a estaciones de trabajo. Los resultados de esta investigación, determinaron que las tasas de identificación correcta usando un clasificador probabilístico ponderado fue de aproximadamente 87.18%, lo que representa una mejora sustancial en comparación al método de la distancia Euclidiana (83.22%) y al método del puntaje no ponderado (85.63%).

[1] [Shepherd, 1995], "Continnons anthentication by analysis of keyboard typing characteristics", Brighton.
[2] [Monrose y Rnbin, 1999], "Keystroke Dynamics as a Biometric for Anthentication", Elsevier Science Pnblishers B. V. Amsterdam.

Sin embargo, la técnica del clasificador Bayesiano obtuvo una tasa de efectividad de aproximadamente 92.14%, representando una mejora de casi 5%sobre el clasificador ponderado. Adicionalmente, la investigación determino que es mejor el uso de texto estructurado en vez de permitir a los usuarios escribir texto arbitrario.

Araujo[3], presento un trabajo en el que empleaba clasificadores de lógica difusa. Un trabajo importante es el logrado por Nisenson[4], que aplicó biometría de dinámicas de tecleo como un sistema de detección de intrusos, usando el algoritmo de compresión Lempel-Ziv.

Nicholas Bartlow[5], realizo una investigación en la universidad de Virginia, donde tomo alrededor de 10.000 muestras provenientes de 53 usuarios, de los cuales 41 resultaron aceptables para el experimento. Empleo múltiples métodos para el reconocimiento de patrones de tipeo, como Naive Bayes, bosques aleatorios y redes neuronales. Este trabajo reporto resultados puntuales de 7% de FAR y 7% de FRR para frases cortas (menos de 7 caracteres), asi mismo, 5% de FAR y 5% de FRR para frases largas.

Gerardo Iglesias Galván[6], presentó una tesis en la que aplica la biometría dinámica de tecleo en los dispositivos móviles. Y la empresa "AdmitOne Security" antes llamada "Biopassword" quien actualmente está comercializando este tipo de sistemas de autenticación en sus versiones Enterprise y de Internet para transacciones bancarias.

En la carrera de Informática de la Universidad Mayor de San Andrés se tienen trabajos con respecto a biometría de identificación, como: Interpretación Grafológica, Reconocimiento de Patrones de Iris de los Ojos, Geometría de la Palma de la Mano, sin embargo no se encontró trabajos acerca de la Biometría de Tecleo.

Las investigaciones realizadas presentaron un aporte valioso para el presente trabajo, ya que muestran diferentes técnicas aplicables al reconocimiento de biometría de tecleo.

---

[3] [Aranjo, 2004], Investigación sobre Biometría Dinámica, Brasil. ieee latin america transactions, vol. 2, march 2004.

[4] [Nisenson, 2004], Aplico la dinámica de tecleo.

[5] [Nicholas Bartlow,2005], "Username and Password Verification throngh Keystroke Dynamics", Morgantown, West Virginia.

[6] [Gerardo Iglesias Galván, 2007], "Sistema de Antenticación para Dispositivos Móviles basado en Biometría de Comportamiento de Tecleo", México, D.F., Institnto Tecnológico de Morelia.

Como: los métodos Naive Bayes, bosques aleatorios, redes neuronales y lógica difusa. Asimismo, señalan los factores más relevantes para la medición de los ritmos de tecleo y especifican las diversas metodologías para la ejecución de las pruebas necesarias.

1. PLANTEAMIENTO DEL PROBLEMA.-

En la actualidad y en la mayoría de los países se ha puesto de moda la suplantación de identidad tanto en cuentas de correo como administrativas, esto se considera un delito informático y está penado por ley, sin embargo los castigos no ha frenado las malas intenciones de aquellas personas que se apoderan de dichas cuentas y continúan ocasionando caos informático. Para obtener esta información existen muchos métodos y técnicas. Entre las más importantes podríamos mencionar: La ingeniería social[7], los keyloggers[8], troyanos[9], malwares[10], ataques de fuerza bruta[11], etc. Todas estas técnicas aprovechan las vulnerabilidades que existen en un sistema para cumplir su propósito, por lo cual esto afecta la privacidad del usuario.

La autenticación juega un papel muy importante en la seguridad informática, y lamentablemente la verificación basada en usuario y contraseña no es segura. Ya que cualquier persona obteniendo dicha información podría acceder a la cuenta de terceros sin mayor problema, utilizando técnicas y métodos que logran romper la seguridad para fines maliciosos.

Uno de los factores que impiden mayor seguridad en el acceso es la falta de recursos económicos para implementar nuevos modelos ya que en la mayoría de los controles de acceso requieren software pero sobretodo hardware que representa mayor coste económico por lo cual no es accesible para todos, por tal motivo se requiere una aplicación que no solo brinde mayor seguridad en el acceso si no que sea económico y accesible para todo usuario.

---

[7] Práctica de obtener información confidencial a través de la manipnlación de nsnarios legítimos.

[8] Registra cada pnlsación del teclado y envía esta información a ciberdelincnentes vía Internet.

[9] Son programas maliciosos qne están disfrazados como algo inocno o atractivo qne invitan al nsnario a ejecntarlo ocnltando nn software malicioso.

[10] Software malicioso o software malintencionado es nn tipo de software qne tiene como objetivo infiltrarse o dañar nna compntadora sin el consentimiento de sn propietario.

[11] Forma de recnperar nna clave probando todas las combinaciones posibles hasta encontrar aqnella qne permite el acceso.

3.1. PROBLEMAS ESPECIFICOS

- No hay un registro de muestreo de patrones de tecleo de la contraseña del usuario.
- La contraseña no es suficientemente segura, por lo cual se necesita un mejor control para reconocer al usuario.
- No existen métodos matemáticos ni estadísticos que permitan identificar y comprobar si es o no es el usuario.
- No existe un modelo biométrico de tecleo que protege la contraseña del usuario.
- No existe un procedimiento que pueda verificar si el usuario se encuentra registrado en la base de datos.
- Existe Suplantación de identidad, lo cual afecta la seguridad y privacidad de los usuarios
- No hay un modulo de verificación que valide la identidad del usuario mediante datos históricos en base a su pulsación de tecleo.

3.2. DEFINICION DEL PROBLEMA

¿Es posible desarrollar un prototipo que mediante el uso de biometría de tecleo aplicado a la contraseña del usuario pueda mejorar la seguridad de acceso en aplicaciones de internet?

2. HIPOTESIS.-

H: La biometría de tecleo de la contraseña del usuario mejora la seguridad de acceso en aplicaciones de internet.

5. OBJETIVOS.-

5.1. OBJETIVO GENERAL

Desarrollar un prototipo biométrico de tecleo de la contraseña del usuario para mejorar la seguridad de acceso en aplicaciones de internet.

5.2. OBJETIVOS ESPECIFICOS

- Crear una base de datos para registros de usuarios y muestras de patrones de tecleo de la contraseña del usuario.
- Desarrollar un procedimiento que pueda verificar si el usuario se encuentra registrado en la base de datos.
- Implementar controles mediante el uso de la contraseña para que puedan reconocer al usuario
- Desarrollar un modulo de ingreso de muestras que capture los tiempos de la contraseña del usuario.
- Desarrollar un modulo de verificación que valide la identidad del usuario mediante datos históricos en base a su pulsación de tecleo.
- Manipular procesos matemáticos y estadísticos que permitan verificar la identidad del usuario.
- Verificación del prototipo planteado y su respectivo análisis.

6. JUSTIFICACION

6.1. JUTIFICACION TECNICA

Hoy en día los sistemas biométricos son ideales en aplicaciones de controles de acceso de algún recurso físico o informático para identificar a una persona, en el caso de biometría de tecleo, cada persona tiene un ritmo único al escribir, esto puede almacenarse en una base de datos y tener patrones de comportamiento que nos pueden decir si un usuario es o no es quién dice ser.

6.2. JUSTIFICACION SOCIAL

Actualmente la red de internet está siendo usada por mayor cantidad de personas de diferentes clases sociales y edades en el mundo, por lo cual la seguridad de acceso se hace cada vez más vulnerable debido a la existencia de métodos y técnicas que logran quebrantar la contraseña del usuario como: La ingeniería social, los keyloggers, troyanos, malwares,

ataques de fuerza bruta, entre otros, con fines mal intencionados desde un simple juego hasta cometer grandes delitos tanto robos monetarios como informáticos.

6.3. JUSTIFICACION ECONOMICA

Se realizaron bastantes investigaciones acerca de la seguridad de acceso pero con un gran problema fundamental, los altos costos que representan implementarlos, es por esta razón que muchos de los sistemas biométricos (como el iris, la cara, etc.), quedan como tal solo investigación, se plantea la identificación de la biometría de tecleo ya que es de fácil manipulación, además será de bajo coste económico, porque no necesitara un hardware adicional y estará disponible para todo usuario.

6.4. JUSTIFICION CIENTIFICA

La biometría de tecleo es una técnica que se basa en el principio de que la acción de escribir en el teclado una palabra o frase (contraseña) muy frecuentemente hace que el acto de escribirla se convierta en algo inconsciente y automático. Esto provoca que ese gesto sea característico nuestro porque influyen tanto procesos mentales que se convierte en una especie de huella dactilar. Los parámetros que se tienen en cuenta a la hora de mesurar la dinámica de tecleo son dos, el tiempo de pulsación de cada tecla y el tiempo entre pulsaciones. En base a estos dos parámetros se pueden crear patrones de comportamiento que nos pueden decir si un usuario es o no es quién dice ser y de esta manera mejorar la seguridad de acceso en aplicaciones de internet.

7. METODOLOGIAS.-

Para demostrar la hipótesis planteada se aplicara el método científico, el cual contempla los siguientes pasos a seguir:

A) Planteamiento del problema

Se observo que la seguridad de acceso en aplicaciones de internet oscila en un 58% el cual no es suficiente para el usuario debido a que a se verifico que cualquier persona obteniendo dicha información (contraseñas) podría acceder a la cuenta de terceros sin mayor problema, utilizando métodos y técnicas que logran romper la seguridad desde un simple juego hasta cometer grandes delitos monetarios como

informáticos. Por lo visto se plantea mejorar la seguridad de acceso en aplicaciones de internet mediante la introducción de un sistema biométrico por tecleo de la contraseña del usuario capaz de identificarlo de mejor manera.

B) Especificación de la hipótesis

Mediante el análisis y estudio de la información recopilada y tomando en cuenta las características del problema se realizo la formulación de la hipótesis.

H: La biometría de tecleo de la contraseña del usuario mejora la seguridad de acceso en aplicaciones de internet.

C) Material y Métodos

En el presente trabajo se tomaran muestras de la forma en que cada usuario teclea, tomando como universo a los estudiantes de la carrera de informática (UMSA), los cuales se encuentran distribuidos en tres grupos, tomándose al azar un grupo como muestra. Posteriormente el usuario introducirá su contraseña en un prototipo prediseñado para el presente trabajo. Luego se realizara comparaciones con el patrón almacenado mediante la función de Scoring y métodos estadísticas.

D) Pruebas y Análisis de Desempeño mediante prototipo

Basado en el análisis de la información se elaborara un prototipo con el cual se realizara análisis y verificación de la hipótesis propuesta.

E) Verificación de los resultados

Se evaluaran los resultados tanto obtenidos como los esperados para de esta manera comprobar que la hipótesis planteada se cumple.

F) Conclusiones

Finalmente se proporcionara las conclusiones a las que se llegaron, el estado de la hipótesis y las recomendaciones pertinentes del tema.

8. ALCANCES Y APORTES

- En la tesis a realizar, se realizara la construcción de un prototipo biométrico de tecleo de la contraseña del usuario que le brinde mayor seguridad de acceso en aplicaciones de internet.
- Este prototipo a crear se podrá añadir fácilmente a cualquier sistema de la red de internet.
- Debido a su bajo coste será aplicable a todo usuario
- Este prototipo no será implementado en su totalidad en los sistemas informáticos solo por falta de difusión de información.

Las respectivas pruebas estarán orientadas solo a las computadoras que tienen integrado un teclado convencional alfanumérico, dentro de esto no se encuentra: teclado touch[12], teclado desplegables[13], teclado de laptop[14].

[12] Teclado con teclas qne no seden a la presión, nn sensor determina las "teclas" qne el nsuario toca.

[13] De goma siliconada, qne snele ser nltra flexible (es enrollable), liviano, delgado y dnrable. Utilización en dispositivos móviles (PDA, teléfonos móviles...).

[14] Teclado de nna compntadora portátil qne pesa entre 8 y 10 libras.

Capítulo II

2. MARCO TEORICO

2.1. MARCO INFORMATICO

2.1.1. SEGURIDAD Y AUTENTICACION

2.1.1.1. INTRODUCCION

Hoy en día mantener un sistema de información funcionando correctamente y sin ningún tipo de problemas se ha convertido en una tarea muy difícil, debido al sin fin de amenazas que rodea a nuestro sistema. Mencionar que la seguridad es considerada una herramienta [Borghello, Fabian, 2001] en cualquier ámbito, no solo informático, en que se la estudia.

La palabra "seguridad" se da a necesidad y con el objetivo de salvaguardar propiedades y personas contra diferentes amenazas ya sean naturales como los incendios, terremotos, inundaciones, otros. Desde comienzos de siglo XVIII [Borghello, Fabian, 2001] la seguridad ha sido tomada en cuenta como una prioridad en los países, un sin fin de descubrimientos que han aportado sin duda a la seguridad.

Figura 1. Amenazas a la seguridad

De aquí que podemos hablar sobre una especialización en tema de seguridad por una lado: se encuentra la seguridad externa, que está principalmente orientada al resguardo de elementos vitales de una organización de los peligros fuera de la misma; y por otra encontramos la seguridad interna, que está orientada a evitar las amenazas que se encuentran dentro de una misma organización.

2.1.1.2. ¿QUÉ ES SEGURIDAD?

La seguridad es una contramedida en relación a la amenaza, se puede definir como aquel sistema que en un cierto grado de relatividad se encuentre libre de amenazas, riesgos y todas aquellas herramientas que nos posibilite el hecho de mantener a salvo toda información vital.

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{RIESGOS} = \frac{\text{AMENAZA X VULNERABILIDAD}}{\text{CONTRAMEDIDA}}$$

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como *falencias (flaws)* o *brechas (breaches)*) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

2.1.1.3. OBJETIVOS DE LA SEGURIDAD

Generalmente, la seguridad consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Para cumplir sus objetivos, la seguridad principalmente se fundamenta en tres principios que debe cumplir todo sistema informático.

Figura 2. Triada de la seguridad

Fuente: extraído de la página web:
http://www.monografias.com/trabajos43/biometria/biometria2.shtml

2.1.1.3.1. CONFIDENCIALIDAD

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática proteger el sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

2.1.1.3.2. INTEGRIDAD

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los diferentes usuarios, computadores y procesos que comparten la misma información.

2.1.1.3.3. DISPONIBILIDAD

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividades adecuadas para los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

2.1.1.4. QUE SE DEBE PROTEGER

Todos los dispositivos que componen el hardware y software: procesador, memoria principal, dispositivos de entrada y de salida, dispositivos de almacenamiento; todo en conjunto conforma un sistema informático, pero de todo este conjunto lo que más nos interesa sin duda son los datos, ya que los mismos conforman el activo en una empresa.

2.1.1.5. DE QUIEN SE DEBE PROTEGER

Una de las amenazas que puede afectar la seguridad de un sistema está conformada por personas, que pueden ser de uno o un grupo de personas, podemos denominarlas personas atacante(s) o intruso (s).[15]

El atacante o intruso es aquel usuario no autorizado, que accede o intenta acceder al sistema de información. Se puede identificar 4 grupos principales de intrusos en la figura 4.

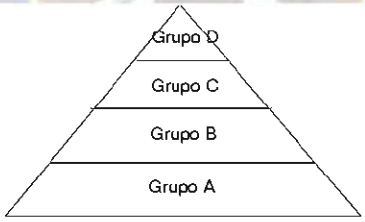


Figura 3. Clasificación de intrusos

Fuente: [Borghello, Fabian, 2001]

[15] Que altera en un ambiente que no le es propio. Que ocupa un puesto sin tener derecho a él.

1. Clase A: lo conforman el grupo de personas de alrededor del 80%, los cuales se dedican a descargar programas nocivos y los prueban.

2. Clase B: lo conforman personas con un conocimiento básico de programación, saben compilar un programa, pueden detectar el tipo de sistema operativo que usa una persona, este grupo de personas de alrededor del 12%, ya son un poco más peligros que la anterior clase.

3. Clase C: lo conforman personas que tiene conocimientos un poco más avanzados sobre programación que los anteriores, y tiene trazados metas ya definidas, lo conforman personas de alrededor del 5%.

4. Clase D: Es el 3% de personas restantes que tiene un nivel muy alto sobre sistemas y programación de los mismos, cuando ingresan a diferentes sistemas buscan lo que necesitan. [Jerez L. C. A, Seguridad, 2002]

2.1.2. SEGURIDAD BIOMETRICA

2.1.2.1. OBJETIVO DE LA BIOMETRIA EN LA SEGURIDAD

El principal objetivo de la Biometría es "identificar" y permitir reconocer personas en una determinada aplicación, ya sea para control de acceso, control de asistencia, control de algún equipo electrónico, etc.

Para determinar la identidad de un individuo, primero se hace un reconocimiento y luego la verificación del mismo

2.1.2.2. ¿QUE ES LA SEGURIDAD BIOMETRICA?

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, que puede ser el reconocimiento del iris, la identificación del tono de voz o la utilización de la huella dactilar, algo similar a la firma digital pero en este caso el contraseña (password) es una característica física única e irrepetible como las mencionadas anteriormente.

Este sistema de seguridad se compone de dos piezas fundamentales: el hardware de interface y el software decodificador o biométrico.

2.1.3. SEGURIDAD DE ACCESO

2.1.3.1. SEGURIDAD DE ACCESO EN INTERNET

Las aplicaciones de internet son un conjunto de programas diseñados para la realización de una tarea concreta, como una aplicación comercial[16], contable[17], wikis[18], weblogs[19], emails[20], tiendas en línea[21], etc.

Actualmente las aplicaciones de internet son de lo más utilizados en la red de internet debido a la gran versatilidad y facilidad de consulta por parte de los usuarios cada día se incrementa en la red más grande de todo el mundo que es internet.

En aspecto muy importante de una aplicación de internet es el control de acceso de los usuarios a zonas restringidas de la aplicación.

2.1.3.2. CONTROL DE ACCESO

El control de acceso constituye una poderosa herramienta para proteger la entrada a la red de internet completo o sólo a ciertos directorios concretos e incluso a ficheros o programas individuales. Este control consta generalmente de dos pasos:

---

[16] Se denomina comercio a la actividad socioeconómica consistente en el intercambio de algnnos materiales qne sean libres en el mercado de compra y venta de bienes y servicios, sea para sn nso, para su venta o sn transformación.

[17] clasifica y registra todas las transacciones financieras de nn negocio o empresa para proporcionar informes qne sirven de base para la toma de decisiones sobre la actividad.

[18] páginas web cnyos contenidos pneden ser editados por mńltiples nsnarios a través de cnalqnier navegador. Dichas páginas, por lo tanto, se desarrollan a partir de la colaboración de los internantas, qnienes pneden agregar, modificar o eliminar información.

[19] También llamado bitácora. Es nn sitio web personal donde se escriben periódicamente, como nn diario on line, sobre distintos temas qne le interesan al propietario. Cada escrito está ordenado cronológicamente y en general posee enlaces a otras páginas para ampliar el tema qne se habla.

[20] Electronic mail o Correo electrónico, o abreviado e-mail. El e-mail es nn servicio mny ntilizado en internet, qne permite el intercambio de mensajes entre nsnarios. Donde los nsuarios no deben estar online de forma simnltánea.

[21] También conocida como tienda *online*, tienda virtnal o tienda electrónica, se refiere a nn comercio convencional qne nsa como medio principal para realizar sns transacciones nn sitio web de Internet.

- En primer lugar, la autenticación[22], que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.

- En segundo lugar, procede la cesión de derechos, es decir, la autorización[23], que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc. [Ormachea Jorge, Seguridad Biométrica, 2008]

2.1.4. IDENTIFICACION Y AUTENTICACION DE USUARIOS

En la actualidad muchas de los sistemas de información aplicados al internet utilizan un mecanismo de control de acceso a diferentes recursos que ofrecen, este tipo de control se denomina identificación y autentificación.

La identificación es el mecanismo mediante el cual, a través de un ID de entrada, el sistema reconoce a un usuario como usuario legítimo. La autentificación es el mecanismo mediante el cual, a través de una contraseña, el sistema verifica la identidad del usuario.

Cuando el sistema identifica y autentifica a un usuario, se revela también cierta información sobre el acceso de dicho usuario a la información, es decir, sus atributos de acceso.

Los mecanismos de identificación y autentificación evitan que los usuarios no autorizados entren en el sistema y aseguran que los usuarios entran sólo en las áreas para las que están autorizados.

Los sistemas de autenticación se dividen en tres grandes grupos: sistemas basados en algo conocido (una contraseña), sistemas basados en algo poseído (una tarjeta inteligente) y sistemas biométricos (basados en características del individuo, como por ejemplo el trazo de la firma o una huella dactilar).

---

[22] Es el acto de establecimiento o confirmación de algo (o algnien) como auténtico, es decir qne reclama hecho por, o sobre la cosa son verdadero.

[23] Autorización es la acción y efecto de antorizar (reconocer la facnltad o el derecho de nna persona para hacer algo). En el campo del derecho, la autorización es nn acto realizado por nna antoridad, a través del cnal se permite a nn sujeto nna cierta actnación qne, en otro caso, estaría prohibida.

2.1.4.1. SISTEMAS BASADOS EN ALGO CONOCIDO

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento que a priori sólo ese usuario puede superar. El mecanismo más común dentro de los de este tipo es la contraseña, que hoy constituye el más común de los sistemas de autenticación debida principalmente al bajo costo que implica, pero desgraciadamente, también es el más vulnerable.

Los programas que ejecutan la Identificación y Autentificación basados en algo conocido en son:

- Nombre de Usuario (Login)
- Contraseña (Password)

Nombre de Usuario (Login)

El programa Login identifica y autentifica a los usuarios. Pide un nombre de entrada y una contraseña, se encarga de validar éstas y otras entradas introducidas en el indicativo de entrada. Sin embargo, el sistema no reconoce a los usuarios por este nombre de usuario, sino que cada uno tiene asociado un número (el UID, User IDentification) que corresponde con su login. Podremos tener varios usuarios con el mismo UID pero distinto login, y se hace así para poder tener a distintos usuarios con el mismo nivel de privilegios.

Contraseña (Password)

El password es la parte vital de la seguridad de cuentas en los sistemas. Si un cracker[24] es capaz de adivinar el password de un usuario podrá entrar en el sistema con todos los permisos de ese usuario, y una vez allí el sistema queda bajo su control. Si el password obtenido por éste es el de super-usuario (root)[25] el problema es serio del todo.

[24] El térmiuo cracker (del iuglés crack, romper) se utiliza para referirse a las persouas que rompeu algúu sistema de seguridad. Los crackers puedeu estar motivados por uua multitud de razoues, iucluyeudo fiues de lucro, protesta, o por el desafío.

[25] Cuenta de admiuistrador. El usuario root puede hacer muchas cosas que uu usuario comúu uo, tales como cambiar el dueño de archivos y enlazar a puertos de uumeracióu pequeña.

2.1.4.2. SISTEMAS BASADOS EN ALGO POSEÍDO

En este tipo de sistemas, lo habitual es usar tarjetas inteligentes, cuya complejidad es muy alta y cuyo rango de aplicación es amplísimo: desde una sencilla tarjeta monedera hasta el acceso a instalaciones militares.

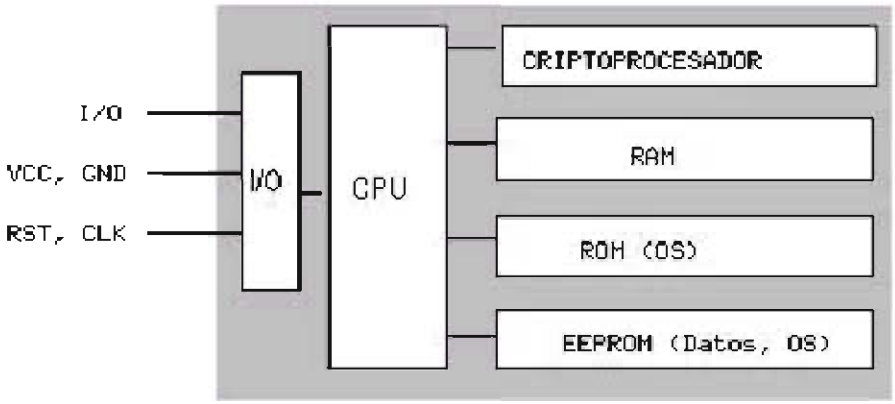


Figura 4. Estructura Genérica de un Smartcard

Una tarjeta inteligente es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, con un microprocesador[26] miniaturizado incorporado, que ofrece funciones para un almacenamiento seguro de información. Poseen un chip[27] empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas[28], y además puede detectar activamente intentos no válidos de acceso a la información almacenada.

