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


TESIS DE GRADO

# “AUTENTICACIÓN BIOMÉTRICA PARA USUARIOS DE CELULARES MEDIANTE DINÁMICA DE TECLEO”

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN INGENIERÍA DE SISTEMAS INFORMÁTICOS

POSTULANTE: UNIV. ALVARO JAVIER MEDINA BALBOA

TUTOR: LIC. ROBERTO VARGAS BLACUTT

REVISOR: LIC. EDGAR PALMIRO CLAVIJO CARDENAS

GESTION: 2010

## INDICE GENERAL

**Título** **Página**

***Agradezco:***

- *A Dios por acompañarme día a día.*
- *Al Lic. Roberto Vargas Blacutt mi tutor y al M. Sc. Edgar Clavijo Cárdenas mi revisor por su comprensión, confianza y apoyo.*
- *A mis compañeros de la carrera de Informática que siempre me apoyaron en todo momento.*
- *A los docentes que me formaron en la carrera de Informática y a la Universidad Mayor de San Andrés*

***Dedicado:***

*Al amor, comprensión, confianza y apoyo de mis Padres Pedro y Elsa, de mis hermanos Ignacio e Iver, de mi pareja Naty y de mi hijo Javier Omar para poder culminar la presente tesis.*

# INDICE DE TABLAS Y FIGURAS

# RESUMEN

Este trabajo de tesis se realizó con el objetivo de encontrar patrones de tecleo asociados a usuarios de teléfonos celulares mediante la aplicación de la dinámica de tecleo para poder hallar indicadores de tasas de error que nos aseguren la aplicación de dicho método en el proceso de autenticación en los teléfonos celulares mediante el ingreso del número PIN.

La principal problemática que se encontró para la realización de la presente tesis fue ¿Es posible encontrar algún mecanismo de protección que pueda reforzar el proceso de autenticación en los teléfonos celulares mediante el ingreso del número PIN para poder evitar la intromisión de cualquier otra persona que no sea el usuario auténtico?.

El plan de trabajo de la presente tesis aplicó el método científico enmarcándose en un diseño cuasi-experimental por lo que se desarrollo un prototipo bajo el lenguaje de programación J2ME, utilizado para el desarrollo de aplicaciones móviles, que luego de ser previamente instalado en un teléfono celular Sony Ericsson F305, se procedió a la fase de experimentación, en donde se aplicó dicho prototipo a una población de 90 personas entre estudiantes universitarios y personas particulares como ser administrativos y demás, todos ellos pertenecientes a la Universidad Mayor de San Andrés.

Los resultados obtenidos una vez concluido la fase de experimentación fueron satisfactorios y prometedores, obteniendo indicadores: para la Tasa de Falsa Aceptación 5%, para la Tasa de Falso Rechazo 8.75% y para la Tasa de Error de Cruce 8%. Lo cual afirma que se puede aplicar la dinámica de tecleo como un método de Autenticación Biométrico en los teléfonos celulares, y de esa manera poder implementar medidas de seguridad confiables.

## 1.1.- INTRODUCCIÓN

Desde la invención del celular en el año 1973, por el estadounidense Martín Copper [Mundo Virtual, 2008], fue percibido como un aparato para comunicarnos con otras personas, hoy en día este producto puede brindarnos un sin fin de servicios, como procesamiento de textos, reproducción de audio y video, algún tipo de entretenimiento como los juegos, incluso alguno que otro celular lleva consigo un sistema operativo propio, una agenda para registrar reuniones y otros.

Pero toda nueva tecnología trae consigo problemas inéditos, y en el caso de los celulares una de las principales dificultades que los acompaña es la seguridad. Estos problemas de seguridad abarcan cuestiones como vulnerabilidades en los protocolos de comunicación inalámbrica como el bluetooth[1] y mecanismos de autenticación y protección de datos débiles dentro del celular. Respecto al primer punto se han estado haciendo grandes esfuerzos durante los últimos años para mejorarlo, pero en cuanto al segundo no se ha considerado lo crítico que es.

La autenticación juega un papel muy importante en la seguridad informática, ya que por definición, a los usuarios autentificados se les permite el acceso a los recursos del sistema.

En los dispositivos móviles estos recursos pueden ser elementos confidenciales como direcciones, teléfonos, correos electrónicos, cuentas bancarias y contraseñas, e incluso accesos a redes remotas, lo cual pondría en peligro los recursos de terceros.