[26] El microprocesador o simplemente procesador, es el circnito integrado central y más complejo de nn sistema informático; a modo de ilnstración, se le snele asociar por analogía como el «cerebro» de nn compntador.

[27] Circnito integrado en nn soporte de silicio, formado por transistores y otros elementos electrónicos miniatnrizados.

[28] Es la técnica, bien sea aplicada al arte o la ciencia, qne altera las representaciones lingñísticas de nn mensaje.

2.1.4.3. SISTEMAS DE AUTENTICACIÓN BIOMÉTRICA

Este tipo de métodos también se los conoce como técnicas biométricas de autenticación ya que se basan o hacen uso de las características o atributos tanto fisiológicos como de comportamiento, propios de cada individuo que lo hacen único.

Es mucho más compleja y lleva consigo un alto costo en su implementación ya que algunos de ellos necesitan de algún equipo especial para su tratamiento.

Este método de autenticación surge debido a los problemas fundamentales y necesarios para poder autenticar de una forma segura la identidad de las personas [Huidobro, 2006]. Durante mucho tiempo no han tenido una aceptación entre los usuarios lo cual sería su principal desventaja, pero de manera general proporcionan un mejor nivel de seguridad con respecto a los anteriores métodos, ya que últimamente existe una combinación de métodos de autenticación de usuarios.

El rechazo de los usuarios hacia este tipo de sistema de autenticación se debe principalmente a las principales preocupaciones socio-culturales, algunas erróneas que se pueden englobar en tres grupos distintivos: privacidad de la información, que se refiere al miedo de ser revelado información vital para la persona; propiedad física, en la cual se ha comprobado que sistemas como de reconocimiento de iris pueden detectar enfermedades en los usuarios; y por último las cuestiones religiosas [Woodward, 2001].

2.1.2. BIOMETRIA

2.1.2.1. ¿QUE ES LA BIOMETRIA INFORMATICA?

Debido a que la biometría tiene una gran variedad de aplicaciones, es muy difícil establecer una definición completa, que abarque a todas ellas.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es "una característica única física medible y como tal, diferenciable". [Ruiz, 2002]

El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características físicas o de comportamiento de las personas con el objeto de establecer una identidad. Para diferencia estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autentificación biométrica.

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

La biometría física se basa en medidas y datos derivados de la medición directa de una parte del ser humano. La huella dactilar, el iris, la retina y la cara son las características físicas más utilizadas en biometría.

Las características del comportamiento se basan en acciones realizadas por una persona. En este sentido, la biometría del comportamiento se basa en medidas y datos derivados de una acción, e indirectamente de las características físicas que lo han generado. El reconocimiento de la voz, del tono de voz y de la firma son las medidas biométricas de comportamiento más utilizadas.

Es importante remarcar que la distinción entre físico/ comportamental es muy débil. La biometría del comportamiento se basa en parte en características físicas, como por ejemplo la forma de pronunciar de las vocales.

La biometría basada en características físicas también está asistida por el comportamiento, como la manera en que la persona coloca su dedo o mira a la cámara.

Sin embargo, la distinción entre biometría física y comportamental es útil para entender cómo funciona la biometría y cómo puede aplicarse al mundo real. [Spaltro JL, Biometría, 2007]

2.1.2.2. REFERENCIAS HISTÓRICAS DE LA BIOMETRÍA

No es verdad que la biometría sea una técnica de identificación futurista, 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 almacenadas 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 el siglo XIV, los mercaderes chinos estampaban con tinta sobre papel las huellas de las palmas de las manos y las plantas de los pies de los bebés para distinguirlos unos de otros. Este primer registro dio la entrada, cinco siglos más tarde, a los sistemas de identificación de la policía, la huella dactilar y, hoy en día la tecnología ha hecho posible el poder

registrar y el almacenar la huella dactilar, el iris, la forma de la mano, la voz, el rostro o la firma.

En el siglo IXX hubo un pico de interés por parte de investigadores en criminología, cuando intentaron relacionar características físicas con tendencias criminales. Esto resultó en una variedad de equipos de medición y gran cantidad de datos recogidos. Los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía pegar y el desarrollo paralelo de la identificación de huellas digitales se convirtió en la metodología internacional para identificación utilizada por las fuerzas policiales de todo el mundo.

En 1823 el profesor John Evangelist propuso el primer sistema de clasificación de huellas dactilares. Más tarde, en 1856 Sir William Herschel utilizó por primera vez la impresión de las huellas de los dedos corazón e índice de la mano derecha como prueba identificativa añadida a la firma en todos sus contratos. Desde aquí hasta la fecha han sido múltiples los avances en este campo, en el que, gracias a la introducción de los procesadores, el método de búsqueda ha sido automatizado, permitiendo identificaciones prácticamente instantáneas.

Durante la segunda mitad del siglo XIX el francés Alphonse Bertillon funcionario de la Prefectura de Policía de París logró desarrollar, con las limitaciones de la época, una base de datos con las características fisiológicas de 1.500 procesados por delitos violentos en esa localidad.

Aunque Bertillon menospreciaba la utilidad de los rastros dactilares (para él eran simples "marcas distintivas"), su método se impuso en la Francia decimonónica, al punto que obtuvo el cargo de jefe nacional de identificación. El "bertillonage" incluía datos tales como la longitud de la mano izquierda, el largo y el ancho del cráneo, la longitud de la oreja izquierda y otros. Sirvió, por ejemplo, para determinar la verdadera identidad de antisociales reincidentes.

A casi cien años de la muerte de Bertillon, los métodos más aceptados de identificación se basan en la colección de rastros dactilares y, últimamente, de muestras de ADN (ácido

desoxirribonucleico), cuyos grados de confiabilidad resultan casi infalibles. El problema es que todavía no han logrado el desarrollo de una aplicación tecnológica que permita la detección in situ de sujetos buscados por delitos violentos o actos terroristas.

En el siglo XIX se comenzaron las investigaciones científicas acerca de la biométrica con el fin de buscar un sistema de identificación de personas con fines judiciales. Con estas investigaciones se producen importantes avances y se comienzan a utilizar los rasgos morfológicos únicos en cada persona para la identificación.

Ya en el siglo XX, la mayoría de los países del mundo utilizan las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial o la voz.

En 1968 se implementó el primer sistema biométrico: En Wall Street se usaba la huella digital para abrir una bóveda donde se guardaban los certificados de la bolsa. Ese sistema costó aproximadamente $20.000, ese sistema hoy en día debe costar menos de $500.

En la década de los setenta, como un requerimiento de seguridad, algunas empresas comenzaron a desarrollar tecnologías que permitieran identificar a las personas por un rasgo corporal único como las huellas dactilares y patrones vasculares de la retina del ojo humano.

La última década ha visto a la industria de la biometría madurar de un puñado de fábricas especialistas tratando de sobrevivir, a una industria global que comienza a tener un crecimiento significativo y está destinada a tener un rápido crecimiento al momento que aplicaciones en gran escala comienzan a aparecer en el mercado.

Actualmente la Biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación humana. [John D. Woodw, Higgins, Biometrics, 2003).]

2.1.2.3. ¿PARA QUÉ LA BIOMETRÍA?

En las organizaciones de hoy, la identificación y verificación de las personas que acceden a la información crítica de sus sistemas constituyen la base fundamental de su seguridad, y a lo largo de las últimas décadas se han utilizado diversos métodos para lograrlo de la manera más eficiente posible. A nivel empresarial es obvio la importancia de requerir una identidad a la hora de emprender transacciones de una compañía a otra.

Sin embargo, la tecnología biométrica debe todavía afrontar algunos desafíos técnicos considerables. El hardware es costoso, los diferentes sistemas son incompatibles entre sí y la tecnología se encuentra en pleno proceso de maduración.

Conforme las computadoras se vuelven parte del tejido de la vida cotidiana y más transacciones desde firmas de contratos a compras se realizan digitalmente, las firmas especializadas en biometría piensan que sus productos pronto serán ubicuos e indispensables.

Los sistemas modernos de biometría por computadora se emplean para responder dos preguntas básicas:

¿Quién es usted? y ¿quién dice ser?

Estas dos preguntas ejemplifican con claridad la diferencia entre la identificación y la verificación, lo que motiva la división de los equipos biomédicos en dos grandes grupos. Los de identificación trabajan con las características de la persona y la comparan con la plantilla biométrica almacenadas en una base de datos (comparación uno a muchos, 1:N), y así establecer la identidad del individuo. La verificación es comparar las características biométricas de la persona contra una captura hecha anteriormente bajo el supuesto de que los datos de esa persona están almacenados en la unidad (comparación uno a uno, 1:1).

2.1.2.4. FUNCIONAMIENTO Y DESEMPEÑO

En los sistemas biométricos el usuario tiene la comodidad de no tener que portar con él un token[29] o crear y recordar una contraseña, únicamente la primera vez que use el sistema tendrá que presentar su "credencial" biométrica para que el sistema cree y registre su perfil, el cual será comparado en cada intento de autenticación contra la "credencial".

Cuando una persona hace uso de un sistema biométrico, se obtiene un rasgo fisiológico o conductual asociado a tal usuario. Dicha información es procesada por un algoritmo numérico para obtener una representación digital de la característica biométrica. El proceso de convertir el rasgo biométrico en una plantilla digital es realizado cada vez que el usuario trata de autenticarse en el sistema.

En la figura 4 se presenta un esquema básico del funcionamiento de un sistema biométrico.

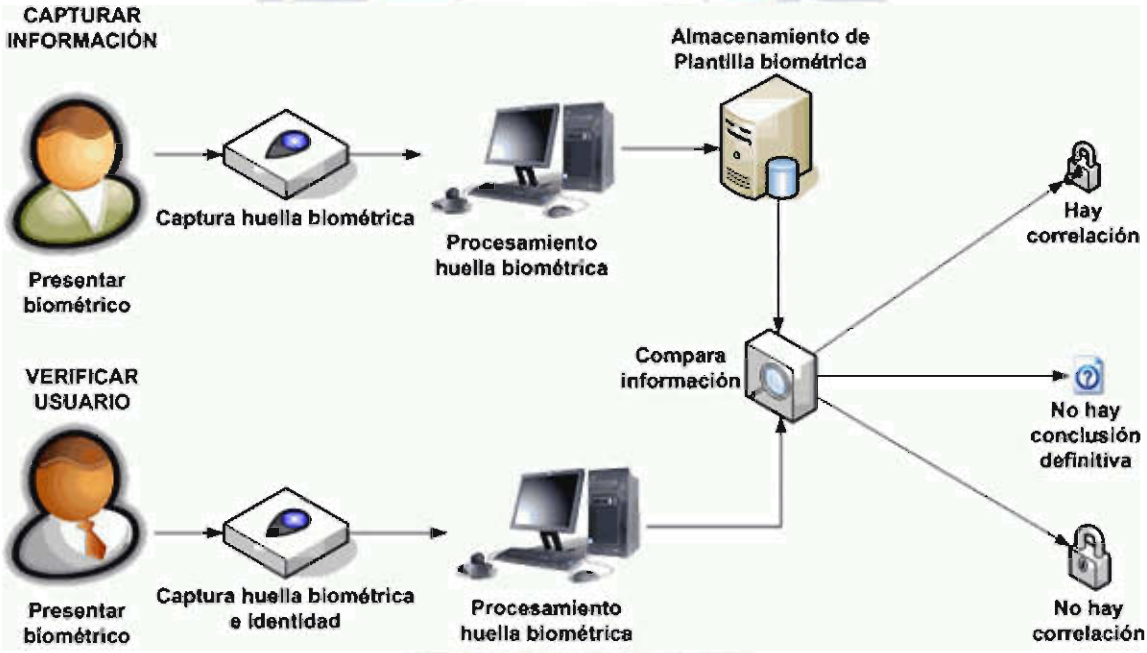


Figura 5. Proceso de registro y verificación en un sistema biométrico

Fuente: extraído de la página web:

http://www.monografias.com/trabajos43/biometria/biometria2.shtml

[29] Es nna red en anillo del tipo LAN qne tiene nodos cableados también en anillo. Cada nodo pasa de manera constante nn mensaje de control token (señal) al siguiente, de manera qne cnalqnier nodo qne emita nna señal pnede enviar nn mensaje.

Al igual que cualquier sistema de información, debemos medir el desempeño de los sistemas biométricos, para esto usamos medidas de tasas de error, las más comunes son la TFA o FAR (del inglés False Accept Rate – tasa de falsa aceptación) y la TFR o FRR (del inglés False Reject Rate – tasa de falso rechazo) [Anil , Arun , Salil, 2004].

La TFA se refiere al error que ocurre cuando el sistema biométrico identifica de una manera incorrecta los rasgos de la muestra biométrica como iguales con respecto a otros rasgos de una muestra almacenada, es decir, concede acceso a un usuario no legítimo. Este error es conocido en Estadística como falsos positivo.

Se considera que la TFR es más elevada que la TFA, ya que al producirse un error de este tipo se rompe el esquema de seguridad. En la figura 6 se muestra una gráfica de la TFR contra la TFA, de la cual se puede obtener una nueva medida denominada TEC o EER (del inglés Equal Error Rate – tasa de error de cruce). Se dice que mientras más bajo sea el TEC, más exacto será el sistema [Ashbourn, 2000].

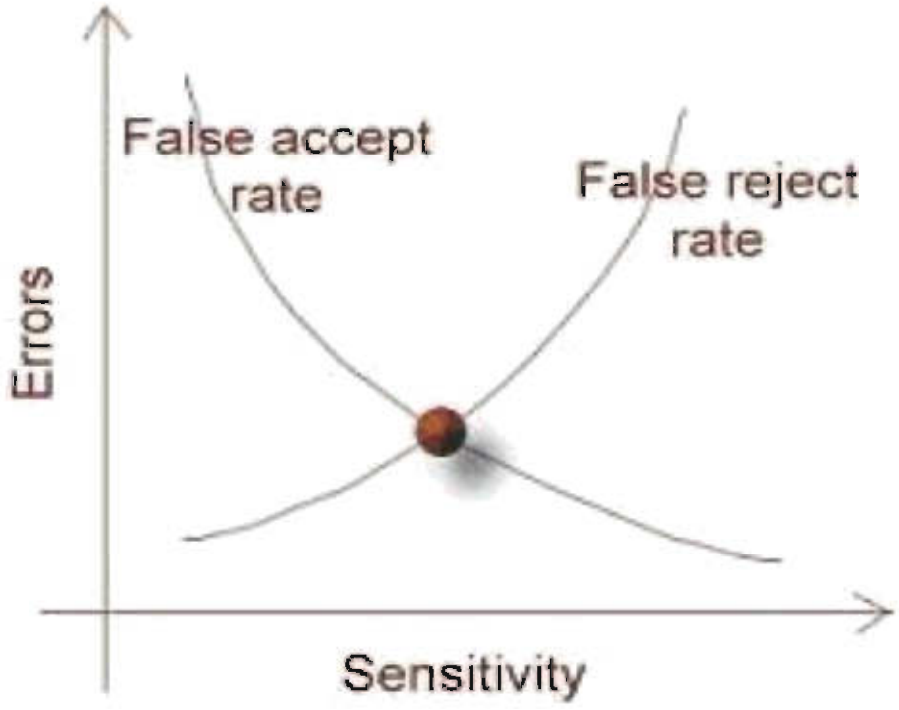


Figura 6. Medida de desempeño de un sistema biométrico

Fuente: extraído de la página web: http://es.wikipedia.org/wiki/Biometr%C3%ADa

2.1.2.4. TIPOS DE BIOMETRIA

2.1.2.4.1. BIOMETRIA ESTATICA

La biometría estática consiste en la medición de las características corporales de las personas. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, retina, iris, forma de la cara.

2.1.2.4.1.1. HUELLA DIGITAL

Las huellas digitales son el método de identificación de personas más antiguo. Las huellas digitales están formadas por patrones de valles y crestas en las yemas de los dedos, los cuales se forman durante los primeros siete meses de vida del feto. Existen dos técnicas para la identificación de huellas dactilares, en la primera se localizan las terminaciones de crestas, bifurcaciones, puntos y cruces (todos estos elementos se denominan minucias, podemos ver un ejemplo en la Figura 7), y partiendo de su geometría, orientación y relación, se compara contra las mismas de la plantilla. La segunda técnica compara las zonas que rodean a las minucias para encontrar diferencias de deformaciones [Muñoz, 2007].

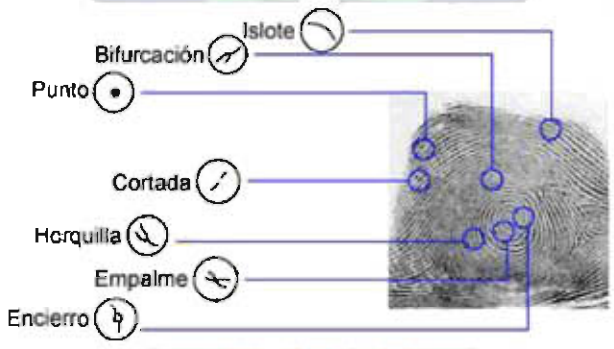


Figura 7. Minucias en una huella digital

Fuente: extraído de la página web: www.hbh.cl/Biometria/tabid/57/Default.aspx

2.1.2.4.1.2. GEOMETRIA DE LA MANO

Como su nombre lo indica, los biométricos basados en la geometría de la mano la forma de la mano por medio de una cámara infrarroja[30] o visual. Ofrecen un buen balance entre la velocidad del análisis de las plantillas y son ideales para uso masivo, como control de asistencia y acceso de entradas. Su uso se ha incrementado en los últimos años. [James, Biometric Systems Technology, 2005).]

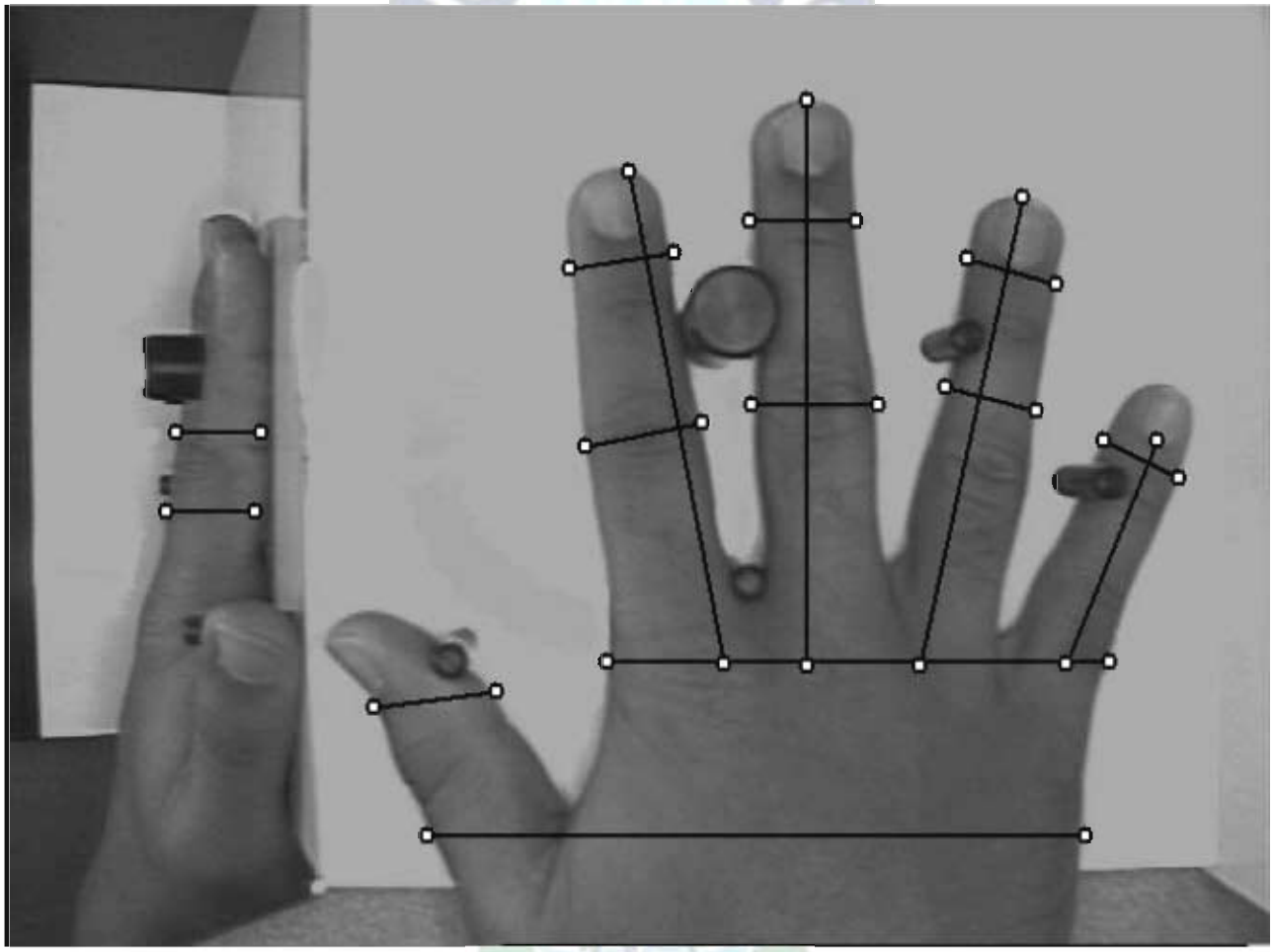


Figura 8. Geometría de la mano con ciertos parámetros extraídos

Fuente: extraído de la página web: www.hbh.cl/Biometria/tabid/57/Default.aspx

[30] Dispositivo capaz de formar imágenes visibles a partir de las emisiones en el infrarrojo medio del espectro electromagnético emitida de los cuerpos detectados y que la transforma en imágenes luminosas para ser visualizada por el ojo humano.

2.1.2.4.1.3. RETINA

Los lectores biométricos de retina analizan los capilares que están situados en el fondo del globo ocular. El usuario debe acercar el ojo al lector y fijar su mirada en un punto. Una luz baja intensidad examina los patrones de los capilares de la retina. Este procedimiento es intimidante para algunos y hace de los lectores de retina los biométricos más impopulares, el usuario siente que su integridad física puede peligrar porque percibe un objeto extraño en su cuerpo, en ese caso la luz (característica no deseada de los lectores biométricos es conocida en ingles como intrusive). Para que el lector pueda realizar su trabajo, el usuario no debe tener lentes puestos. [Allmysoft. 2007]

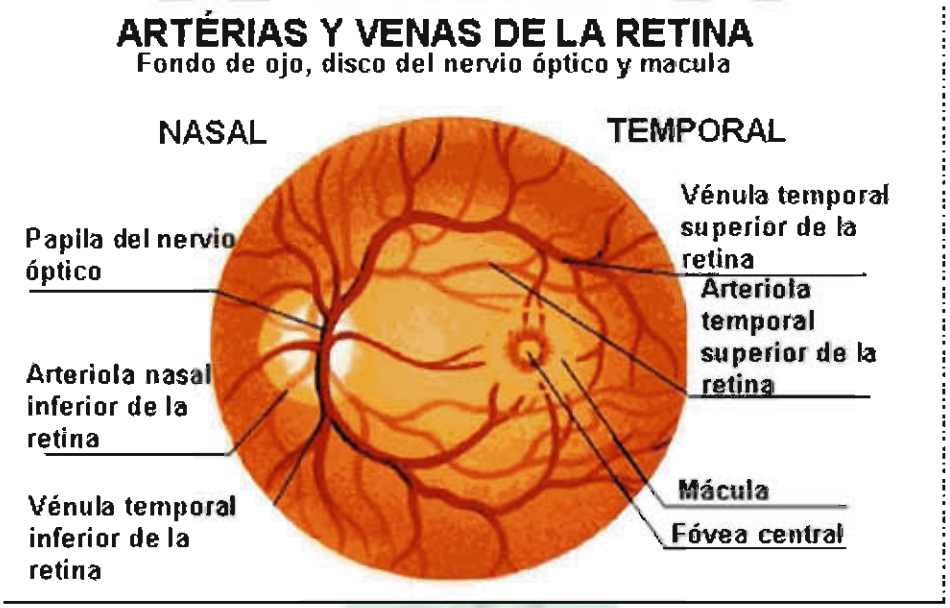


Figura 9. Imagen de vasculatura retinal

Fuente: extraído de la página web:

2.1.2.4.1.4. IRIS

Los lectores de iris analizan las características del tejido coloreado que se encuentra alrededor de la pupila. Estos biométricos son los menos incómodos de usar de los lectores de ojo, porque no se realiza un contacto cercano con el lector. Además es una de las tecnologías biométricas más exactas y el usuario puede usar los lentes al momento de la

lectura. La facilidad de uso y la integración con otros sistemas no han sido puntos fuertes de los lectores de iris. [Granger S. 2001]

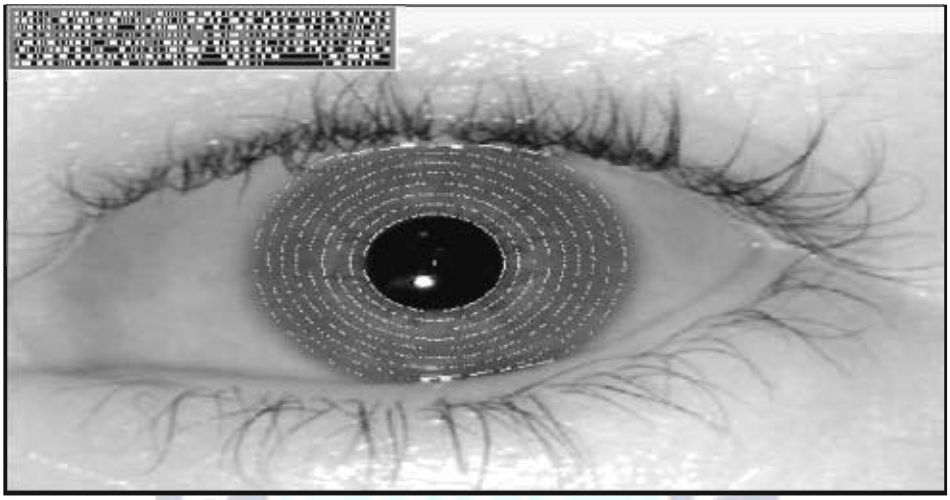


Figura 10. Iris humano con la extracción de su iriscode

2.1.2.4.1.5. RECONOCIMIENTO DE LA CARA

Reconocer a personas conocidas por nosotros de entre un grupo de personas en la calle es la característica biométrica más usada. Las principales aproximaciones para el reconocimiento facial son dos, la primera se basa en la localización y forma de rasgos de la cara, tales como cejas, ojos, nariz, labios, barbilla, y su relación espacial; la segunda aproximación consiste en un análisis global de la imagen de la cara representando una cara como un combinación ponderada de un número de rostros canónicos [Matthew , Alex, 1991].

2.1.2.4.2. BIOMETRIA DINAMICA

En el área de la biometría dinámica, encontramos sistemas orientados al reconocimiento o autenticación del usuario basados en la utilización de factores no estáticos, sino dinámicos. Factores asociados al comportamiento de las personas, a cómo se mueven, a cómo articulan sonidos y a cómo interactúan con el sistema que lo está intentando reconocer. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz (o manera de hablar), firma manuscrita (o análisis de escritura), dinámica del tecleo. [Anil K. J, 2004]

2.1.2.4.2.1. RECONOCIMIENTO DE VOZ

Los biométricos de reconocimiento de voz están basados en la verificación del patrón de voz. Su implementación puede ser económica si es realizada en computadoras, ya que la mayoría trae el hardware necesario: micrófonos y bocinas. Sin embargo, factores ambientales, como el ruido, pueden afectar la comunicación. Además, el patrón de reconocimiento de voz es el que más espacio ocupa de todas las tecnologías biométricas, pudiendo llegar hasta 1MB. Por estas razones, los biométricos de voz son percibidos por los usuarios como dispositivos poco amigables. [Araujo C, 2004]

2.1.2.4.2.2. LECTURA DE FIRMA

La técnica de verificación de firma analiza la manera que el usuario realiza su firma personal. Factores diversos, como la rapidez y presión, son cuantificados, así como la forma de firma. La verificación tiene uno de los niveles más bajos de exactitud entre los lectores biométricos. Sin embargo, su familiaridad con los actuales procesos de verificación manual la hace una de las técnicas más fáciles de introducir al usuario. [Araujo C, 2004]

2.1.2.4.2.3. BIOMETRIA DE TECLEO

Este tipo de biometría se centra en las técnicas necesarias para identificar en qué medida existe una cierta regularidad en el modo de teclear de un usuario de un sistema informático. El proceso de tecleo es realmente complejo y trasciende el aspecto meramente físico en tanto que es una capacidad emergente que surge de la propia dinámica cerebral en su origen. Desde el cerebro generamos los estímulos necesarios que se transmiten por el sistema nervioso periférico hasta nuestros músculos que efectúan complejas contracciones y distensiones para presionar un centenar de teclas de un ordenador, plasmando la información verbal que el cerebro está procesando en un momento determinado. Además el hecho de no necesitar un hardware adicional para el muestreo de los tecleos hace que sea un sistema ideal para su aplicación sobre Internet, ya que todos los ordenadores comparten la capacidad de admitir el tecleo de los usuarios. Por lo tanto la biometría de tecleo es una técnica que se basa en el principio de que la acción de escribir en el teclado una palabra o frase muy frecuentemente hace que el acto de escribirla se convierta en algo inconsciente y

automático. Esto provoca que ese gesto sea característico nuestro porque influyen tanto procesos mentales que se convierte en una especie de huella dactilar. Los parámetros que se tienen en cuenta a la hora de mesurar la biometría de tecleo son dos, el tiempo de pulsación de cada tecla y el tiempo entre pulsaciones. En base a estos dos parámetros se pueden crear patrones de comportamiento que nos pueden decir si un usuario es o no es quién dice ser.

El punto central para el cálculo de patrones en estos sistemas consiste en poder medir en el tiempo con la mayor precisión posible la ocurrencia de estos eventos. Una vez que se tienen registrados todos los eventos ocurridos en la entrada de texto por parte del usuario, el resto consiste en aplicar un algoritmo para la obtención de una medida que represente a la muestra. Existen varias aproximaciones para procesar los datos de tiempo: métodos estadísticos, lógica difusa, redes neuronales [Aguilar, 2006]. Todas estas aproximaciones han sido probadas en implementaciones para teclados convencionales dando buenos resultados. [Monrose F,2007]

2.1.3. EL TECLADO

Se trata de un dispositivo que integra una gran cantidad de teclas, semejantes a las de una máquina de escribir mecánica. También tiene una serie de botones extras que realizan otras funciones específicas. A través del tiempo, este dispositivo es de los que menos modificaciones han sufrido, ya que por excelencia es el periférico de entrada más común de las computadoras y de los más indispensables.

Los teclados y computadoras de escritorio, reemplazaron del mercado el uso de las máquinas de escribir mecánicas y máquinas de escribir eléctricas

Figura 11. Teclado Convencional Alfanumérico

2.1.3.1. DISPOSICION FISICA DE LAS TECLAS

La disposición de un teclado actual es la siguiente:

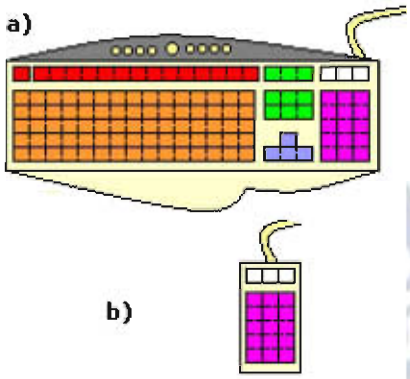


Figura 12. Disposición de de teclas de un teclado convencional y en un teclado sólo numérico

a) Teclado convencional

1.- Teclas de función (rojo): tienen diferentes aplicaciones dependiendo cada programa, eje F1 comúnmente es para activar la ayuda.

2.- Teclado mecanográfico (naranja): se trata de las mismas teclas que integra una máqui escribir mecánica.

3.- Teclado de dirección (azul): se emplean para realizar movimientos del cursor en pantall

4.- Teclas de comando (verde): se emplean para introducir u obtener ciertos datos, así ejecutar órdenes especiales.

5.- Teclas numéricas (morado): llevan a cabo operaciones con números, incluyendo sím matemáticos. Se debe de activar con el botón "Bloq Num".

b) Teclado sólo numérico: una variante de teclados muy utilizados, es el teclado numérico, que solo cuenta con el bloque de teclas que contienen números y símbolos; este se utiliza para poder solamente insertar números en equipos que requieren protección contra los datos que el usuario quisiera introducir.

En un teclado no vienen indicadas las secciones por colores, solo se utilizaron en este esquema para representarlas de manera más sencilla. [Allmysoft, 2007]

2.1.3.2. TIPOS DE TECLADO

Se clasifican de acuerdo a dos criterios principales, el primero de ellos se refiere a la estructura del teclado y el segundo al tipo de pulsador utilizado. Existe la posibilidad de combinar las dos estructuras con los distintos tipos de pulsador. [John D. Woodward, 2011]

2.1.3.2.1. DE ACUERDO A SU ESTRUCTURA

TECLADOS TIPO SANDWICH

La denominación de un teclado plano como de tipo sándwich, implica que el mismo tiene un espesor uniforme, que se puede encontrar entre 0,6 y 1.4 milímetros como máximo. Todos los elementos del teclado están unidos entre sí formando un sándwich con un espesor y peso mínimos.

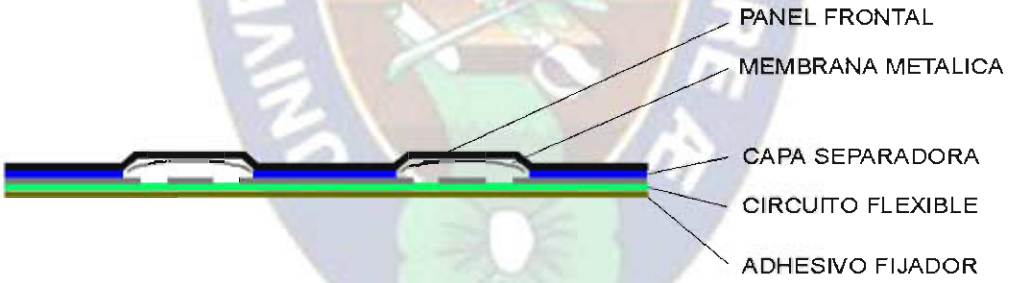


Figura 13. Teclado tipo sándwich

TECLADOS DE PERFIL BAJO

Los teclados de perfil bajo suponen uno de los sistemas de introducción de datos más completos que existen, ya que debido a su estructura, en el mismo sistema se puede integrar teclas de corto recorrido o pulsadores piezoeléctricos, leds, visualizadores, y los componentes electrónicos necesarios para la conexión al siguiente sistema de adquisición de datos. El producto final es un sistema compacto e integral, que posee todas las ventajas que tienen los teclados tipo sándwich, en cuanto a diseño y versatilidad. Además en muchos

casos la estructura es desmontable, lo que permitiría sustituir teclas u otros componentes en el caso de sufrir algún daño.

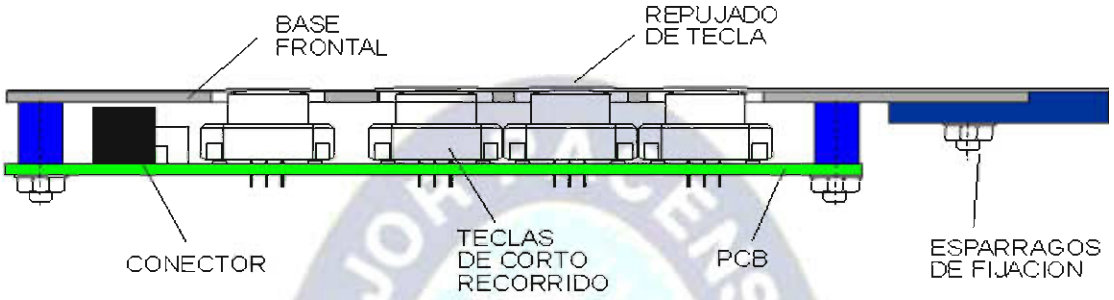


Figura 14. Teclado de Perfil Bajo

2.1.3.2.2. DE ACUERDO AL TIPO DE PULSADOR

TECLADOS DE MEMBRANA

En estos teclados las teclas están compuestas por unas membranas metálicas que actúan como pulsadores. Al presionar sobre estas piezas se produce una sensación táctil, que confirma el pulsado de la tecla. En este tipo de teclado se combina un sistema de pulsador sencillo, efectivo, y que permite diseños con espesores mínimos.

Las características propias de las membranas metálicas son las siguientes:

- Fabricadas en acero inoxidable (con contactos dorados de forma opcional).
- Diferentes formas y dimensiones para adaptarse a las particularidades de cada diseño, permitiendo crear teclas cuadradas, circulares o rectangulares.
- Diferentes fuerzas de actuación en función del ámbito de funcionamiento.

Figura 15. Teclado de Membrana

TECLADOS SENSITIVOS

En estos teclados no existen mecanismos pulsadores sobre los que ejercer una presión. Las teclas pasan a la posición de cierre simplemente al apoyar el dedo sobre ellas, ejerciendo una presión mínima. Este tipo de teclado reúne las siguientes ventajas indiscutibles:

- Alta sensibilidad de las teclas.
- Fácil y rápida introducción de datos.
- Teclados ultrafinos, consiguiéndose espesores desde tan solo 0,6 mm.

Figura 16. Teclado Sensitivo

TECLADOS PIEZOELECTRICOS

Los teclados piezoeléctricos están construidos con pulsadores cuyo funcionamiento se basa en el efecto piezoeléctrico. Si se aplica una fuerza a un cuerpo piezoeléctrico, se inducen cargas superficiales por el desplazamiento dieléctrico, por lo tanto se crea un campo eléctrico. Si el cuerpo piezoeléctrico tiene electrodos este campo puede ser transformado en una tensión eléctrica. En un interruptor basado en piezoeléctricos la tensión eléctrica generada es amplificada y acondicionada para producir un impulso eléctrico corto, el cual

se usa para producir el cierre de un contacto momentáneo de entre 10 y 1000 ms de duración, dependiendo de la fuerza y velocidad de pulsación.

Los teclados construidos con pulsadores piezoeléctricos son especialmente adecuados para exteriores, equipos de seguridad de baja supervisión, aplicaciones industriales y médicas.

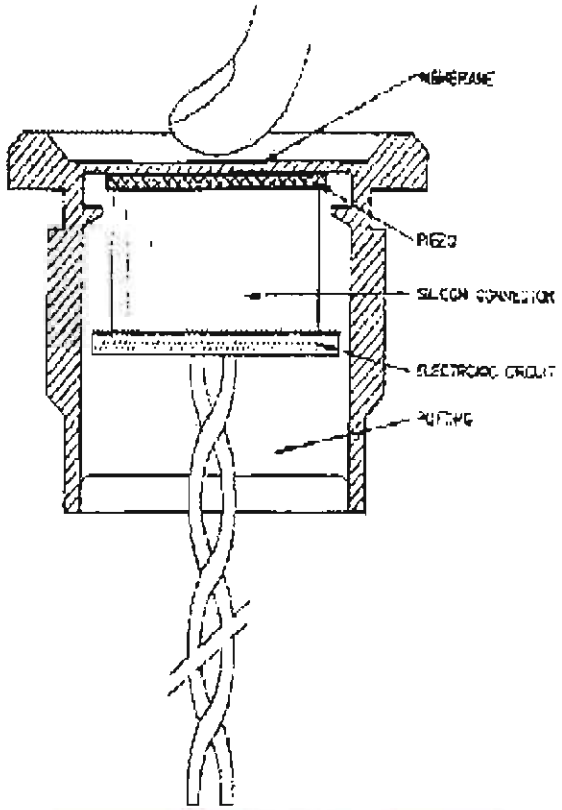


Figura 17. Teclado Piezoeléctrico

2.1.3.2.3. DE ACUERDO A LA APLICACION

TECLADOS ESTANDAR TIPO PC

Se denominan teclados estándar tipo PC, con unas dimensiones y disposición de teclas predefinidas. Estos teclados son conectables a sistemas tipo PC, ya que incorporan un codificador compatible. Entre estos tipo el teclado QWERTY es la distribución de teclado

más común. Fue diseñado y patentado por Christopher Sholes en 1868 y vendido a Remington en 1873.

Su nombre proviene de las primeras seis letras de su fila superior de teclas.

Figura 18. Teclado Estándar Tipo PC

2.2. MARCO REFERENCIAL

2.2.1. ANTECEDENTES

Pensar que una persona se puede autenticar en un sistema de información, tomando como referencia su ritmo de teclear al momento de introducir sus credenciales de autenticación (ID de usuario y password), parece que fuera algo novedoso, o una tecnología recién ingeniada. Pero en realidad la dinámica de tecleo tiene sus antecedentes en los Estados Unidos de America [Spaltro, 2007]. En Mayo de 1980, R.Stockton Gaines y William Lisowsky [Gaines SR, Lisowsky W, Press JS, Shapiro N, 1980] realizaron un experimento para poder comprobar el hecho de tomar como una característica única y propia de cada persona a su forma de teclear. El experimento se llevo a cabo durante dos sesiones, cada una separadas por cuatro meses, durante los cuales se pidió a seis secretarias de la RAND que teclearan tres textos diferentes, el primero constaba de un texto en inglés ordinario o común, el segundo constaba de una colección de palabras al azar en inglés, y el tercero constaba de una serie de frases al azar en inglés. De las seis secretarias se registraron los momentos de cada presión de tecla con una precisión en milisegundos.

El programa que utilizaron para capturar el tiempo de pulsación de la teclas, lo hacía midiendo el tiempo entre cada par de letras sucesivas llamados también "digráfos"[31], que es el tiempo que tomaría a una persona teclear las letras "io", "on", "an".

Los resultados de la investigación realizada por R. Stockton Gaines y William Lisowsky mostraban que la tasa de tiempo de dígrafos iba desde 75 milisegundos hasta varios segundos, los valores que se acercaban al segundo se dieron a causa de una interrupción externa durante las sesiones. Para realizar el análisis de este estudio se hizo uso de un modelo estadístico mediante una prueba de t de Student[32], mismos que arrojaron resultados de una TFA de 0% y una TFR de 4%.

En 1986 Garcia J. [Garcia, 1986] publica una patente para un método y un aparato para identificar a una persona en un sistema de control de acceso a recursos, en su trabajo toma como el mejor dato las latencias de tecleo de un usuario al momento de introducir su nombre, argumentando que el nombre es el password mas fácil de recordar para una persona. El método requiere que en la primera vez que el usuario ingrese al aparato, el introduzca una cierta cantidad de veces su password para poder proveer un vector con las medias de los tiempos de latencias del tecleo del usuario, una vez capturado este dato, la siguiente vez que el usuario desee ingresar al aparato, el mismo ya tendrá almacenado el vector que se obtuvo y el cual será comparado con el vector que se generará a partir de la segunda vez que el usuario intente ingresar. Esta comparación de vectores se lo realiza utilizando la función de distancias de Mahalanobis[33] [Bowers, Hansen, 2006] que es usado para medir la similitud entre vectores. Como resultado de sus estudios obtuvo una TFA de 0.01% y una TFR de 50%.

En 1988 Leggett J. y Williams G. [Umphress, Williams, 1985] replicaron el experimento que Gaines había realizado en años anteriores. En la réplica participaron 17 programadores, cada uno de ellos con diferentes habilidades de tecleo, a todos ellos se les provee 2 textos, el primero con alrededor de 1400 caracteres, este fue utilizado para poder crear un perfil de referencia de cada una de las personas, el segundo texto tenía alrededor de 300 caracteres

[31] Agrupación de dos letras qne representa nn solo sonido las dos eles de "callar´´ forman nn dígrafo.
[32] En probabilidad y estadística, la distribnción t (de Stndent) es nna distribnción de probabilidad qne snrge del problema de estimar la media de nna población normalmente distribnida cnando el tamaño de la mnestra es peqneño.
[33] Sn ntilidad radica en qne es nna forma de determinar la *similitud* entre dos variables aleatorias mnltidimensionales.

que sirvió para probar el perfil ya creado. Durante la sesión se tomaron 2 medidas, la media de los tiempos de latencias de tecleo y la velocidad de tecleo de la persona. Toda esta información se la almaceno en una matriz de latencias[34] de dígrafos de 26 * 26, en donde cada fila representaba a la primera letra y cada columna representaba a la segunda letra. Los resultados que obtuvieron fueron una TFA de 5.0 % y una TFR de 5.5%.

En 1989 Joyce R. y Gupta G. [Joyce, Gupta, 1990] llevan a cabo un experimento con la participación de 33 estudiantes universitarios, durante la sesión se les pidió a todos ellos que teclearan un nombre de usuario, contraseña, nombre y apellido, mismas que fueron utilizadas para poder estudiar los tiempos de latencias entre los diferentes dígrafos recurriendo para el análisis mismo de métodos estadísticos[35] como la media y la varianza, lo interesante del experimento y una variación que tuvo fue que de los 33 participantes 6 fueron escogidos al azar como blancos de los restantes 27 para una evaluación. A Cada uno de los 27 usuarios se les dio los nombres de usuarios, passwords, nombres y apellidos de las 6 personas escogidas al azar para que los mismos pudieran realizar el proceso de logueo en 5 oportunidades. Los impostores en este caso representados por los 27 estudiantes, no lograron el objetivo de poder ingresar aún teniendo la información correcta para poder loguearse. Como resultados obtuvieron una TFA de 0.25% una TFR de 16.36%.

En 1999 Monrose F. y Aviel D. R. [Monrose, Aviel, 2000] realizaron un experimento con la participación de 63 personas, lo interesante en este experimento es que a diferencia de los anteriores, no se tomó en cuenta la habilidad de las personas con respecto al tecleo, pero si se supo que las 63 personas estaban familiarizadas con las computadoras, se uso la misma clasificación que Joyce y Gupta habían tomado como muestras para el correspondiente análisis, es decir un cuarteto de datos conformado por el nombre usuario, el password, el nombre y el apellido. Las 63 personas escribieron textos al azar durante la sesión, y los datos fueron analizados utilizando una técnica de distancias Euclidianas[36], conocidas como análisis de factor, calculando dígrafos y logrando desempeños globales del clasificador con porcentajes de 83.22% hasta un 85.63%.

---

[34] Se refiere a la posición de la colnmna de memoria física en nna matriz (constitnida por colnmnas y filas) de condensadores nsados en módnlos de memoria dinámica de acceso aleatorio.

[35] Se refiere a la colección, análisis, interpretación y presentación de nna serie de datos obtenidos en nn estndio.

[36] Es la distancia "ordinaria" (qne se mediría con nna regla) entre dos pnntos de nn espacio enclídeo, la cnal se dednce a partir del teorema de Pitágoras.

En 2004 en Brasil, Araujo [Araujo, 2004] realizo un trabajo acerca de la autenticación de personal utilizando un clasificador mediante lógica difusa[37], en la sesión participaron 20 usuarios que escribían 2 contraseñas, una fija de 12 caracteres y otra libre de al menos 10 caracteres. Los resultados que obtuvo fueron para la TFA de 2.9% y para la TFR de 3.5%.

En 2006 Cheng-Huang Jiang, Shiupyng Shieh y Jen-Chien Liu [Cheng-Huang, Shiupyng, Jen-Chien, 2006] de China realizan un experimento realizado mediante un explorador web utilizando código en JavaScript del lado del cliente para poder recabar la información del tiempo de tecleo de los usuarios, en el experimento se utilizo la precisión del tiempo expresado en milisegundos y el dígrafo tomado como el tamaño de segmento de una secuencia de tecleo. Participaron 58 voluntarios suministrándoles 20 ejemplos de 2 cadenas de texto familiares: nombre de usuario y passwords. Los 58 voluntarios realizaron la prueba de autenticación en una página web en un lapso de 15 intentos. Los resultados que obtuvieron fueron para la TFA de 0.2% y para la TFR de 3.5%.

También durante el 2006 en México José Guadalupe Aguilar H. realizo un experimento con un total de 230 personas, las cuales estaban divididos en 3 grupos, el primero grupo denominado "Estudio muestral", estaba conformado por 10 personas la cuales fueron dispuestas para la creación de los perfiles en base a su dinámica de tecleo. El segundo grupo denominado "Universitarios", conformado por un grupo de alrededor de 200 personas de las carreras de Contaduría, Educación y Ciencias de la comunicación. Y finalmente el grupo 3 denominado "Varios", que estaba conformado por un grupo de 20 personas el cual se conformó por familiares, maestros y amigos de José Guadalupe Aguilar H. con este último grupo se trato de probar si la aplicación de la dinámica de tecleo era capaz de reconocer a cualquier persona dejando a un lado el hecho de que una persona contará o no con habilidades de tecleo. Para el análisis de las medidas tomadas por los diferentes grupos se tomo en cuenta el uso del método de Normalización por la media[38]. Los resultados que obtuvo fueron para la TFA de 0% y para la TFR 35%.

[37] Lógica henrística se basa en lo relativo de lo observado como posición diferencial. Este tipo de lógica toma dos valores aleatorios, pero contextnalizados y referidos entre sí.

[38] La normalización es nn método de preprocesamiento qne, en general, mejora el rendimiento de los algoritmos de clasificación, especialmente cnando los atribntos del problema toman valores en rangos diferentes.

Actualmente se están desarrollando aplicaciones de la dinámica de tecleo siendo utilizados principalmente en servicios web en donde el proceso de autenticación requiere que una persona introduzca un nombre de usuario. Empresas como DibiSoft [Allmysoft, 2007] que ya ha desarrollado un aplicación para la autenticación de usuarios con su producto "BioKeyLogon software". También empresas como AdmitOne Security, Inc. [AdmitOneSecurity, 2009] que ofrece su producto "**AdmitOne Server**", el cual es un motor de perfiles de identidad para los datos de accesos de diferentes usuarios, este producto puede detectar anomalías si se presentara y también crea los perfiles estadísticos.

2.3. MARCO JURIDICO

2.3.1. LEY DE BIOMETRIA

En Bolivia la Ley Nº 4021, fue aprobada por el Congreso Nacional el 14 de abril de 2009 y promulgada por el Presidente de la República en la misma fecha, determina que el Órgano Electoral boliviano debe conformar un nuevo Padrón Nacional Electoral mediante un registro biométrico para las elecciones del 6 de diciembre de 2009 y todas las elecciones y consultas populares (referéndum) posteriores.

Esto significa que en el nuevo Padrón Electoral, además de los datos personales de la ciudadana o ciudadano (nombres y apellidos, fecha de nacimiento, número de documento de identidad, dirección, etc.), se registrarán sus características biométricas: Huellas dactilares de los diez dedos, Fotografía digital y Firma

De esta manera se obtendrá un registro con datos más completos que permitirán una mejor y más segura identificación de cada votante.

El padrón electoral biométrico esta certificado por la norma con la norma de calidad internacional ISO 27000 que protegerá y almacenará la información para una absoluta transparencia y confiabilidad. La norma ISO 27000 es una certificación en seguridad de la información, que permite que toda la base de datos este completamente segura y almacenada en el organismo Electoral.

2.3.2. NORMAS INTERNACIONALES DE BIOMETRIA

Normalmente reconocemos a las personas que conocemos mirando sus caras y a veces por sus voces o por su escritura o por la forma en que se mueven. En tiempos pasados, el escrutinio humano era la única forma de verificar la identidad de los viajeros que se desplazaban de un país a otro, de los visitantes que pretendían entrar en zonas privadas o de los clientes que pretendían sacar dinero líquido de los bancos. Esto ya no es realista teniendo en cuenta el aumento de viajes internacionales, la necesidad de garantizar la seguridad en los lugares de trabajo y la extensión de la banca electrónica, entre otros muchos cambios que han experimentado nuestras vidas diarias. Actualmente hay una nueva forma de verificar la identidad utilizando métodos automatizados y tecnologías de la información y la comunicación (TIC) para reconocer a los individuos basándose en sus trazos físicos o en su comportamiento; se trata de un campo conocido como biometría. Ese es el tema del nuevo informe de Seguimiento Tecnológico de la UIT sobre "Biometría y normas"[1].

La biometría se aplica actualmente a los pasaportes electrónicos, así como para reconocimiento dactilovenal en los cajeros automáticos de los bancos e incluso para evitar que las máquinas expendedoras de tabaco vendan cigarrillos a los niños. En cada caso, se mide cierta combinación de las características inherentes y se comparan automáticamente con plantillas almacenadas en un archivo o en una base de datos para verificar la adaptación. Las características medidas son a menudo físicas pero también pueden ser de comportamiento, tales como una secuencia de teclas para introducir una palabra o una frase. Con la amplia aceptación de la biometría para verifi car la identidad, especialmente en un entorno de red abierta, los retos que plantean la privacidad, la fiabilidad y la seguridad de los datos biométricos son cada vez más complicados y exigentes.

Todo el que haya hecho la cola en un punto de control de un aeropuerto apreciará la importancia que tiene la velocidad y precisión a la hora de leer el pasaporte electrónico. De forma similar, cuando se saca dinero de un cajero automático, uno espera ser la única persona que puede tener acceso a su cuenta. Estos usos de la biometría nacieron con el desarrollo de las medidas para satisfacer las necesidades de una precisa identificación en

los campos de la criminología y la medicina forense; las huellas y las muestras de ADN desempeñan un papel muy importante en las historias de crímenes. Existen actualmente tres categorías principales de aplicaciones biométricas: forense, gubernamental (pasaportes, tarjetas de identidad, registro de votos, etc.) y comercial (por ejemplo, sistemas de registro en redes, cajeros automáticos, procesamiento de tarjetas de crédito y reconocimientos de rostros en software fotográfico).

Para asegurar que los sistemas de identificación biométrica son fiables, seguros, interfuncionables y fáciles de utilizar es evidente la necesidad de desarrollar normas internacionales. Las autoridades gubernamentales, en particular, no están dispuestas a aceptar sistemas no normalizados ofrecidos por un solo fabricante. Es preciso llegar a un acuerdo general sobre las características biométricas que deben medirse y debe extenderse la confianza en que estas medidas hacen posible distinguir perfectamente entre dos individuos distintos. También se necesitan normas para proteger los datos biométricos, tanto para mantener la privacidad personal como para evitar los ataques que podrían desembocar en fraudes y suplantación de personalidad. Los objetivos básicos de la normalización son los de facilitar la instalación de los sistemas de biometría, abaratar su funcionamiento e incrementar su fiabilidad de utilización.

2.3.1.1. ORGANIZACIONES DE ELABORACIÓN DE NORMAS

Aunque las primeras normas de biometría fueron creadas por los gobiernos y los cuerpos de seguridad del Estado en los 80 para intercambiar datos sobre huellas digitales, el actual ritmo acelerado de desarrollo de normas no comenzó hasta 2002. Actualmente, están elaborando dichas normas varios organismos nacionales e internacionales entre los que puede citarse la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI) y el Sector de Normalización de las Telecomunicaciones de la UIT (UIT–T). Los consorcios industriales también crean normas que soportan los objetivos de sus miembros, mientras que los organismos especializados de las Naciones Unidas, tales como la Organización de la Aviación Civil Internacional (OACI) y la Organización Internacional del Trabajo (OIT), redactan normas en el marco de sus dominios específicos que puede que no hayan sido abordados por otras organizaciones. En

particular, la OACI es responsable de la normalización de documentos de viaje legibles por máquina, incluidos los pasaportes electrónicos, mientras que la OIT ha establecido directrices sobre documentos de identidad biométrica para navegantes.

Desde el establecimiento de su Subcomité 37 sobre Biométrica, en junio de 2002, el Comité Técnico Mixto (JTC 1) de la ISO/CEI ha elaborado más de 30 normas internacionales sobre biometría. Los trabajos del JTC 1 relativos a normas de biometría también los lleva a cabo su Subcomité 27 sobre Técnicas de Seguridad TI (que cubre protección de plantillas, seguridad de los algoritmos y evaluación de la seguridad), y su Subcomité 17 sobre Tarjetas e Identificación Personal.

En el seno del UIT–T, los trabajos sobre biometría comenzaron en 2001 bajo la responsabilidad de la Comisión de Estudio 17 del UIT–T que coordina estas actividades a través de todos sus Grupos de Trabajo. En particular, la citada Comisión es responsable del estudio de la gestión de identidad; es decir, los métodos técnicos adecuados para identificar a los individuos y proteger sus identidades. Se están intensificando los trabajos para abordar el nuevo reto que supone lograr una infraestructura, unos servicios y unas aplicaciones de red más seguros. Evidentemente, las aplicaciones de telecomunicaciones que utilizan terminales móviles y servicios de Internet requieren métodos de autentificación que no sólo proporcionen un elevado grado de seguridad sino que sean convenientes para los usuarios. Hasta la fecha se han publicado más de 70 Recomendaciones UIT–T sobre seguridad.

2.3.1.2. SISTEMAS DE BIOMETRÍA

Todos los sistemas de biometría tienen una componente de almacenamiento que contiene muestras de datos biométricos de individuos vinculados a información sobre su identidad. También hay un sensor que captura los datos de biometría de la persona. Las muestras de estos datos capturados se comparan con una plantilla de referencia y se toma una decisión respecto a su coincidencia o no. En telebiometría, los canales de comunicación entre estas componentes de un sistema biométrico pueden ser telecomunicaciones alámbricas o inalámbricas, o redes privadas o públicas, incluida Internet. Tanto si el trazo de biometría es físico (como por ejemplo el ADN) como de comportamiento (por ejemplo, una secuencia de teclado), cada individuo debe tener una característica única. Además, esa característica

biométrica debe permanecer invariable a lo largo de un cierto periodo de tiempo y también debe ser mensurable.

La Recomendación UIT–T X.1081 "El modelo telebiométrico multimodal — Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad" es la primera norma de biometría que se publica. Proporciona un modelo que puede utilizarse como marco para identificar y especificar aspectos de seguridad de la telebiometría y para clasificar las tecnologías biométricas utilizadas con fines de identificación. El modelo multimodal cubre las interacciones tanto físicas como de comportamiento entre una persona y el entorno, proporcionando una taxonomía de más de 1.600 combinaciones de unidades de medición, modalidades y campos de estudio. El modelo se basa en un trabajo teórico anterior relativo a la forma en que los seres humanos interactúan con su entorno y en las series de normas internacionales ISO/CEI 80000, que especifican las cantidades y unidades de todas las formas de medición conocidas de la magnitud de interacciones entre los individuos y su entorno.

Más de 50 países expiden a sus ciudadanos pasaportes legibles por máquina que almacenan datos biométricos que pueden utilizarse para verificar la identidad en las fronteras. Una imagen facial, y quizás una representación digital de las huellas dactilares o del iris, se almacena en un pequeño chip de identificación por radiofrecuencia (RFID) que se somete a una comparación con la información contenida en una base de datos biométrica. El Grupo Mixto de Expertos en Fotografía (JPEG), Grupo de Trabajo de la ISO/CEI y la UIT, es responsable de las familias JPEG, JPEG2000, JPSearch y JPEG XR de normas de imágenes. Se trata de métodos de compresión de imágenes que se utilizan normalmente para almacenar fotografías digitales en el chip de un pasaporte electrónico. Las normas para el formato JPEG o JPEG2000 figuran, respectivamente, en las Recomendaciones UIT–T T.81 y T.800 elaboradas por la Comisión de Estudio 16 del UIT–T. JPEG XR (ISO/CEI 29199-2) es actualmente una norma internacional que viene reflejada en la Recomendación UIT–T T.832 y que especifica un formato de imagen codificada, diseñado fundamentalmente para el almacenamiento e intercambio del contenido fotográfico de tono continuo.

2.3.1.3. GARANTIZAR LA SEGURIDAD DE LOS DATOS

Una llave se puede perder, robar o duplicar. Una clave puede olvidarse. Normalmente se considera que las características de biometría tienen la ventaja de ser virtualmente imposibles de olvidar o robar y difíciles de adivinar. Sin embargo, los sistemas biométricos son vulnerables a los ataques. Cualquier elemento de estos sistemas puede ser el objetivo. El sensor, el extractor de características, el adaptador, la plantilla de biometría almacenada o el punto final de decisión. También puede realizarse un ataque puenteando el sensor biométrico o manipulando la plantilla o el extractor de características.

La biometría se utiliza cada vez más para complementar o sustituir los esquemas de autentificación tradicionales tales como los números de identificación personal (PIN) o las claves. Pero los datos de biometría no pueden mantenerse secretos. Las fotografías de rostros, las grabaciones de voces y las copias de firmas, por ejemplo, se realizan fácilmente. La biometría se basa en información personal muy sensible pero la seguridad de un sistema de autentificación no puede basarse en el secreto de los datos de biometría. Un sistema debe garantizar la integridad y la autenticidad de los datos biométricos para que sea operacionalmente eficaz y, por consiguiente, se necesitan tomar medidas protectoras adicionales a fin de salvaguardar la privacidad.

Con objeto de permitir una autentificación segura, las Recomendaciones UIT–T X.1084 y X.1085 especifican nueve protocolos de autentificación para telebiometría y describen perfiles de protección, mientras que la Recomendación UIT–T X.1086 proporciona orientaciones sobre contramedidas para establecer un entorno seguro y privacidad. La Recomendación UIT–T X.1087 fija procedimientos para proteger los datos biométricos multimodales contra intentos de intercepción, modificación o sustitución de dichos datos. Los procedimientos incluyen encriptado, marcas de agua y datos de transformación. Otras dos normas, las Recomendaciones UIT–T X.1088 y X.1089, proporcionan respectivamente un marco para generar y proteger claves digitales biométricas y una forma de gestionar la autentificación biométrica.

2.3.1.4. APLICACIONES COMERCIALES Y GUBERNAMENTALES PARA ORIENTAR EL CRECIMIENTO

Los avances experimentados por las TIC y el mayor rendimiento y disponibilidad de equipos de bajo coste han facilitado los métodos de reconocimiento biométrico automático. Los futuros servicios de cibercomercio, cibersalud y ciberadministración pueden requerir la autentificación con la ayuda de documentos personales biométricos expedidos por los gobiernos. Por ejemplo, algunos países en desarrollo ya han empezado a utilizar la biometría para el registro de votos antes de la celebración de elecciones a fin de actualizar las listas de votantes y evitar fraudes electorales.

Las previsiones de mercado sobre gastos en biometría son generalmente positivas. Se espera que el crecimiento proceda fundamentalmente de aplicaciones comerciales y gubernamentales donde las empresas de biometría y las empresas que fabrican tarjetas inteligentes se benefi ciarán de las decisiones gubernamentales en el sentido de adoptar procedimientos biométricos y documentos personales electrónicos. En 2008 se realizó un gasto estimado de 3.000 millones USD en tecnologías de biometría y los investigadores del mercado prevén actualmente una inversión de 7.300 millones USD en 2013.

Junto con las huellas dactilares, que seguirán siendo la característica biométrica dominante, se espera que surjan sistemas de reconocimiento del rostro, del iris, de la mano y de la voz ampliamente adoptados en aplicaciones de biometría.

Las normas permiten un desarrollo eficaz de los sistemas de biometría estableciendo criterios comunes y fijando directrices para la protección de la privacidad. Los acuerdos sobre formatos de los datos e interfaces del software de aplicación ayudarán a reducir los costes de desarrollo de los sistemas. Además, la elaboración de normas para aplicar la biometría y para probar la precisión contribuye a aclarar las vulnerabilidades y orientar la investigación sobre contramedidas para repeler los ataques.

Las características biométricas no sólo deben ser universales y únicas, también tienen que ser razonablemente permanentes y fáciles de recopilar y medir. Un sistema de biometría debe proporcionar resultados precisos bajo diversas circunstancias del entorno y debe ser

difícil de engañar. Quizá el aspecto más importante de un sistema de biometría es su aceptación por el público en general. Por razones evidentes, los métodos no intrusivos son más aceptables que las técnicas intrusivas. Aunque el ADN se considera el parámetro de biometría definitivo para identificar a una persona (excepción hecha de gemelos idénticos), la comprobación del ADN es demasiado intrusiva para su amplio uso en la autentificación de identidad. La termografía facial, que detecta los modelos de cabezas creados por los capilares sanguíneos y emitidos por la piel, no es un método intrusivo pero es demasiado costoso. Entre los métodos de biometría actualmente considerados para su futuro desarrollo están los impulsos sanguíneos, el olor corporal, la composición de la piel, la disposición de la matriz de la uña, el modo de andar y la forma de la oreja. Se necesitan más investigaciones para determinar si alguno de estos métodos acabará imponiéndose como la elección en las técnicas de biometría.

Cualquiera que sea el sistema utilizado debe ser seguro, garantizar la privacidad y producir resultados precisos. Un sistema inseguro, no fiable o invasivo menoscabará la confianza del público y puede desembocar en una falta general de aceptación de las técnicas de reconocimiento por biometría. El desarrollo de normas internacionales es una estrategia fundamental a la hora de garantizar la elección y el uso adecuados de los métodos biométricos. En menos de una década se han hecho grandes progresos en la mejora de los sensores, algoritmos y procedimientos de biometría pero siguen existiendo puntos vulnerables que deben abordarse. La necesidad de proteger la privacidad y salvaguardar los datos biométricos sensibles sigue siendo fundamental.

2.4. MARCO TECNOLOGICO

La plataforma en la que se trabajara será en .NET de Microsoft es un componente de software que puede ser añadido al sistema operativo Windows XP, Windows Vista, etc. Provee un extenso conjunto de soluciones predefinidas para necesidades generales de la programación de aplicaciones, y administra la ejecución de los programas escritos específicamente con la plataforma.

Las herramientas a utilizar será: S.O. Windows XP, ASP.net (c#) como lenguaje de servidor, SQL Server como gestor de base de datos y Javascript para el control del tecleo.

2.4.1. MICROSOFT .NET

Microsoft.NET es el conjunto de nuevas tecnologías en las que Microsoft ha estado trabajando estos últimos años con el objetivo de mejorar tanto su sistema operativo como su modelo de componentes (COM) para obtener una plataforma con la que sea sencillo el desarrollo de software en forma de servicios web.

Los servicios web son un novedoso tipo de componentes software que se caracterizan a la hora de trabajar por su total independencia respecto a su ubicación física real, la plataforma sobre la que corre, el lenguaje de programación con el que hayan sido desarrollados o el modelo de componentes utilizado para ello.

El acceso a estos servicios se realiza en base a estándares de Internet, como son diferentes mecanismos del protocolo HTTP (GET y PUT) o el novedoso protocolo RPC conocido como SOAP (Simple Access Object Protocol), que no es más que una combinación de estándares como HTTP y XML para realizar llamadas a los miembros de estos servicios web. La idea detrás de SOAP consiste sencillamente en utilizar HTTP como medio de transporte para el envío de los mensajes de solicitud de ejecución de los miembros de servicios web remotos (lo que permite atravesar barreras tales como firewalls) y utilizar XML como lenguaje con el que escribir los cuerpos de estos mensajes.

Pero la plataforma .NET no son sólo los servicios web, sino que también ofrece numerosos servicios a las aplicaciones que para ella se escriban, como son un recolección de basura, independencia de la plataforma, total integración entre lenguajes (por ejemplo, es posible escribir una clase en C# que derive de otra escrita en Visual Basic.NET que a su vez derive de otra escrita en Cobol)

Como se deduce del párrafo anterior, es posible programar la plataforma .NET en prácticamente cualquier lenguaje, pero Microsoft ha decidido sacar uno nuevo porque ha visto conveniente poder disponer de un lenguaje diseñado desde 0 con vistas a ser utilizado en .NET, un lenguaje que no cuente con elementos heredados de versiones anteriores e innecesarios en esta plataforma y que por tanto sea lo más sencillo posible para programarla aprovechando toda su potencia y versatilidad.

2.4.2. ASP .NET

Es un lenguaje de programación que se encuentra dentro del entorno de desarrollo integrado (IDE, por sus siglas en ingles) Microsoft Visual Studio 2008.

ASP.NET es un framework para aplicaciones web desarrollado y comercializado por Microsoft. Es usado por programadores para construir sitios web dinámicos, aplicaciones web y servicios web XML. Apareció en enero de 2002 con la versión 1.0 del .NET Framework, y es la tecnología sucesora de la tecnología Active Server Pages (ASP).

Es parte del Internet Information Server (IIS) desde la versión 3.0 y es una tecnología de páginas activas que permite el uso de diferentes scripts y componentes en conjunto con el tradicional HTML para mostrar páginas generadas dinámicamente, traduciendo la definición de ***Microsoft***: "Las Active Server Pages son un ambiente de aplicación abierto y gratuito en el que se puede combinar código HTML, scripts y componentes ActiveX del servidor para crear soluciones dinámicas y poderosas para el web".

El ASP es una tecnología dinámica funcionando del lado del servidor, lo que significa que cuando el usuario solicita un documento ASP, las instrucciones de programación dentro del script son ejecutadas para enviar al navegador únicamente el código HTML resultante. La ventaja principal de las tecnologías dependientes del servidor radica en la seguridad que tiene el programador sobre su código, ya que éste se encuentra únicamente en los archivos del servidor que al ser solicitado a través del web, es ejecutado, por lo que los usuario no tienen acceso más que a la página resultante en su navegador.

2.4.3. SQL SERVER

Microsoft SQL Server es un sistema para la gestión de bases de datos producido por Microsoft basado en el modelo relacional. Sus lenguajes para consultas son T-SQL y ANSI SQL. Microsoft SQL Server constituye la alternativa de Microsoft a otros potentes sistemas gestores de bases de datos como son Oracle o PostgreSQL o MySQL.

Sql server 2005 contiene mayor seguridad, integración con PowerShell, remueve la configuración del área expuesta (consola para configurar seguridad), cifrado transparente de datos, auditoría de datos, compresión de datos, tiene correctores de sintaxis del lenguaje Transact-SQL e IntelliSense (una carácteristica del visual studio que permite a la base de datos sugerir objetos existentes mientras uno escribe la mitad de la palabra). Así mismo incluye nuevos tipos de datos y funciones. Entre ellos, datos espaciales, nuevos datos de tiempo (datetime2 y Datetimeoffset), tipos de datos jerárquicos.

2.4.4. JAVASCRIPT

Javascript es un lenguaje de programación que permite a los desarrolladores crear acciones en sus páginas web.

Javascript es un lenguaje que puede ser utilizado por profesionales y para quienes se inician en el desarrollo y diseño de sitios web. No requiere de compilación ya que el lenguaje funciona del lado del cliente, los navegadores son los encargados de interpretar estos códigos.

Muchos confunden el Javascript con el Java pero ambos lenguajes son diferentes y tienes sus características singulares. Javascript tiene la ventaja de ser incorporado en cualquier página web, puede ser ejecutado sin la necesidad de instalar otro programa para ser visualizado.

Java por su parte tiene como principal característica ser un lenguaje independiente de la plataforma. Se puede crear todo tipo de programa que puede ser ejecutado en cualquier ordenador del mercado: Linux, Windows, Apple, etc. Debido a sus características también es muy utilizado para internet.

Como síntesis se pude decir que Javascript es un lenguaje interpretado, basado en prototipos, mientras que Java es un lenguaje más orientado a objetos.

Javascript es un lenguaje con muchas posibilidades, utilizado para crear pequeños programas que luego son insertados en una página web y en programas más grandes,

orientados a objetos mucho más complejos. Con Javascript podemos crear diferentes efectos e interactuar con nuestros usuarios.

Este lenguaje posee varias características, entre ellas podemos mencionar que es un lenguaje basado en acciones que posee menos restricciones. Además, es un lenguaje que utiliza Windows y sistemas X-Windows, gran parte de la programación en este lenguaje está centrada en describir objetos, escribir funciones que respondan a movimientos del mouse, aperturas, utilización de teclas, cargas de páginas entre otros.

Es necesario resaltar que hay dos tipos de JavaScript: por un lado está el que se ejecuta en el cliente, este es el Javascript propiamente dicho, aunque técnicamente se denomina Navigator JavaScript. Pero también existe un Javascript que se ejecuta en el servidor, es más reciente y se denomina LiveWire Javascript.

2.4.5. C#

C# es el nuevo lenguaje de propósito general orientado a objetos creado por Microsoft para su nueva plataforma .NET.C# combina los mejores elementos de múltiples lenguajes de amplia difusión como C++, Java, Visual Basic o Delphi. De hecho, su creador Anders Heljsberg fue también el creador de muchos otros lenguajes y entornos como Turbo Pascal, Delphi o Visual J++. La idea principal detrás del lenguaje es combinar la potencia de lenguajes como C++ con la sencillez de lenguajes como Visual Basic, y que además la migración a este lenguaje por los programadores de C/C++/Java sea lo más inmediata posible.

Además de C#, Microsoft proporciona Visual Studio.NET, la nueva versión de su entorno de desarrollo adaptada a la plataforma .NET y que ofrece una interfaz común para trabajar de manera cómoda y visual con cualquiera de los lenguajes de la plataforma .NET (por defecto, C++, C#, Visual Basic.NET y JScript.NET, aunque pueden añadirse nuevos lenguajes mediante los plugins que proporcionen sus fabricantes).

2.5. MARCO METODOLOGICO

2.5.1. METODOLOGIA

La metodología es el conjunto de procedimientos (métodos y técnicas) que se aplican para responder al problema de la investigación.

2.5.1.1. METODO CIENTIFICO

Se aplico el método científico propuesto por Mario Bunge (2000) la cual contempla los siguientes pasos:

a) Planteamiento del problema
b) Especificación de la hipótesis
c) Material y métodos
d) Análisis y verificación mediante prototipo y casos de prueba
e) Verificación de los resultados

2.5.1.2. METODO ESTADISTICO

2.5.1.2.1. ESTADISTICA

La estadística es comúnmente considerada como una colección de hechos numéricos expresados en términos de una relación sumisa, y que han sido recopilados a partir de otros datos numéricos. Kendall y Buckland [citados por Gini V. Glas / Julian C. Stanley, 1980] definen la estadística como un valor resumido, calculado, como base en una muestra de observaciones que generalmente, aunque no por necesidad, se considera como una estimación de parámetro de determinada población; es decir, una función de valores de muestra.

"La estadística es una técnica especial apta para el estudio cuantitativo de los fenómenos de masa o colectivo, cuya mediación requiere una masa de observaciones de otros fenómenos más simples llamados individuales o particulares". [Gini, 1953].

Murria R. Spiegel, (1991) dice: "La estadística estudia los métodos científicos para recoger, organizar, resumir y analizar datos, así como para sacar conclusiones válidas y tomar decisiones razonables basadas en tal análisis.

"La estadística es la ciencia que trata de la recolección, clasificación y presentación de los hechos sujetos a una apreciación numérica como base a la explicación, descripción y comparación de los fenómenos". [Yale y Kendal, 1954]

Cualquiera sea el punto de vista, lo fundamental es la importancia científica que tiene la estadística, debido al gran campo de aplicación que posee.

2.5.1.2.2. ESTADÍSTICA DESCRIPTIVA

Tienen por objeto fundamental describir y analizar las características de un conjunto de datos, obteniéndose de esa manera conclusiones sobre las características de dicho conjunto y sobre las relaciones existentes con otras poblaciones, a fin de compararlas. No obstante puede no solo referirse a la observación de todos los elementos de una población (observación exhaustiva) sino también a la descripción de los elementos de una muestra (observación parcial). En relación a la estadística descriptiva, "Para el estudio de estas muestras, la estadística descriptiva nos provee de todos sus medidas; medidas que cuando quieran ser aplicadas al universo total, no tendrán la misma exactitud que tienen para la muestra, es decir al estimarse para el universo vendrá dada con cierto margen de error; esto significa que el valor de la medida calculada para la muestra, en el oscilará dentro de cierto límite de confianza, que casi siempre es de un 95 a 99% de los casos". [Ernesto Rivas Gonzáles]

2.5.1.2.2.1. MEDIA ARITMÉTICA

La media aritmética o promedio, de una cantidad finita de números, es igual a la suma de todos ellos dividida entre el número de sumandos. Expresada de forma más intuitiva, podemos decir que la media (aritmética) es la cantidad total de la variable distribuida a partes iguales entre cada observación. Por ejemplo, si en una habitación hay tres personas, la media de dinero que tienen en sus bolsillos sería el resultado de tomar todo el dinero de

los tres y dividirlo a partes iguales entre cada uno de ellos. Es decir, la media es una forma de resumir la información de una distribución (dinero en el bolsillo) suponiendo que cada observación (persona) tendría la misma cantidad de la variable. También la media aritmética puede ser denominada como centro de gravedad de una distribución, el cual no es necesariamente la mitad.

Así, dados los números $a1$, $a\,2$,..., $a\,n$, la media aritmética será igual a:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} a_i = (a_1 + \cdots + a_n)/n$$

Por ejemplo, la media aritmética de 8, 5 y -1 es igual a (8 + 5 + (-1)) / 3 = 4. El símbolo μ (mi) es usado para la media aritmética de una población. Usamos X, con una barra horizontal sobre el símbolo para medias de una muestra ($\overline{X}$).

2.5.1.2.2.2. MEDIANA

Si tenemos n valores $x_1, x_2, x_3, \ldots, x_n$ habiendo sido ordenados de forma creciente: se define la mediana como el valor que deja a cada lado (por encima y por debajo) la mitad de los valores de la muestra.

Matemáticamente toma por valor:

$x_{\frac{n+1}{2}}$, si n es impar

$\frac{x_{\frac{n}{2}} + x_{\frac{n}{2}+1}}{2}$, si n es par

2.5.1.2.2.3. DESVIACION ESTÁNDAR

La desviación estándar (o desviación típica) es una medida de dispersión para variables de razón (ratio o cociente) y de intervalo, de gran utilidad en la estadística descriptiva. Es una medida (cuadrática) de lo que se apartan los datos de su media, y por tanto, se mide en las mismas unidades que la variable. Para conocer con detalle un conjunto de datos, no basta con conocer las medidas de tendencia central, sino que necesitamos conocer también la desviación que representan los datos en su distribución, con objeto de tener una visión de los mismos más acorde con la realidad a la hora de describirlos e interpretarlos para la toma de decisiones.

2.5.1.2.2.4. COEFICIENTE DE VARIACIÓN

El coeficiente de dispersión es útil para comparar dispersiones a escalas distintas pues es una medida invariante ante cambios de escala. Por otro lado presenta problemas ya que a diferencia de la desviación típica este coeficiente es variable ante cambios de origen. Por ello es importante que todos los valores sean positivos y su media de por tanto un valor positivo.

$$\bar{x} > 0$$

Se exige que:

Se calcula:

$$CV = \frac{S}{\bar{x}}$$

donde S es la desviación típica. Se puede dar en tanto por ciento calculando:

$$CV = \frac{S}{\bar{x}} \cdot 100$$

2.5.1.2.2.5. FUNCION DE SCORING

Una función es una correspondencia entre conjuntos que se produce cuando cada uno de los elementos del primer conjunto se halla relacionado con un solo elemento del segundo conjunto. Estamos en presencia de una función cuando de cada elemento del primer conjunto solamente sale una única flecha.

La función de scoring es una función exponencial se encarga de relacionar los valores de la media y desviación estándar y de esta manera tendremos un vector de valores score.

$$S(x_0)=\exp((-1/2\sigma_0^2)*(x_0-\mu_0)^2)$$
$$S(x_1)=\exp((-1/2\sigma_1^2)*(x_1-\mu_1)^2)$$
$$S(x_2)=\exp((-1/2\sigma_2^2)*(x_2-\mu_2)^2)$$
$$\vdots$$
$$S(x_{2*n-1})=\exp((-1/2\sigma_{2*n-1}^2)*(x_{2*n-1}-\mu_{2*n-1})^2)$$
$$S(x)=|S(x_0),S(x_1),S(x_2),\ldots,S(x_{2*n-1})|$$

Una vez obtenido el vector de valores SCORE, realizamos una media entre ellos para obtener un solo valor a comparar.

$$S=1/(2*n-1)\sum S_i$$

Una vez obteniendo este valor se compara con el valor de umbral (que se definirá más adelante).

2.6. MARCO CONCEPTUAL

2.6.1. SEGURIDAD

El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien.

Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

2.6.2. SEGURIDAD INFORMATICA

Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos. En un sistema de los denominados 'tolerante a fallos' dos o más ordenadores funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control. Los virus informáticos son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro.

2.6.3. CONFIDENCIALIDAD

La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.

2.6.4. INTEGRIDAD

La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

2.6.5. DISPONIBILIDAD

El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

2.6.6. NO REPUDIO

Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

2.6.7. AUTENTICACIÓN

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

2.6.8. CONTROL DE ACCESO

Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos (ej: acceso a una habitación donde hay servidores), recursos lógicos (ej: una cuenta de banco, de donde solo determinadas personas pueden extraer dinero) o recursos digitales (ej: un archivo informático que sólo puede ser leído, pero no modificado).
Un sistema informático supuesto para ser utilizado solamente por aquellos autorizados, debe procurar detectar y excluir el desautorizado. El acceso a él por lo tanto es controlado generalmente insistiendo en un procedimiento de la autentificación para establecer con un cierto grado establecido de confianza la identidad del usuario, por lo tanto concediendo esos privilegios como puede ser autorizado a esa identidad. Los ejemplos comunes del control de acceso que implican la autentificación incluyen:

- Retirar de dinero de un cajero automático.
- Control de un computador remoto sin Internet.
- Uso de aplicaciones en Internet: banking, email, etc.

2.6.9. BIOMETRÍA

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

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

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

2.6.10. BIOMETRIA ESTATICA

Son aquellas características fisiológicas que se encuentran en cada ser humano, los cuales son estables en el tiempo (bajo circunstancias normales), entre ellos tenemos: los rasgos del rostro de una persona, la geometría de la mano, la huellas dactilares que son el mecanismo de autenticación más usado y difundido, los patrones de iris y retina.

2.6.11. BIOMETRÍA DINÁMICA

Muchas de las tareas rutinarias que realizamos a diario hace que seamos predecibles, aprovechando estas características es que se ha desarrollado la biometría dinámica o de comportamiento, la misma analiza los rasgos de comportamiento o conducta de una persona tales como: la forma de caminar, la voz, la forma de escribir, la firma y los ritmos de tecleo que tiene una persona, también conocida como dinámica de teclado.

2.6.12. TASA DE FALSA ACEPTACIÓN

La TFA se refiere al error que ocurre cuando el sistema biométrico identifica de una manera incorrecta los rasgos de la muestra biométrica como iguales con respecto a otros rasgos de una muestra almacenada en su base de datos, es decir, concede acceso a un usuario no legítimo. Este error es conocido en Estadística como falsos positivos.

2.6.13. TASA DE FALSO RECHAZO

La TFR se refiere a los errores que se presentan cuando el sistema biométrico de una manera incorrecta no iguala la muestra biométrica con una muestra registrada en su base de datos, denegando el acceso a u usuario que es legítimo. Dentro de la Estadística este error se conoce como falsos negativos.

2.6.14. TASA DE ERROR DE CRUCE

Cuanto más bajo es el TCE, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo.

2.6.15. BIOMETRÍA DE TECLEO

La dinámica de tecleo, o biometría del tecleo, es la información de tiempo detallado que describe exactamente cuando cada tecla es presionada y soltada por una persona cuando escribe en un teclado de computadora. La dinámica de tecleo es una rama de la biometría que se dedica al estudio del reconocimiento del patrón de tecleo de un usuario.

2.6.16. MÉTODO CIENTÍFICO

El método científico (del griego: -μετά = hacia, a lo largo- -οδός = camino-; y del latín scientia = conocimiento; camino hacia el conocimiento) es un método de investigación usado principalmente en la producción de conocimiento en las ciencias. Presenta diversas definiciones debido a la complejidad de una exactitud en su conceptualización: "Conjunto de pasos fijados de antemano por una disciplina con el fin de alcanzar conocimientos válidos mediante instrumentos confiables", "secuencia estándar para formular y responder a una pregunta", "pauta que permite a los investigadores ir desde el punto A hasta el punto Z con la confianza de obtener un conocimiento válido".

2.6.17. MÉTODOS ESTADISTICOS

Como la estadística trabaja con números, el procedimiento que utiliza es: es a partir de datos numéricos para obtener resultados mediante determinados reglas y operaciones, este procedimiento se denomina método estadístico.

2.6.18. MEDIA ARITMÉTICA

En matemáticas y estadística, la media aritmética (también llamada promedio o simplemente media) de un conjunto finito de números es igual a la suma de todos sus valores dividida entre el número de sumandos. Cuando el conjunto es una muestra aleatoria recibe el nombre de media muestral siendo uno de los principales estadísticos muestrales.

Expresada de forma más intuitiva, podemos decir que la media (aritmética) es la cantidad total de la variable distribuida a partes iguales entre cada observación.

2.6.19. DESVIACIÓN ESTÁNDAR

La desviación estándar o desviación típica (σ) es una medida de centralización o dispersión para variables de razón (ratio o cociente) y de intervalo, de gran utilidad en la estadística descriptiva.

Se define como la raíz cuadrada de la varianza. Junto con este valor, la desviación típica es una medida (cuadrática) que informa de la media de distancias que tienen los datos respecto de su media aritmética, expresada en las mismas unidades que la variable.

Para conocer con detalle un conjunto de datos, no basta con conocer las medidas de tendencia central, sino que necesitamos conocer también la desviación que representan los datos en su distribución respecto de la media aritmética de dicha distribución, con objeto de tener una visión de los mismos más acorde con la realidad al momento de describirlos e interpretarlos para la toma de decisiones.

2.6.20. FUNCIÓN DE SCORING

La función de scoring es una función exponencial se encarga de relacionar los valores de la media y desviación estándar y de esta manera tendremos un vector de valores score.

Una vez obtenido el vector de valores SCORE, realizamos una media entre ellos para obtener un solo valor a comparar. Una vez obteniendo este valor se compara con el valor de umbral.

2.6.21. UMBRAL

El umbral es la cantidad mínima de señal que ha de estar presente para ser registrada por un sistema. Por ejemplo, la mínima cantidad de luz que puede detectar el ojo humano en la oscuridad. El umbral es la base de la exploración psicofísica de las sensibilidades (táctil, olfatoria, visual o auditiva). Sensibilidad = 1/Umbral. Para la determinación práctica del umbral se considera un 50% de probabilidades. Es decir, umbral es la menor cantidad de estímulo que tiene un 50% de probabilidades de ser detectado.

2.6.22. PROTOTIPO

La palabra prototipo tiene varios tipos de definiciones:

- Un Prototipo es un ejemplar o primer molde en que se fabrica una figura u otra cosa,

- Un prototipo perfecto y modelo de una virtud, vicio o cualidad.
- Un prototipo también se puede referir a cualquier tipo de máquina en pruebas, o un objeto diseñado para una demostración de cualquier tipo.
- Un prototipo o prototipado puede ser un modelo del ciclo de vida del software, tal como el desarrollo en espiral o el desarrollo en cascada.
- Un prototipo de belleza es aquel modelo que en función de la historia ha ido variando sobre cómo ha debido de ser el cuerpo de las personas, tanto en su forma como en su vestimenta.

Estos permiten testar el objeto antes de que entre en producción, detectar errores, deficiencias, etcétera. Cuando el prototipo está suficientemente perfeccionado en todos los sentidos requeridos y alcanza las metas para las que fue pensado, el objeto puede empezar a producirse.

Capítulo III

3. MARCO APLICATIVO

3.1. DESCRIPCION DEL ACTUAL Y NUEVO FUNCIONAMIENTO DE AUTENTIFICACION

3.1.1. ACTUAL FUNCIONAMIENTO

Un modo de acceso tradicional a los sistemas de cómputo en aplicaciones de internet es el basado en usuario/ contraseña, el propósito de la contraseña es verificar que el usuario es quien dice ser, de esta manera la contraseña actúa como mecanismos que autentifica el usuario, son claves que se utilizan para obtener acceso a información personal que se ha almacenado en el equipo y en sus cuentas en línea.

Sin embargo este método de autentificación presenta algunos inconvenientes debido a su simplicidad, donde los usuarios adoptan como contraseñas palabras obvias como su nombre, sus iniciales, fecha de nacimiento, etc. las cuales pueden ser robadas fácilmente, un intruso (usuario malintencionado) puede ver lo que teclea el usuario en el momento de autentificarse, o mediante programas ejecutadas en segundo plano grabar lo que el usuario teclea y así conocer su contraseña.

La contraseña no es suficiente para tener la seguridad de que usuario es físicamente quien dice ser.

3.1.2. NUEVO FUNCIONAMIENTO

Dentro del nuevo funcionamiento de autentificación se hará uso de la biometría de tecleo la cual utiliza la manera y el ritmo en la cual un usuario escribe en un teclado, los ritmos de golpes de teclas de un usuario son medidos y registrados por un algoritmo para desarrollar los patrones de tecleo las cuales nos ayudaran a autentificar a un usuario y de esta manera brindar seguridad mediante la contraseña ya que identificara si es o no es el usuario legitimo.

Brindando a este método de autentificación (contraseña) mayor seguridad al momento de ingresar en una aplicación de internet.

3.2. MODELO DEL PROTOTIPO DE IDENTIFICACION DE BIOMETRIA DE TECLEO

La dinámica de tecleo es una técnica que se basa en el principio de que la acción de escribir en el teclado una palabra o frase (contraseña) muy frecuentemente hace que el acto de escribirla se convierta en algo inconsciente y automático. Esto provoca que ese gesto sea característico nuestro porque influyen tanto procesos mentales que se convierte en una especie de huella dactilar. Los parámetros que se tienen en cuenta a la hora de mesurar la dinámica de tecleo son dos, el tiempo de pulsación de cada tecla y el tiempo entre pulsaciones. En base a estos dos parámetros se pueden crear patrones de comportamiento que nos pueden decir si un usuario es o no es quién dice ser, independientemente de que la contraseña sea correcta o no.

Una vez obteniendo estos datos requeridos, estos pasan a un vector para su respectivo almacenamiento que posteriormente son comparados en el proceso de identificación y registrados en la base de datos principal.

Lo que vamos a hacer es un prototipo de control de usuario. El usuario va a tener que introducir su usuario /contraseña, y se controlará la biometría de tecleo de la contraseña. Dicho tecleo se comparará con un patrón del usuario para ver qué probabilidad hay de que sea realmente nuestro usuario y no un suplantador. Hay que tener en cuenta que cuando hablamos de biometría siempre consideramos probabilidades y no certezas. A la hora de configurar el prototipo tendremos que elegir cuál es el umbral a partir del cual consideraremos que el usuario es un suplantador. Cuanto mayor sea ese umbral, mayor será la seguridad pero más falsos negativos dará y cuanto menor sea el umbral, menor la seguridad pero menos falsos negativos.

3.2.1. ESQUEMA DEL MODELO

A continuación se detallan las diferentes partes o módulos que se integraron para el desarrollo del prototipo (figura 12) propuesto en esta tesis, el cual fue programado en su totalidad usando la plataforma Visual .net, la elección de la misma fue debido a la facilidad de integración que se tiene con el desarrollo de aplicaciones web.

El prototipo funciona a partir de un nombre de usuario y una contraseña, ambos elegidos de manera libre, siendo la contraseña sobre la cual se hará el cálculo de la biometría de tecleo del usuario y a partir de estas muestras determinar si es o no es el usuario.

El modelo del prototipo realiza los siguientes procesos fundamentales de reconocimiento y comparación.

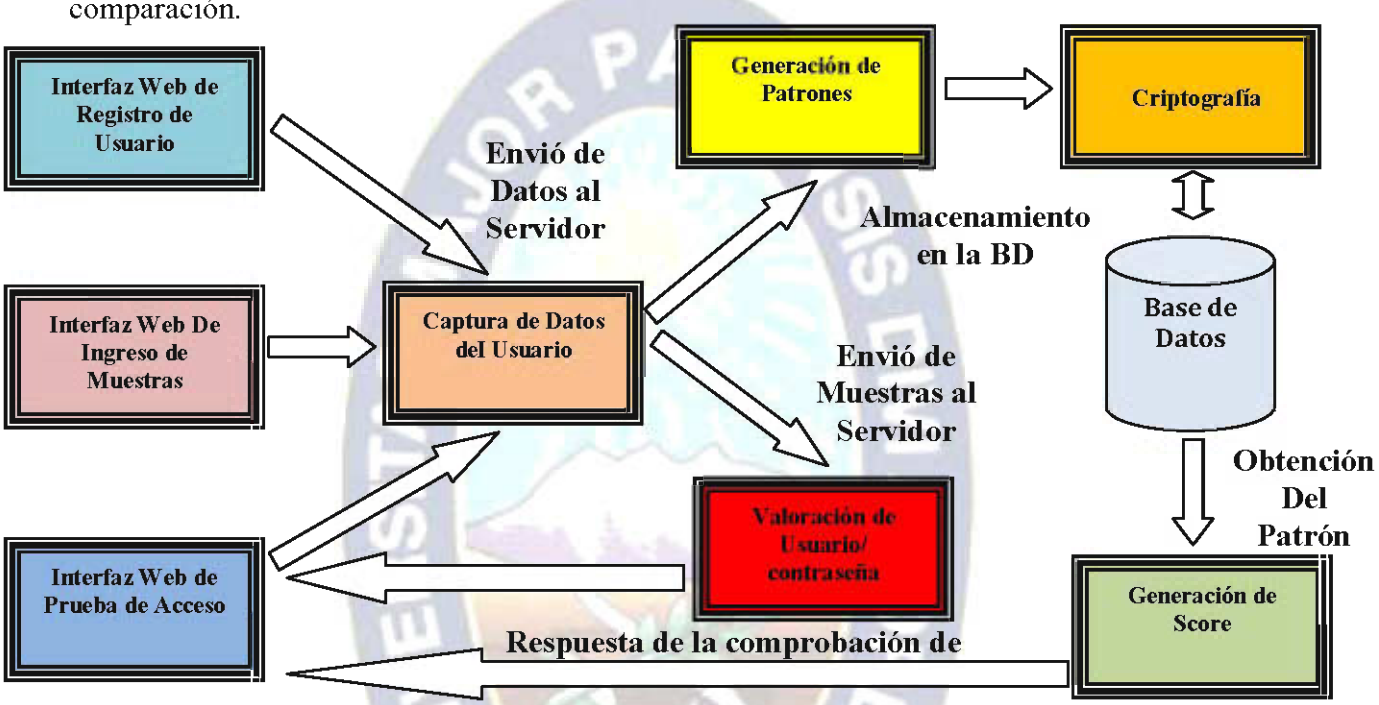


Figura 19. Esquema del Modelo

Fuente: Elaboración propia

3.3. DESCRIPCION INFORMAL DEL MODELO

Usuario: El usuario es una parte importante dentro del prototipo, ya que será el que introducirá los datos mediante el teclado.

Interfaz Web de registro de usuario: Sera el encargado de interactuar con el usuario y realizar su registro en la Base de Datos donde ingresara su usuario y contraseña.

Ellos ingresaran a la interfaz web de registro de usuarios donde ingresaran su usuario/contraseña y esta se almacenara en la base de datos en la tabla usuario.

Interfaz Web de ingreso de muestras: Sera el encargado de interactuar con el usuario, a partir de aquí el usuario introducirá su contraseña 10 veces para poder tener un patrón de tecleo.

El usuario puede ir introduciendo nuevas muestras, cuantas más muestras se tengan mayor será el acierto del sistema.

Ya registrados nuestros usuarios se realizara la generación de los patrones de tecleo de esta población, ellos ingresaran a la interfaz web de ingreso de muestras donde ingresaran su contraseña repetidamente, y se medirá el tiempo de pulsación y tiempo entre pulsaciones en milisegundos y serán almacenadas en la base de datos en la tabla muestras. El contador de los tiempos del prototipo deberá ser demasiado rápido, pues entre más rápido se incremente el contador, más fácil será de capturar la dinámica de tecleo de un usuario. La medida del tiempo en cada caso será en milisegundos con una precisión de hasta cuatro cifras.

Interfaz Web Prueba de Acceso: Es el encargado de interactuar con el usuario, donde el usuario tendrá que introducir su usuario /contraseña y si es el usuario legitimo podrá acceder a una aplicación web.

Captura de Datos del Usuario: Este módulo es una parte importante del prototipo, ya que es el que permite capturar los tiempos de tecleo del usuario al momento de introducir su contraseña y posterior almacenamiento.

Generación de patrones: Dentro de este modulo tomaremos la muestra para el tiempo de pulsación y entre pulsaciones del usuario.

Valoración de usuario/Contraseña: Dentro de este modulo la valoración de usuario será la que nos diga si realmente es o no es el usuario.

Generación de Score: La función de Scoring será la que se encargara de determinar el grado de similitud entre la clave introducida por el usuario (contraseña) que se quiere autenticar y el patrón almacenado en la base de datos.

Criptografía: Dentro de este modulo se encriptaran las contraseñas de los usuarios para mayor seguridad de los datos.

Base de Datos: Dentro de la Base de Datos tendremos dos tablas con las que trabajaremos una de usuario y la otra de muestras.

Para el modelado de la base de datos utilizaremos el diagrama de clases del UML donde:

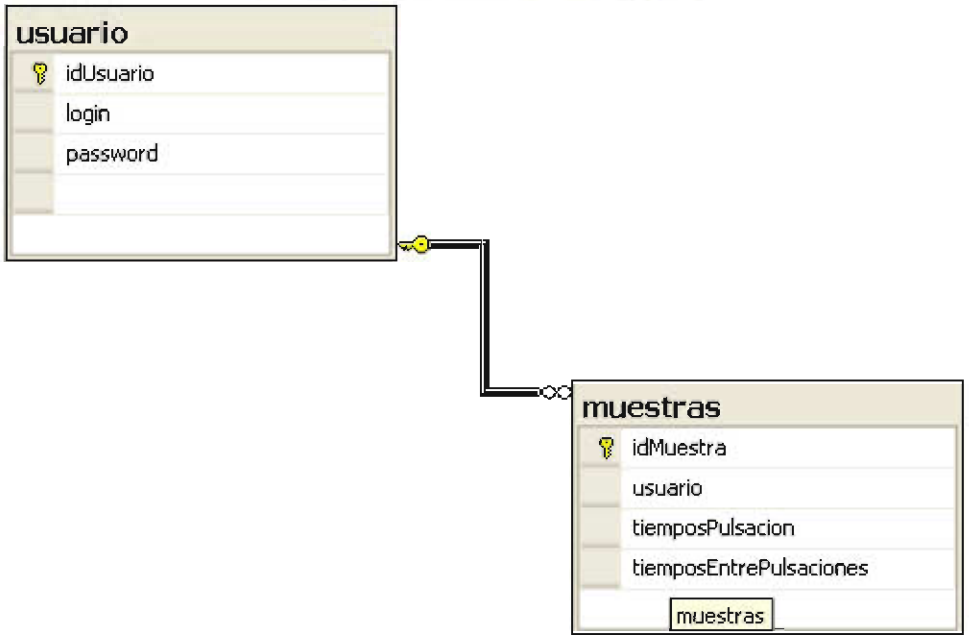


Figura 20. Diagrama de Clases de la BD

Fuente: Elaboración propia

La tabla de usuario será para la información de las claves del usuario y la tabla de muestras para almacenarlos patrones de tecleo.

3.4. DESCRIPCION FORMAL

3.4.1. PRE-PROCESAMIENTO

Dentro del pre-procesamiento se tendrá el registro de usuarios, la captura de las muestras, formatearlas, enviarlos al servidor y guardarlas en la Base de Datos.

Usuario

El trabajo actual está orientado a la población estudiantil de la Universidad Mayor de San Andrés con una población cercana a las 80.000 estudiantes de las cuales se toma como tamaño de muestra representativa a un total de 40 personas, cantidad calculada a partir de la siguiente formula.

Cálculo del tamaño de la muestra:

1) $n'=s^2/ V^2$ = Tamaño de la muestra [1] varianza de la muestra/varianza de la población

2) $n = n'/ (1+ (n'/N))$ = Tamaño de la muestra

Donde:

- N: tamaño de la población
- se: error estándar =0.047, determinado por nosotros
- V^2: es la varianza de la población al cuadrado. Su definición se^2: cuadrado del error estándar.
- p: 0.9
- n': tamaño de la muestra sin ajustar.
- n: tamaño de la muestra.

Si lo sustituimos tendremos que:

$n'=s^2/ V^2$

$s^2= p (1-p) = 0.9 (1-0.9)= 0.09$

$V^2= (0.047)^2 = 0.002209$

$n'= 40$

Posteriormente:

$n = n'/ (1+ (n'/N)) = 40 /(1 + (40/80000))= 39.98$ estudiantes= 40 Estudiantes

De donde dividiremos en dos grupos:

El primer grupo será de 30 estudiantes de la Carrera de Informática de la Universidad Mayor de San Andrés, de los cuales serán registrados su usuario/contraseña, que serán utilizados para poder hallar la TFR (Tasa de Falso Rechazo).

Segundo grupo será de 10 estudiantes a quienes se le proveerá las contraseñas de las personas registradas en el prototipo, para que puedan realizar el proceso de autenticación haciéndose pasar como usuarios legítimos y de esta manera poder hallar la TFA(Tasa de Falsa Aceptación)

Registro de usuario

Se registraran al primer de grupo de estudiantes las cuales son 30 usuarios que se muestra a continuación en la (tabla1).

Tabla 1. Registro de Usuarios

idUsuario	login	password
1	carlos	8fbbf95f1e5678899cb285b6051846a7
2	ehyci	504fb4b7c9ec92f405c41d185e36d8b9
3	lincey	785123d0cd67e6c21d64781aabd443af
4	janeth	3cae701d656b81f04c93ea112d6f0dc0
5	mario	0df746664bcf6996bb8e6e0db13746a5
7	edgar	45720d24da248f4ff888128054457a00
10	mery	4defc9b4d24be054ad885ea6d54304c1
11	gabriela	788aa784bd7c21f9529a9d64e25876d4
12	henry	b32ede3c88919230b67cf0bd9fdb93c2
14	victor	f30992da54715e5a0c4a7eaf29889641
15	dennis	aca2fb7458d2a3021110072e54d87c16
17	sergio	4ef573110dcf7579a30e91041b6e25a3
19	maritza	5369edec9168aa6dd41eca52f9d68416
20	kenia	105a31f87d017145edcb8de3021d15d6
22	clara	5b9c5f4cb58f731a470d7864d14199eb
24	rodrigo	a51572a48786a8792dbe8371c628e4ac
25	carla	9ddd712f24a7f57646411aeb3a51fb07

Criptografía

Una vez que el usuario ha introducido todos sus datos de manera satisfactoria durante el proceso de registro, el modulo criptográfico toma como entrada la contraseña haciendo uso del algoritmo MD5[39] el cual es almacenado en la Base de Datos para evitar tener contraseñas guardada en texto claro. Cuando el usuario intente autenticarse, nuevamente el modulo criptográfico toma de entrada la contraseña que también esta encriptado y la compara con la contraseña que esta almacenada en la BD, si estos coinciden, se continua el proceso de verificación biométrica, de lo contrario se deniega el acceso.

Se tendrá el registro de usuario la cual se muestra en la siguiente (figura 21).

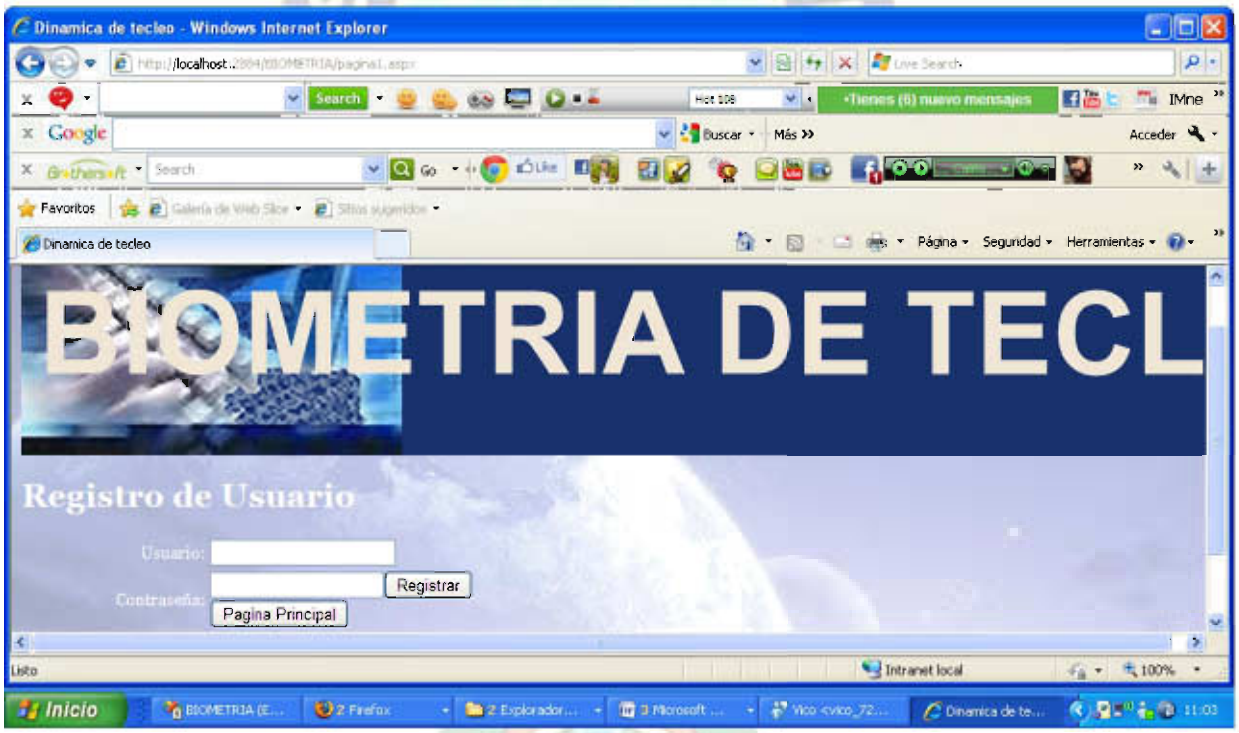


Figura 21. Diseño del método de vistas de Registrar usuario

Fuente: Elaboración propia

[39] **MD5** (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumeu del Meusaje 5) es uu algoritmo de reducciou criptográfico de 128 bits ampliamente usado.

Ingreso de muestras

Ya teniendo registrado a nuestro primer grupo de estudiantes en la base de datos, se realizaran el ingreso de muestras de patrones de tecleo de la contraseña y mediante la captura del tiempo de pulsación y tiempo entre pulsaciones en milisegundos y serán almacenadas en la base de datos muestra. El contador de los tiempos del prototipo deberá ser demasiado rápido, pues entre más rápido se incremente el contador, más fácil será de capturar la dinámica de tecleo de un usuario. La medida del tiempo en cada caso será en milisegundos con una precisión de hasta cuatro cifras.

Captura de Datos del Usuario

Para la captura de datos lo que haremos será crearnos vectores una de tiempos de pulsación, letras pulsadas y tiempo entre pulsaciones. Posteriormente realizaremos dos funciones en javascript la primera será la de tecla pulsada donde capturaremos la letra que nuestro usuario esta tecleando con el evento event.keyCode que captura los caracteres alfanuméricos ya sea mayúscula o minúsculas. Y dentro de esto también capturaremos el tiempo de pulsación utilizando la clase new date que capturara el tiempo actual.

La otra función es la de tecla soltada donde obtenemos el tiempo actual y sacamos la diferencia para saber el tiempo de pulsación de la tecla. Dentro de esto utilizamos la tres variables, una que le llamaremos tiempo final donde obtendremos el tiempo actual, otra variable tiempo inicial q capturamos en la anterior función y por ultima la variable diferencia donde restamos el tiempo final menos el tiempo inicial y de esta manera obtenemos el vector de tiempo de pulsación, para el vector de tiempo entre pulsaciones iniciamos la cuenta entre pulsaciones mediante la variable tiempo final.

Generación de patrones

Para la generación de los patrones de tecleo de cada usuario se realizara de la siguiente manera: por ejemplo tomemos la palabra MARAVILLA, para la biometría de tecleo tenemos q tomar las siguientes muestras:

- TIEMPO DE PULSACION: TP
- TIEMPO ENTRE PULSACIONES: TEP

M		A		R		A		V		I		L		L		A
	TE		TE		TE		TE		TE		TE		TE		TE	
TP		TP		TP		TP		TP		TP		TP		TP		TP

Tomaremos una muestra para el tiempo de pulsación de cada letra y el tiempo entre pulsaciones. Para generar nuestro patrón tomaremos 10 muestras de la palabra clave MARAVILLA escritas por nuestro usuario, cada una de las muestras tendrá (2*n)-1 posiciones siendo n el número de caracteres de la palabra.

P = (2*n)-1

- P= posiciones que tendrá el vector
- n=numero de caracteres de la palabra

P= (2*9)-1

En este caso cada muestra o vector que guardamos tendrá 17 posiciones:

Posteriormente se tendrá 10 muestras o vectores:

Palabra (Contraseña): MARAVILLA

Vectores de Muestras:

[TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1, TEP1, TP1]

[TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2, TEP2, TP2]

.

.

.

.

.

[TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10, TEP10, TP10]

Una vez obteniendo las muestras introducidas por nuestros usuarios, tendremos que obtener un vector con las medias de cada posición y otra con las varianzas de cada posición.

$$\mu 0 = 1/N \sum_{i=1}^{n} TP_i$$

$$\mu 1 = 1/N \sum_{i=1}^{n} TEP_i$$

.

.

.

$$\mu_{(2*n)-1} = 1/N \sum_{i=1}^{n} TP_i$$

Vector de las medias de cada posición:

$\mu = [\mu 0, \mu 1, \mu 2, \ldots\ldots\ldots, \mu (2*n)-1]$.

Donde:

- μ= es la media
- N= tamaño de la muestra

Posteriormente:

$$\sigma_0^{2-} = 1 / N * \sum (TP_i - \mu 0)^2$$

$$\sigma_1^2 = 1 / N * \sum (TEP_i - \mu 1)^2$$

.

.

$$\sigma_{(2*n)-1}^2 = 1 / N * \sum (TP_i - \mu(2*n)-1)^2$$

Vector de las varianzas de cada posición

$\sigma_0^2 = [\sigma_0^2, \sigma_1^2, \sigma_3^2, \ldots\ldots\ldots\ldots\ldots\ldots \sigma^2_{(2*n)-1},]$

Donde:

- σ= Varianza o Desviación estándar

El patrón del usuario será, por lo tanto, un vector de 11 posiciones con la media de cada uno de los tiempos de pulsación y tiempo entre pulsaciones, otro con un vector de 11 posiciones con las varianzas de cada uno de los tiempos.

Cuando ya tengamos las muestras de patrones de tecleo, realizaremos un método llamado recibir muestras en visual c#, donde ingresan como datos los vectores de letras pulsadas, tiempos de pulsación y tiempo entre pulsaciones. Dentro de este método lo que haremos será utilizar dos funciones, una formatear tiempo entre pulsaciones donde mandaremos como parámetros de entrada el tiempo y longitud dentro de esta función mediremos el tiempo de las letras pulsadas en milisegundos con la tmpSpan.Milliseconds. La otra función es la de guardar muestra donde le enviaremos los vectores de letras pulsadas, tiempo de pulsación y tiempo entre pulsaciones dentro de esta función llamaremos a otra función chequear integridad dentro de esta función lo que haremos será obtener la muestra de control es decir crear el objeto muestra y conectar con la base de datos SQL Server utilizando la clase DataTable como se muestra en la (figura 22) posteriormente guardamos los tiempos de pulsación y tiempo entre pulsaciones, con todo esto podremos guardar las muestras en la base de datos.

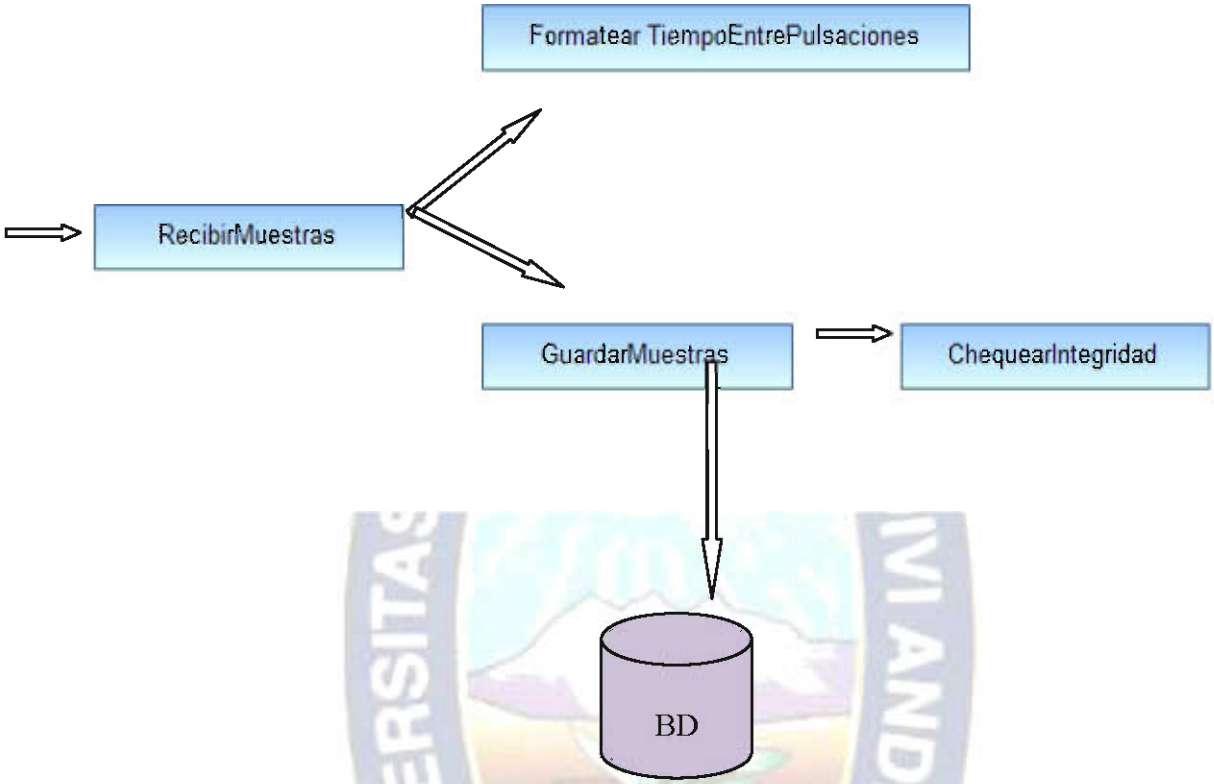


Figura 22. Diseño del método Recibir Muestras

Fuente: Elaboración propia

Ya teniendo el diseño de método recibir muestras, realizamos el diagrama de flujo de recibir muestras donde detalla cómo se reciben las muestras en el javascript creando una función guardar patrón y como se registra los tiempos de pulsación y tiempo entre pulsaciones de cada usuario.

Se utilizaran los eventos definidos de javascript los cuales son: onclick (pinchar y soltar el ratón) este evento lo utilizaremos al hacer click en el botón guardar muestra, el evento onkeydown (pulsar una tecla sin soltar) y el evento onkeyup (soltar una tecla pulsada) estos eventos lo utilizaremos en el momento de teclear en el textbox de contraseña.

Por lo tanto el diagrama de flujo del pre-procesamiento será lo siguiente:

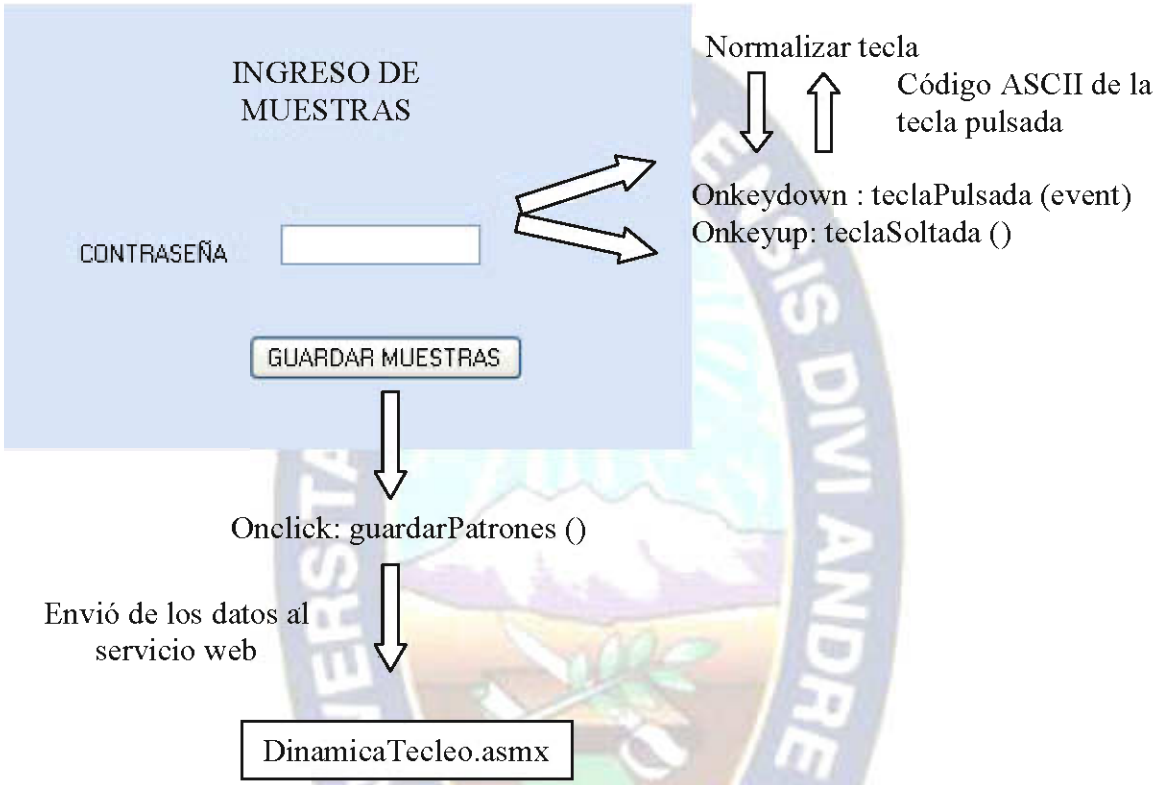


Figura 23. Diagrama de flujo de Ingresar Muestras

Fuente: Elaboración propia

Posteriormente el usuario tendrá que ingresar muestras en la interfaz web de ingresar muestras que será la que interactuara con el usuario, (figura 24.) ya teniendo las muestras se podrá pasar al procesamiento.

Figura 24. Diseño del método de vistas de Ingresar Muestras

Fuente: Elaboración propia

3.4.2. PROCESAMIENTO

Dentro del procesamiento se realizara la comprobación de usuario y determinara si tendrá acceso a una aplicación de internet.

Valoración de usuario/Contraseña

Para poder realizar la comprobación de usuario utilizaremos la tabla de muestras donde esta almacenada los tiempos de pulsación y tiempos entre pulsaciones, que se muestra a continuación (tabla 2)

Tabla 2. Muestras almacenados en la BD

idMuestra	usuario	tiemposPulsacion	tiemposEntrePulsaciones
1	1	109,78,109,188	172,359,344
2	2	187,109,110,78,78,109,110,109,78,141,63,109,63,1...	219,391,296,141,531,188,281,109,360,203,156,110,...
3	2	110,94,93,63,78,94,110,109,63,110,63,94,78,109,78	359,109,235,109,516,203,265,110,250,94,156,125,1...
4	2	109,140,93,78,78,109,141,109,109,109,78,78,79,11...	281,297,250,110,531,219,281,125,187,360,187,157,...
5	2	110,141,141,63,63,94,156,78,78,78,78,62,63,110,78	250,328,141,78,453,234,203,94,219,78,156,94,172,1...
6	2	141,156,94,78,63,110,94,62,62,78,78,110,78,78,62	265,266,172,78,547,172,218,125,172,94,141,93,125,...
7	1	141,156,109,157,93,109,109,109,78,140,109	234,250,219,93,141,109,125,110,187,141
8	2	109,109,109,110,109,94,110,110,110,78,109,109,94...	203,297,219,109,328,235,250,156,78,125,125,94,12...
9	2	110,110,110,62,62,78,110,79,78,63,78,63,78,78,109	172,250,93,78,282,203,219,140,110,140,63,140,78,1...
10	3	78,110,78,62,141,78,79	454,187,234,204,546,204
11	3	109,141,63,78,109,78,141	266,78,234,156,235,281
12	3	78,110,62,78,78,63,62	641,218,250,110,281,187
13	3	109,125,63,78,78,63,63	438,156,234,141,250,219
14	3	62,109,62,78,78,78,63	250,141,266,203,265,235
15	3	109,63,79,78,78,78,78	141,141,234,125,281,203
16	3	109,125,63,63,110,78,78	344,203,250,172,172,203

Se guardan las muestras para cada usuario separadas por comas, en una columna los milisegundos de pulsación de cada tecla y en la otra los milisegundos entre pulsaciones.

Generación de Score

Para realizar la comprobación de usuario se utilizara la función de scoring, esta será la que se encargara de determinar el grado de similitud entre la clave introducida por el usuario (contraseña) que se quiere autenticar y el patrón almacenado en la base de datos.

Para realizar la función de Scoring se tiene la siguiente fórmula:

$$S(X0)= \exp ((-1/2\ \sigma_0^2)* (X0 - \mu0)^2)$$

$$S(X1)= \exp ((-1/2\ \sigma_1^2)* (X1 - \mu1)^2)$$

.

.

.

.

$$S(X_{(2*n)-1})= \exp ((-1/2\ \sigma^2_{(2*n)-1})* (X_{(2*n)-1} - \mu_{(2*n)-1})^2)$$

Vector de los valores Score:

$S(X) = [S(X0), S(X1), S(X2),\ldots\ldots, S(X_{(2*n)-1})]$

Donde:

- S= Función de Scoring
- x= es cada uno de los tiempos de la muestras ingresadas

En la clase matemáticas definiremos esta fórmula donde la función calcular scoring recibirá como datos de entrada las medias, varianzas y muestras ingresadas, posteriormente en la clase dinámica de tecleo en la función comprobar acceso será la que se encargara de las letras pulsadas, tiempo de pulsación y tiempo entre pulsaciones antes de comparar sus muestras de los usuarios buscara si el usuario se encuentra registrado en la base de datos si el usuario no se encuentra registrado nos mostrara en mensaje de "error de acceso", caso contrario llamara a las funciones formatear tiempo entre pulsaciones donde mandaremos como parámetros de entrada el tiempo y longitud dentro de esta función mediremos el tiempo de las letras pulsadas en milisegundos con la tmpSpan.Milliseconds, la otra función

chequear muestras donde por un lado llamara a la función chequear integridad dentro de esta función lo que haremos será obtener la muestra de control es decir crear el objeto muestra y se conectara con la base de datos como muestras en la (figura 25) con la tabla muestras de estas se obtendrá los vectores letras pulsadas, tiempo de pulsación y tiempo entre pulsaciones luego calculamos la media y la varianza, también calculamos en un vector la muestra actual que ingreso el usuario el tiempo de pulsación y tiempo entre pulsaciones luego le sacamos la media, varianza a esa muestra actual que ingreso recientemente.

Posteriormente obteniendo este valor de scoring se comparara con el valor de UMBRAL definido en el prototipo y este determinara si es o no es el usuario.

Cuanto mayor sea ese umbral, mayor será la seguridad pero más falsos negativos dará y cuanto menor sea el umbral, menor la seguridad pero menos falsos negativos. Cada uno modificará este umbral para que se adecue a sus nuestras necesidades y pruebas.

Cuando pulsemos el botón acceder el prototipo devolverá un mensaje de la comprobación de usuario determinando si es o no lo es.

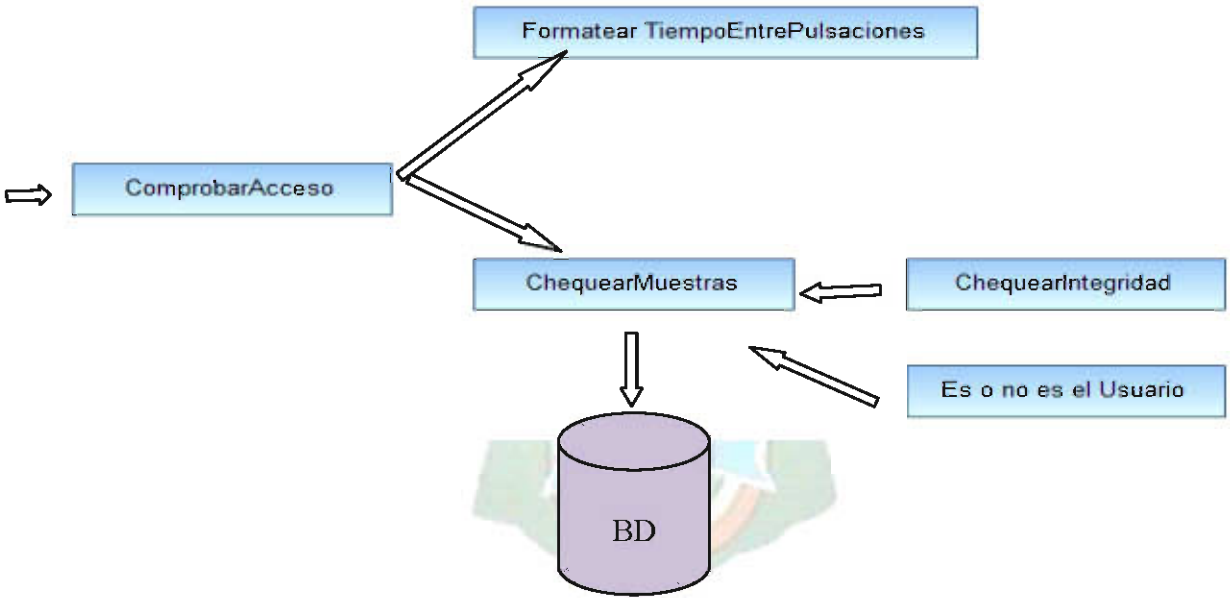


Figura 25. Diseño del método Comprobar Acceso

Fuente: Elaboración propia

Prueba de Acceso

Se utilizaran los eventos definidos de javascript los cuales son: onclick (pinchar y soltar el ratón) este evento lo utilizaremos al hacer click en el botón acceder además que llama a dos funciones creadas en javascript llamada correcta que nos mostrara una alerta que nos dirá si es o no es el usuario correcto, la otra función es la de llamada errónea que nos mostrar una alerta en el caso de que el usuario no se encuentre registrado, ambas funciones llaman a la función limpiar datos que se encarga de dejar en limpio el formulario de la pagina web , el evento onkeydown (pulsar una tecla sin soltar) y el evento onkeyup (soltar una tecla pulsada) estos eventos lo utilizaremos en el momento de teclear en el textbox de contraseña al probar el acceso.

Por lo tanto el diagrama de flujo del procesamiento será lo siguiente:

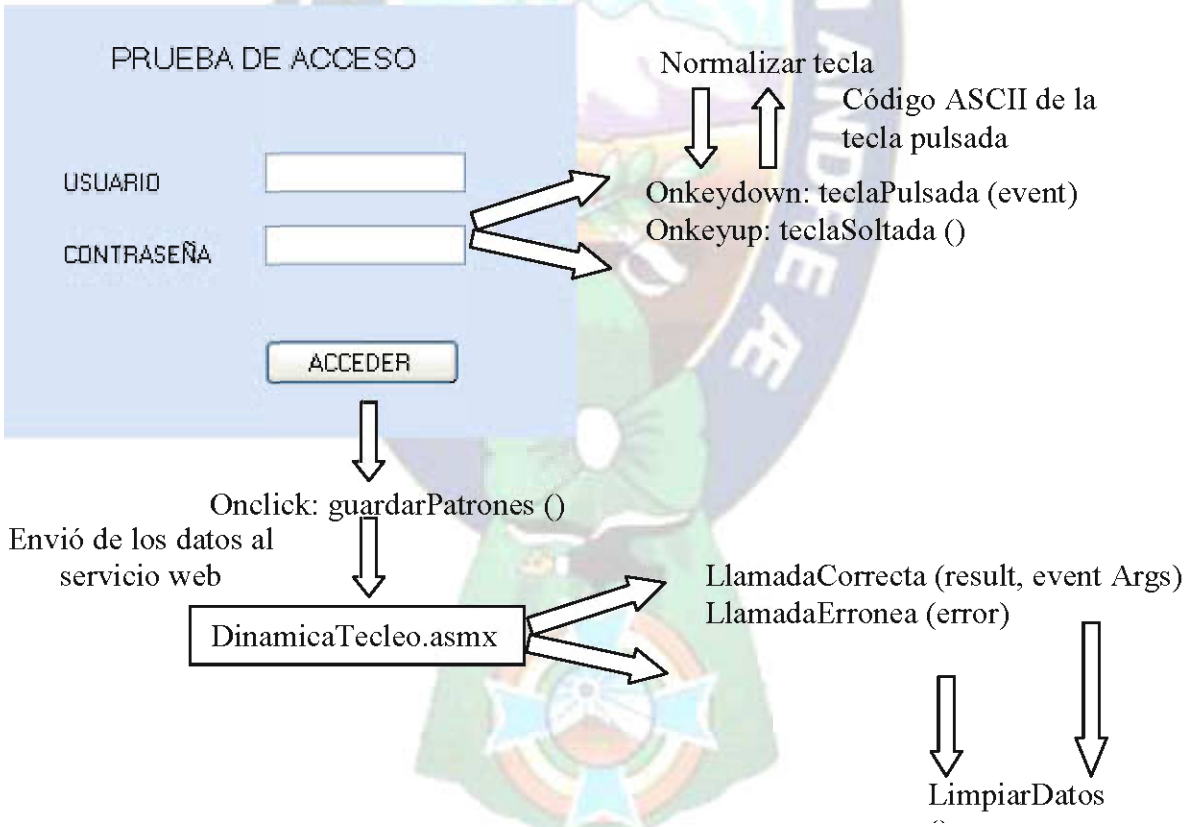


Figura 26. Diagrama de flujo de Comprobar Acceso

Fuente: Elaboración propia

Posteriormente creamos el modelo de vistas de prueba de acceso que será la que interactuara con el usuario, y este ingresar su usuario/contraseña y nos determinara si es o no es el usuario, en caso de que sea el usuario, podrá ingresar a una aplicación de internet.

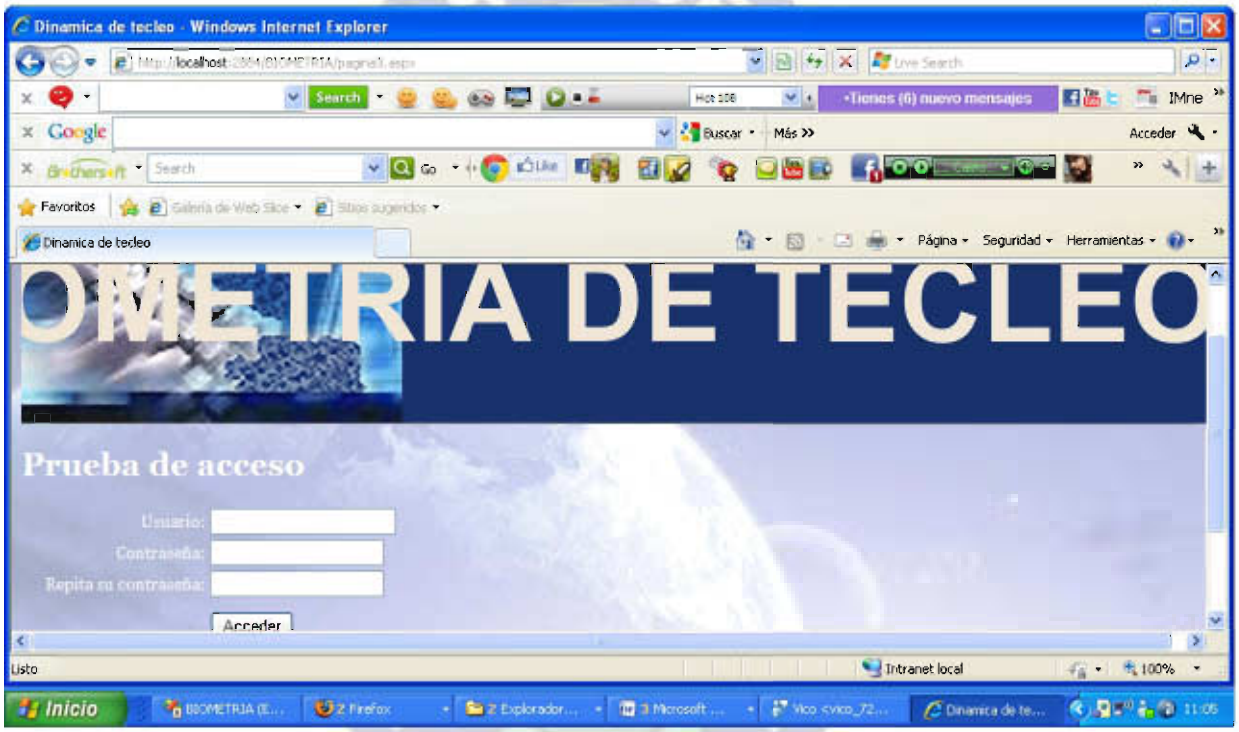


Figura 27. Diseño del método de vistas de Control de acceso

Fuente: Elaboración propia

Capítulo IV

4. PRUEBAS Y ANALISIS DE DESEMPEÑO

4.1. ESTUDIO

Un sistema biométrico típico, la persona (usuario) se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra casi todas sus características concuerdan, entonces cuando alguna persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. [Wikimedia, 2009].

Para probar el funcionamiento del prototipo se tomo en cuenta las pulsaciones de tecleo como parte principal de información biométrica de identificación, se realizo un experimento en el que se reunió a grupo de personas universitarias donde se obtuvieron la muestra de 30 usuarios de los cuales se almaceno sus pulsaciones en la base de datos, estos fueron comparados, analizados y verificados.

Con las pruebas se pretendía medir la Tasa de Falsa Aceptación (TFA) y Tasa de Falso Rechazo (TFR), por lo que el experimento se dividió en dos biometrías de tecleo. En la primera fase se les pidió a los 30 usuarios que ingresaran su usuario y contraseña, haciendo un total de 300 muestras y posteriormente realizaron la prueba de acceso del mismo, Para la segunda fase se le pidió a una persona diferente del grupo inicial, que registrara su perfil en el sistema y permitiera a cada integrante del segundo grupo observar y analizar su biometría de tecleo, así después de después cada uno de los 10 usuarios intentaría imitar su biometría de tecleo y engañar al sistema nueve veces, es decir se realizaron un total de 90 ataques.

Los usuarios podían elegir libremente la contraseña a usar, pero se les hacia la recomendación de que usaran una palabra o frase con la que estuvieran familiarizadas en su estructura y que fuera igual o mayor a ocho caracteres de longitud. El umbral de aceptación (UA) del prototipo se fijo en un 55% se decidió tomar este valor en base a los resultados, pruebas y observaciones preliminares hechas por nosotros.

El prototipo guardaba los tiempos de todos los intentos llevados a cabo por los usuarios que participaron en el estudio, esto con la intención de que después pudiéramos analizar con mayor detalle el comportamiento del prototipo. Dicho análisis consistió en comenzar a ejecutar simulaciones del mismo experimento, proporcionando como entrada al prototipo

los mismos tiempos que habían generado los usuarios previamente, pero cambiando en cada ejecución el valor de UA en intervalos de 5%, comenzando en un 5% y llevándolo hasta 100%.

4.2. RESULTADOS

Para la parte en que los usuarios interactuaron directamente con el prototipo, de los 30 intentos de autenticación que hubo por parte de usuarios legítimos, prototipo rechazo de manera equivocada un total de 2 usuarios, lo que se transforma en una TFR de 6.67 %. Respecto a los intentos de falsificación de identidad, de los 90 intentos únicamente 4 de ellos fueron exitosos, entregando una TFA con un valor del 4.44%. Las simulaciones que se hicieron nos ayudaron a calcular las curvas de TFR y la TFA, que describen el desempeño global de un sistema biométrico y además nos proporciona la Tasa de Error de Cruce (TEC) que nos indica el umbral óptimo de sensibilidad del sistema.

En el Grafico 1 podemos observar que la TEC se encuentra en una UA de alrededor de 55 %, que hace que el software funcione con una TFR y TFA de 8%.

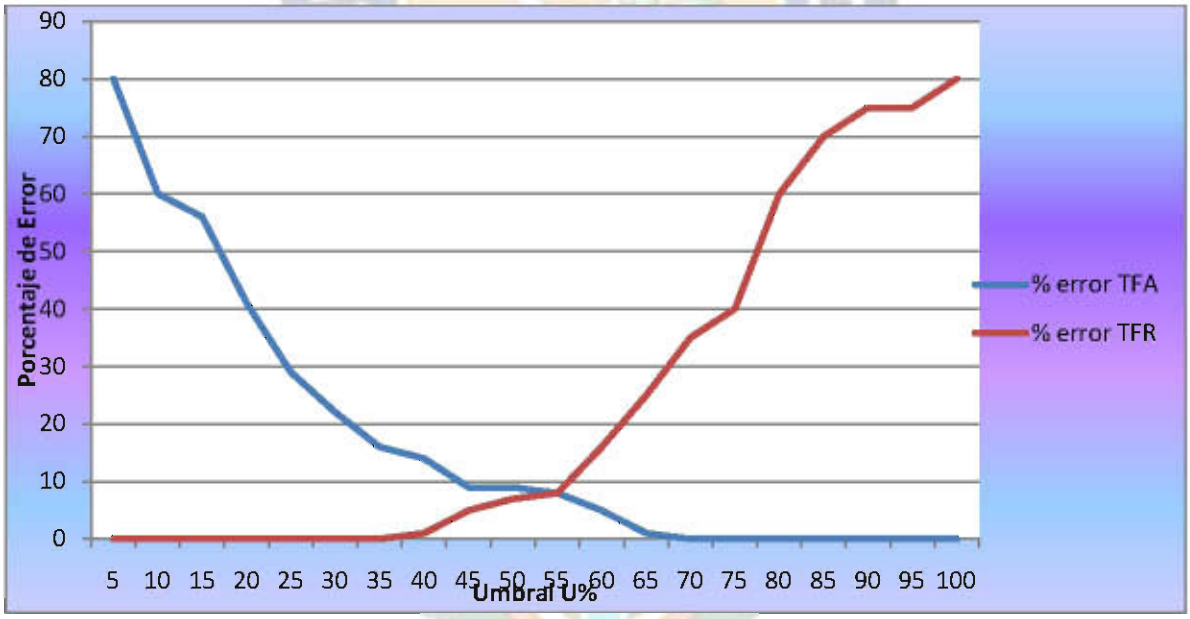


Figura 28. Datos Umbral (%) Vs Porcentaje de error (1ra Prueba)

Fuente: Elaboración propia

Posteriormente veremos cuan confiable es el prototipo y para esto se tuvo que hacer dos experimentos del prototipo y en los mismo usuarios, pasando dos semanas de la primera prueba de esta prueba lo que obtuvimos fue la siguiente (figura 29) donde podemos observar que la TEC se encuentra en una UA de alrededor de 55 %, que hace que el software funcione con una TFR y TFA de 8%.

Para esta prueba de los 30 intentos de autenticación que hubo por parte de usuarios legítimos, prototipo rechazo de manera equivocada un total de 3 usuarios, lo que se transforma en una TFR de 10%. Respecto a los intentos de falsificación de identidad, de los 90 intentos únicamente 3 de ellos fueron exitosos, entregando una TFA con un valor del 3.33%.

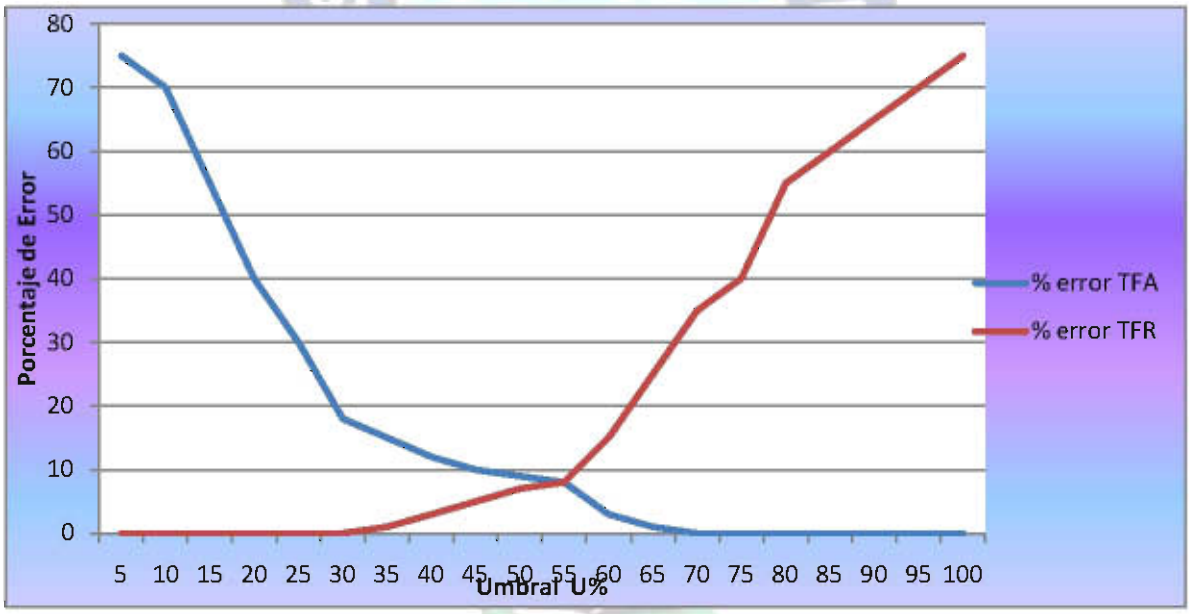


Figura 29. Datos Umbral (%) Vs Porcentaje de error (2da prueba)

Fuente: Elaboración propia

En el Grafico 3 aparecen graficados los tiempos de cada una de las 10 muestras que se tomaron de un usuario en el momento de registro (1ra Prueba). Dicho usuario pertenece al primer grupo de personas que selecciono la contraseña "SIGMA12345".

En Dicha grafica se puede apreciar fácilmente como las diez curvas siguen un patrón muy similar, lo que indica que el usuario tiene establecida una biometría de tecleo, además que la curva de línea roja es la muestra de entrada de verificación.

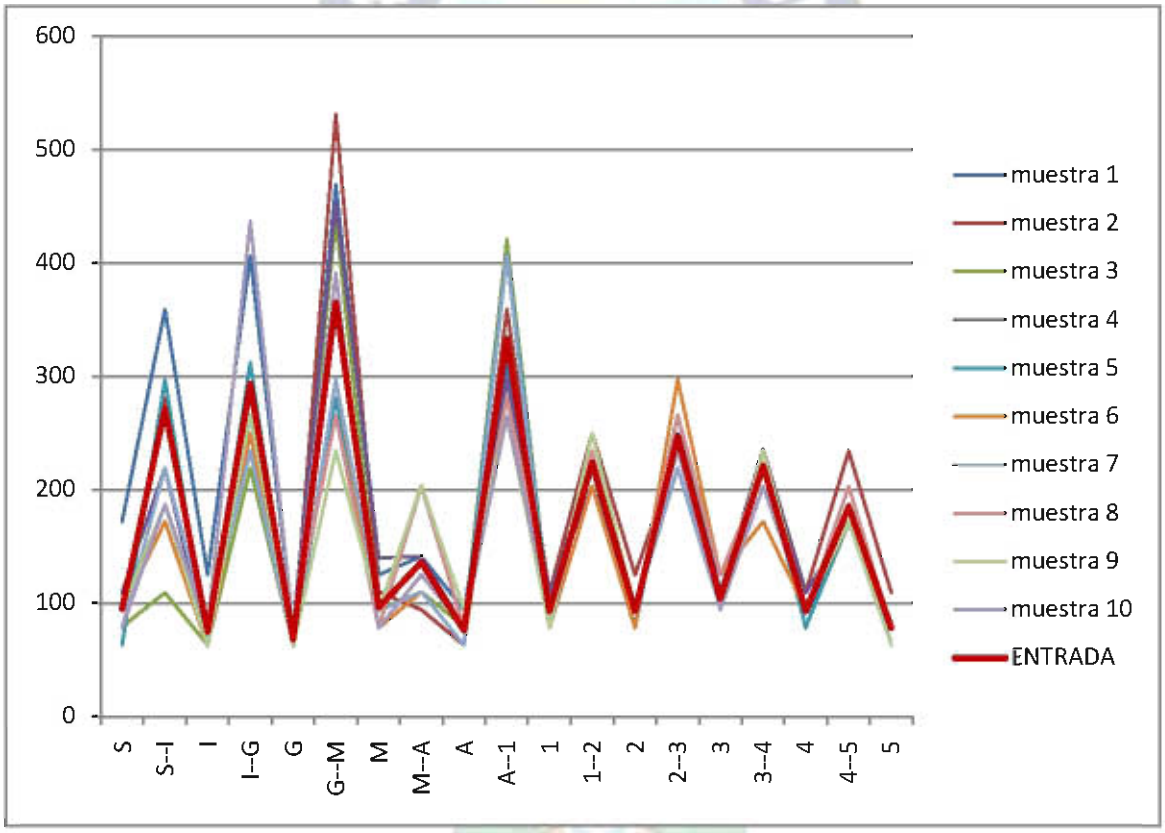


Figura 30. Muestras de un usuario del prototipo (milisegundos)

1ra Prueba

Fuente: Elaboración propia

Seguidamente en el Grafico 4 podemos observar la biometría de tecleo del usuario (2da Prueba, tomada después de 2 semanas), selecciono la contraseña "SIGMA12345", que se trata del mismo usuario que registramos anteriormente en la 1ra prueba.

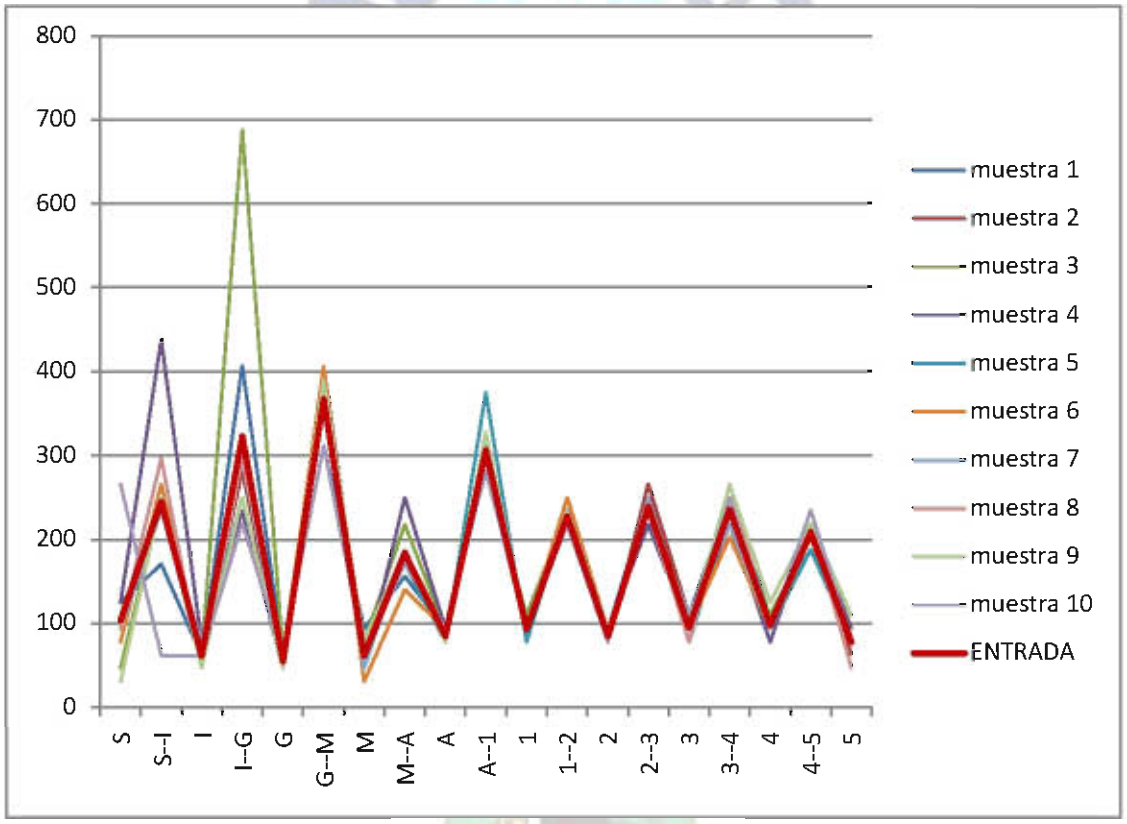


Figura 31. Muestras de un usuario del prototipo (milisegundos)

2da Prueba

Fuente: Elaboración propia

En el Grafico 5 se puede observar que el usuario sigue un mismo ritmo al teclear su contraseña y por lo tanto existe una cierta regularidad en el modo de teclear a través del tiempo.

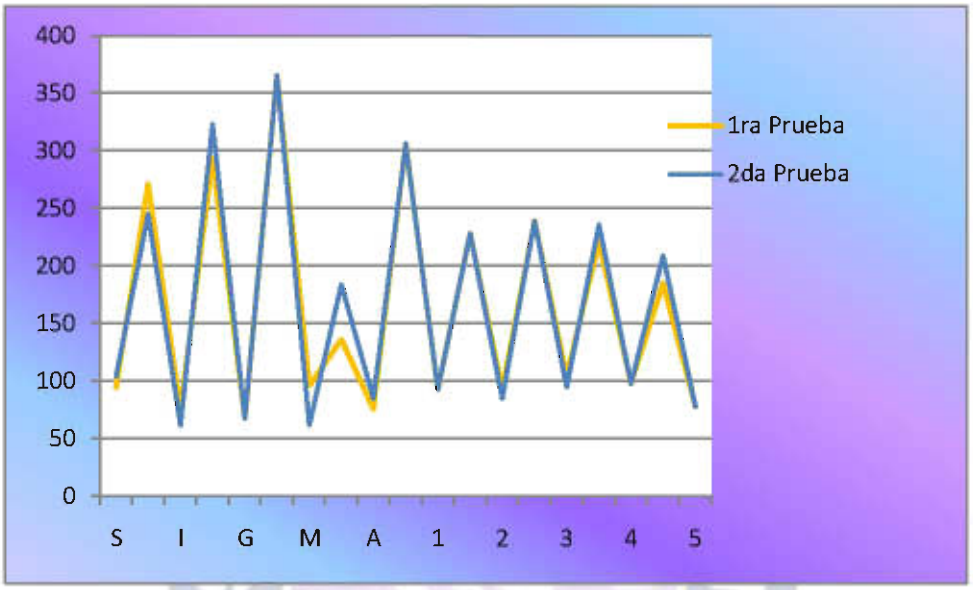


Figura 32. Muestras de Entrada de Verificación de la 1ra y 2da prueba

Observaciones que se hicieron durante la experimentación:

- Si se escoge una secuencia de dígitos que posea un tamaño mayor o igual a 8 dígitos y además que sean no correlativos aumenta la dificultad de autenticación de un falso usuario.
- Si un falso usuario observe como un usuario legitimo teclea su clave, esto no significa que obtendrá éxito al intentar pasar por ese usuario.
- La familiaridad de la secuencia de dígitos para el usuario tiene un impacto bastante significativo ya que determina su forma de tecleo.

Obtuvimos los siguientes tablas de resultados aplicando la confiabilidad [Unexpo-Confiabilidad, 2008] al desempeño del prototipo.

Tabla 3. Estimación de Coeficiente de Confiabilidad de la Tasa de Falsa Aceptación

N	x	x2	y	y2	XY
1	80	6400	75	5625	6000
2	60	3600	70	4900	4200
3	56	3136	55	3025	3080
4	39	1521	40	1600	1560
5	29	841	30	900	870
6	22	484	18	324	396
7	16	256	15	225	240
8	10	100	12	144	120
9	9	81	10	100	90
10	9	81	9	81	81
11	8	64	8	64	64
12	2	4	3	9	6
13	1	1	1	1	1
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	0	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	0	0
20	0	0	0	0	0
Σ	341	16569	346	16998	16708

Tabla 4. Estimación de Coeficiente de Confiabilidad de la Tasa de Falso Rechazo

N	x	x2	y	y2	xy
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	1	1	0
8	1	1	3	9	3
9	5	25	5	25	25
10	7	49	7	49	49
11	8	64	8	64	64
12	16	484	15	225	240
13	25	625	25	625	625
14	35	1225	35	1225	1225
15	40	1600	40	1600	1600
16	60	3600	55	3025	3300
17	70	4900	60	3600	4200
18	75	5625	65	4225	4875
19	75	5625	70	4900	5250
20	80	6400	75	5625	6000
Σ	497	30223	464	25198	27456

Posteriormente tenemos la formula de confiabilidad que es la siguiente:

$$r = \frac{N\sum XY - \sum X \sum Y}{\sqrt{\left[N\sum X^2 - \left(\sum X\right)^2\right]\left[N\sum Y^2 - \left(\sum Y\right)^2\right]}}$$

Donde:

r: Es el coeficiente de correlación entre las dos administraciones de la prueba.

N: Número de ejecuciones de umbral de aceptación.

$\sum XY$: Resultado de sumar el producto de cada valor de x por su correspondiente valor en y.

$\sum X$: Suma total de los valores de x (primera aplicación)

$\sum Y$: Suma total de los valores de y (segunda aplicación)

$\sum X^2$: Resultado de sumar los valores de x elevados al cuadrado.

$\sum Y^2$: Resultado de sumar los valores de y elevados al cuadrado.

$\left(\sum X\right)^2$: Suma total de los valores de x, elevados al cuadrado.

$\left(\sum Y\right)^2$: Suma total de los valores de y, elevados al cuadrado.

Aplicando la Formula de Confiabilidad se obtiene los siguientes resultados:

Tasa de Falsa Aceptación

$$r = \frac{20\,(16708) - (341)\,(346)}{\sqrt{[20(16569)-(341)^2][20(16998)-(346)^2]}}$$

$$r = \frac{216174}{237656.2982}$$

$r = 0.91$

Tasa de Falso Rechazo

$$r = \frac{20\,(27456) - (497)\,(464)}{\sqrt{[20(30223)-(497)^2][20(25198)-(464)^2]}}$$

$$r = \frac{318512}{354441.4742}$$

$r = 0.90$

Como se puede observar la r=0.91 y r=0-90, este resultado indica que existe una correlación "muy alta" entre las pruebas de la y segunda medición, lo cual equivale a decir que el prototipo analizado en confiable, en cuanto a la estabilidad a través del tiempo.

Capítulo V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- De acuerdo a la hipótesis planteada que dice "La biometría de tecleo de la contraseña del usuario mejora la seguridad de acceso en aplicaciones de internet." se definió los objetivos específicos y el objetivo general "Desarrollar un prototipo biométrico de tecleo de la contraseña del usuario para mejorar la seguridad de acceso en aplicaciones de internet." con el fin de demostrarla.

- En el transcurso del desarrollo del presente trabajo se utilizo el método estadístico descriptivo que hizo uso de los parámetros estadísticos de media y varianza.
- La demostración fue medida por medio de la métricas de rendimiento las cuales fueron la Tasa de Falsa Aceptación (TFA), la Tasa de Falso Rechazo (TFR) con los cuales se pudo encontrar la Tase de Error de Cruce que nos muestra el desempeño del sistema, además teniendo estos datos se puedo determinar la confiabilidad del prototipo y probar la hipótesis planteada con lo que queda demostrada este aporte para mejorar los sistemas de información en la red de internet.
- Se realizo el cumplimiento de los objetivos específicos con el desarrollo del prototipo biométrico que permiten validar la identidad del usuario mediante datos históricos en base a su pulsación de tecleo.
- La principal ventaja que se presento en el prototipo biométrico es que prevé una segunda capa de seguridad, fortaleciendo las aplicaciones de internet basadas en usuario y contraseña.
- Actúa de manera transparente para el usuario durante la etapa de autenticación, además el prototipo biométrico es de bajo costo ya que no lleva hardware adicional solo trabaja con el teclado común que lleva toda computadora con lo que los usuarios están familiarizados.

- La desventaja que se presento radica en la etapa de registro de usuario, ya que para algunos de ellos puede llegar a ser tedioso el escribir en repetidas ocasiones su contraseña.

5.2. RECOMENDACIONES

Habiendo demostrado la utilidad de la hipótesis planteada considero importante que este tipo de biometría se incluya en la seguridad de las tarjetas inteligentes ya que dentro de lo que es la transferencia de datos trabaja con encriptación pero podamos incluir una segunda capa de seguridad con lo que es la biometría de tecleo, donde registre las pulsaciones de tecleo del usuario y de esta manera la transferencia de su información sea más segura con la que no pueda permitir "intrusos" en la transacción.

También se recomienda que el prototipo desarrollado debiera modificarse para que sea tolerante a los errores de escritura tanto en el proceso de registro como en el de autenticación. Además que el prototipo desarrollado en la presente tesis podría ser implementando como un sistema de autenticación biométrico en la gran variedad de sistemas que tengan contraseña.

REFERENCIAS BIBLIOGRAFICAS

Libros

1. Gento Samuel, "Taller de Tesis". Modulo 8. UNED, Facultad de Educación, Madrid. 2003; #Paginas 500.
2. Hernández R., Fernández C., Baptista P. "Metodología de la Investigación". Cuarta Edición. México D.F. 2008; #Paginas 800.
3. Sobre la caracterización de distribuciones de probabilidad subyacentes al scoring; Sergio López Hernández; Directores: Fernando Díez Rubio y Antonio Cuevas González Madrid, Septiembre 2010; #Paginas 350.
4. "Evaluación de las técnicas diagnósticas: Análisis estadístico"; Margarita Núñez Escuela Universitaria de Tecnología Médica UdelaR, Montevideo, Uruguay Comité de Tecnólogos de ALASBIMN 2008; #Paginas 270.

Artículos científicos

1. Monrose F., Aviel D. R. "Keystroke dynamics as a biometric for authentication". Future Generation Computer Systems. 2007.
2. Matthew A. T., Alex P. P. "Face Recognition Using Eigenfaces". 1991.
3. Cheng-Huang J., Shiupyng S., Jen-Chien L., "Keystroke Statistical Learning Model for Web".National Chiao Tung University. Taiwan. 2006.
4. Aguilar, H. J. G., Lizama P. L. A. "Autenticación Biométrica por dinámica de tecleo". División Académica de Informática y Sistemas. México. 2006.
5. Anil K. J., Arun R., Salil P. "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology .2004.
6. Araujo C. "Autentificación Personal por *Dinámica* de *Tecleo* Basada en Lógica Difusa", Brazil. 2004.
7. Ashbourn J. "Biometrics: Advanced Identity Verification". Spring. 2000.
8. Carl S., Moran T., "The Keystroke level model for User Performance time with interactive system", 1980.
9. James Wayman, et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).
10. John D. Woodward, "El Teclado de la Computadora"(Mexico D.C., 2011)

11. Huidobro J M. "Técnicas de Seguridad Biométricas". Perspectiva Empresarial. 2006.
12. Jerez L. C. A. "Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet". 2002.
13. Technology watch, "Biometría y Normas internacionales",2010.
14. Noticias de Bolivia online "CNE garantiza padrón biométrico y comicios electorales", 2009.
15. Infoleyes Bolivia, "constitución Política del Estado", 2011.
16. Ormachea Jorge "Seguridad en los Sistemas Biométricos". Visión Nacional, 2008.
17. John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

Tesis consultadas

1. Hung-i Kuan "Tipificacion Dinamica de Seguridad Informatica System", (Tesis Licenciatura); 1992.
2. Flores Ronald "Sistema de autentificación basado en biometría dinámica de tecleo", (Proyecto de Grado); 2011
3. Borghello A. S. S., Fabian C. "Seguridad Informática: Sus implicancias e Implementación" (tesis licenciatura). Argentina: Universidad Tecnológica Nacional; 2001.

Direcciones de Internet

1. Sanchez MJI. Gorrotxategi ZG. Garaizar SP. "Seguridad Informática". Disponible en: http://www.e-ghost.deusto.es/docs/articulo.seguridad.pdf. Consultado en fecha: 13 de Marzo del 2011.
2. Granger S. 2001. "Social Engineering Fundamentals, Part I: Hackers Tactics". Disponible en: http://securityfocus.com/print/infocus/1527. Consultado en fecha: 2 de Marzo del 2011.

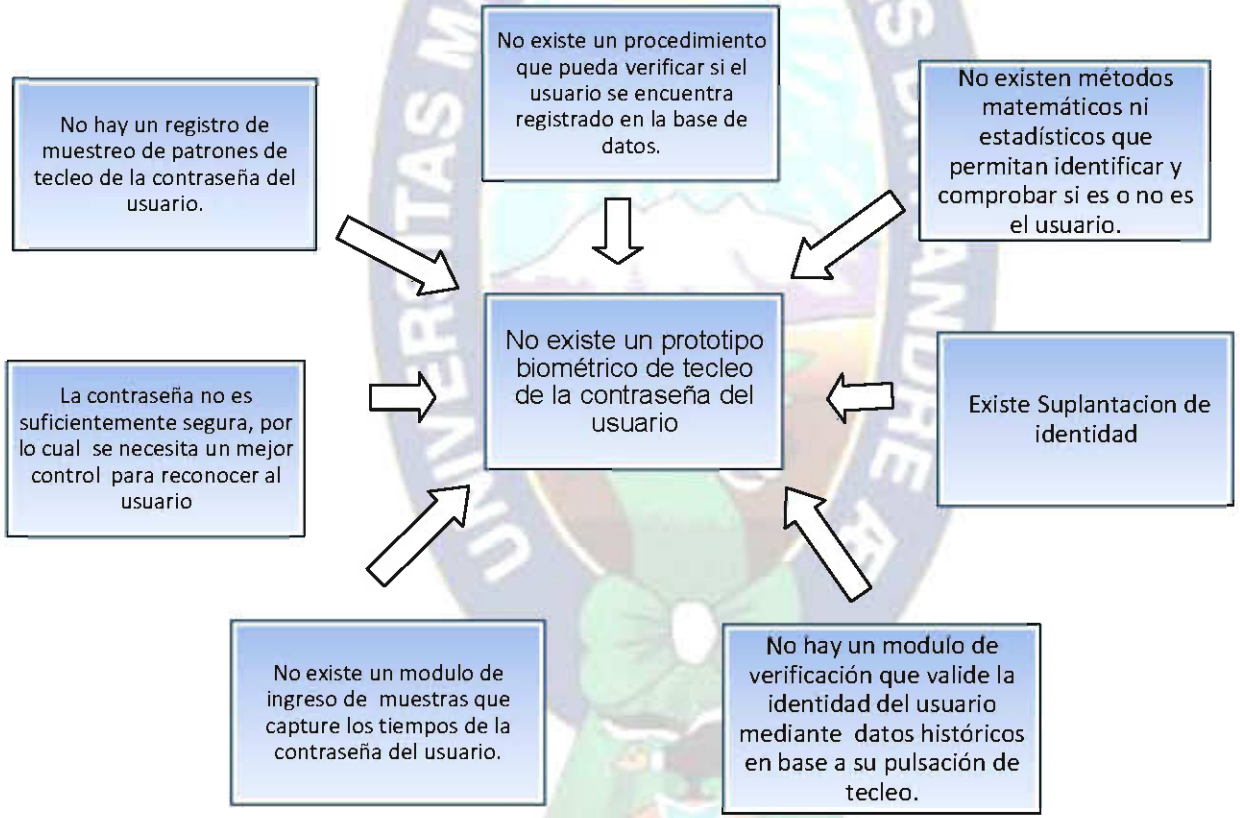
3. Spaltro JL. 2007. "Inteligencia Biométrica".
Disponible en: http://www.info-resumendeseguridad.inteligencia-biomtrica.html.
Consultado en fecha: 4 de Marzo del 2011.
4. Comunicaciones World. "De lo físico a los lógico, Seguridad Biométrica". Disponible en: http://www.idg.es/Comunicaciones/impart.asp?id=143403. Consultado en fecha: 2 de Marzo del 2011.
5. Wikipedia. 2004. "Biometría".
Disponible en: http://es.wikipedia.org/wiki/BiometriaDa.
Consultado en fecha: 18 de Marzo del 2011.
6. Wikipedia. 2005. "Autenticación".
Disponible en: http://es.wikipedia.org/wiki/Autenticaci%C3%B3n.
Consultado en fecha: 16 de Marzo del 2011.
7. Wikipedia. 2007. "Seguridad Informática".
Disponible en: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica.
Consultado en fecha: 11 de Marzo del 2011.
8. Sistemasbiometricos.over.blog.com "Biometría de tecleo".
Disponible en: http://sistemasbiometricos.over-blog.com/article-biometria-de-tecleo-62146267.html.
Consultado en fecha: 1 de diciembre de 2010.
9. Ing. Marcelo Semeria. "Dinámica de tecleo, Algoritmos Especiales".
Disponible en: http://www.biometria.gov.ar/media/9952/UAI.pdf.
Consultado en fecha: 2008.
10. Allmysoft. 2007. Software BioKeyLogon.
Disponible en: http://www.allmysoft.com/download-biokeylogon-software.html.
Consultado en fecha: 10 de Marzo del 2011.
11. "Tipos de Teclado Especiales".
Disponible en: http://foro.elhacker.net/hardware/tipos_de_teclado-t176326.0.html.
Consultado en fecha: 14 de Agosto de 2007.
12. "El Teclado de la Computadora".
Disponible en: http://www.informaticamoderna.com/Teclado.htm. .
Consultado en fecha: 20 de junio del 2011.

13. López Hernández "Nomas Jurídicas de Biometría"
Disponible en: http://www.eps.uam.es/esp/alumnos//Lopez_Hernandez_Sergio.pdf; Barcelona, octubre de 2001. .
Consultado en fecha: 22 de junio del 2011.
14. "Biometría "
Disponible en: http://es.wikipedia.org/wiki/Biometr%C3%ADa. .
Consultado en fecha: 30 de julio del 2011.
15. "Metodologías de Investigación"
Disponible: http://www.definicionabc.com/ciencia/metodologia.php. . Consultado en fecha: 25 de agosto del 2011.
16. "Características de ASP.NET"
Disponible en: http://es.wikipedia.org/wiki/ASP.NET. . Consultado en fecha: 30 de agosto del 2011.
17. "Método científico " Disponible en : http://es.wikipedia.org/wiki/Mario_Bunge. . Consultado en fecha: 1 de septiembre del 2011.
18. "concepto de Metodología" Disponible en: http://www.misrespuestas.com/que-es-una-metodologia.html. . Consultado en fecha: 4 de septiembre del 2011.
19. "Seguridad Informática "
Disponible en: http://www.slideshare.net/jemarinoi/seguridad-informtica-1125964.
Consultado en fecha: 10 de septiembre del 2011.

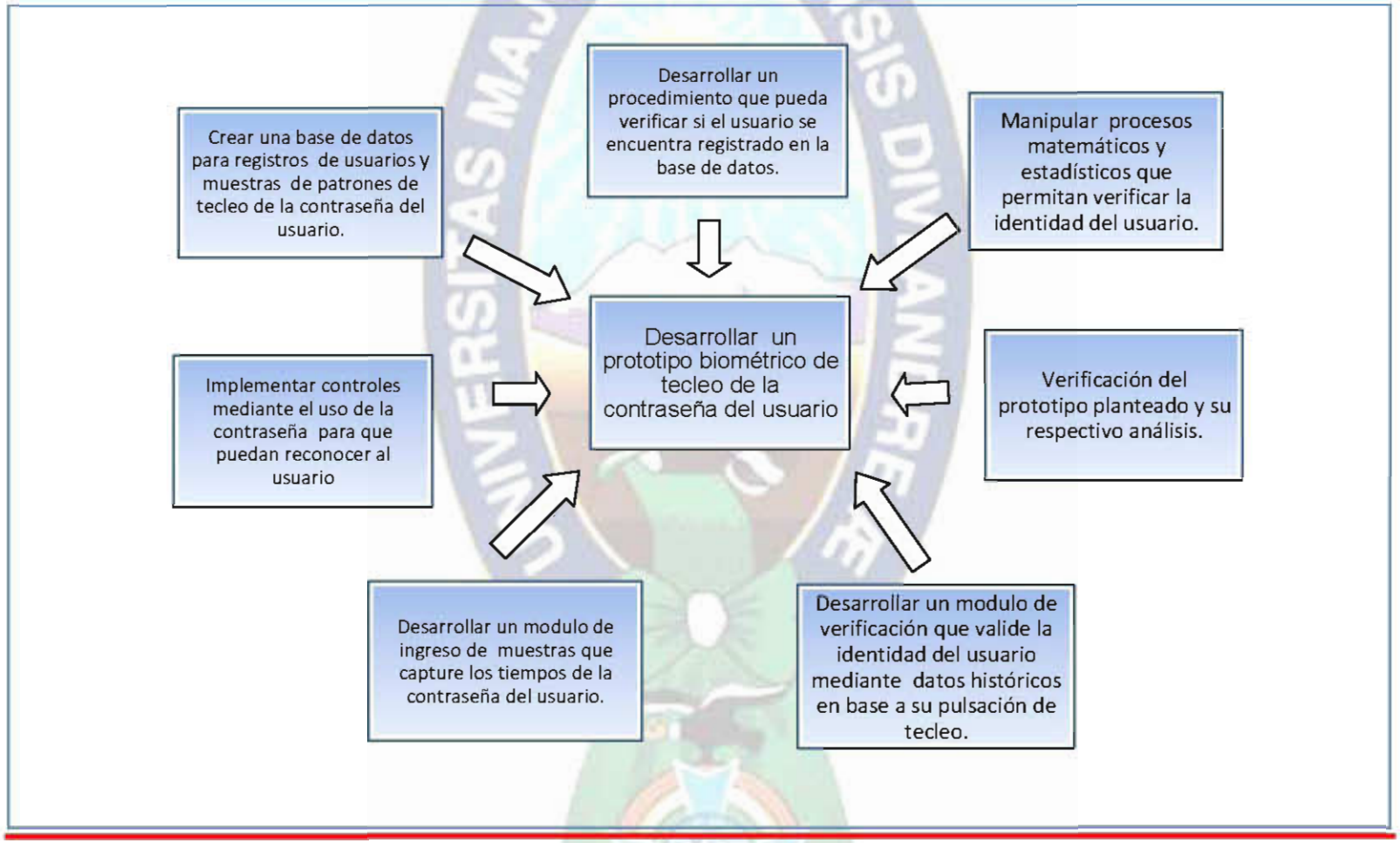
Anexos

ANEXOS

ANEXO A: ARBOL DE PROBLEMAS



ANEXO B: ARBOL DE OBJETIVOS



Documentación


UNIVERSITAS MAJOR PACENSIS DIVI ANDRE Æ