[1] El *bluetooth* es una tecnología bastante potente y útil para la transmisión de datos y voz (manos libres del coche), pero su nivel de seguridad no lo es tanto, y depende en cierta medida del uso adecuado que haga el usuario de ella

Todo lo antes expuesto es lo que motivó la realización del actual proyecto de tesis, el cual pretende desarrollar un prototipo capaz de reconocer dinámicas de tecleo y que pueda trabajar en conjunto, de forma transparente, con los tradicionales sistemas de autenticación basados en nombre de usuario y contraseña, y fortalecer la seguridad proporcionada por éstos últimos.

El resto de esta tesis está organizado como sigue: en el Capítulo 1 se detallan los trabajos anteriores realizados a la presente tesis, se plantea la principal problemática que aquejan los usuarios de celulares, se plantean los objetivos principales y secundarios que se pretenden alcanzar, se justifica la principal motivación para realizar la tesis, se plantea la hipótesis identificando las variables independientes y dependientes, finalmente se plantea los alcances y limites. En el Capítulo 2 se introduce la Biometría y sus divisiones. El Capítulo 3, está dedicado al diseño metodológico utilizado en la presente tesis y los diferentes mecanismos que se usaron para probar la hipótesis planteada en la presente tesis, al mismo tiempo también se hace referencia al desarrollo del prototipo. Finalizando la tesis se plantean las conclusiones generales de la presente tesis, al mismo tiempo se hace referencia a los trabajos futuros.

A futuro se espera que la presente tesis sea una motivación para seguir investigando en el campo de los métodos biométricos de comportamiento que durante mucho tiempo han sido relegados, tal es el caso de la dinámica de tecleo cuya aplicación en nuestra realidad apenas está comenzando a tomar importancia.

## 1.2.- ANTECEDENTES

En 1860 los primeros telégrafos [Wikipedia, 2009] eran utilizados para el envío o transmisión a distancia de información encriptada[9] en un sistema de códigos llamado Morse [Wikipedia, 2008]. El sistema se basa en una serie de pulsaciones de combinaciones de líneas y puntos los cuales posteriormente son traducidos a letras. Se ha conocido que las personas que han utilizado el telégrafo desarrollaban un "estilo telegráfico" [Gaines SR, Lisowsky W, Press JS, Shapiro N, 1980] que era distintivo, así muchos operadores de radio cuando recibían un mensaje sabían cual de sus amigos estaba enviando el mensaje, antes de que llegara la identificación del emisor del mensaje.

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[10] 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.

[9] La encriptación es el proceso para volver ilegible información considera importante La información una vez encriptada sólo puede leerse aplicándole una clave
[10] La RAND Corporation es una institución sin fines de lucro que ayuda a mejorar la política y la toma de decisiones a través de la investigación y el análisis

El programa que utilizaron para capturar el tiempo de pulsación de la teclas, lo hacia midiendo el tiempo entre cada par de letras sucesivas llamados también "digráfos[11]", 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, mismos que arrojaron resultados de una Tasa de Falsa Aceptación de 0% y una Tasa de Falso Rechazo 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 [Bowers, Hansen, 2006] que es usado para medir la similitud entre vectores. Como resultado de sus estudios obtuvo una Tasa de Falsa Aceptación de 0.01% y una Tasa de Falso Rechazo de 50%.

[11] digráfo, secuencia de cadena constituida por 2 caracteres unidos, ejemplos "ae", "on", "ra", "tr", otros

En 1988 Leggett J. y Williams G. [Umphress, Williams, 1985] replicaron el experimento que Gaines et Al 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 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 almacenó en una matriz de latencias 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 Tasa de Falsa Aceptación de 5.0 % y una Tasa de Falso Rechazo 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 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 Tasa de Falsa Aceptación de 0.25% una Tasa de Falso Rechazo 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, conocidas como análisis de factor, calculando dígrafos y logrando desempeños globales del clasificador con porcentajes de 83.22% hasta un 85.63%.

En 2004 en Brasil, Araujo [Araujo, 2004] realizo un trabajo acerca de la autenticación de personal utilizando un clasificador mediante lógica difusa, 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 Tasa de Falsa Aceptación de 2.9% y para la Tasa de Falso Rechazo 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 Tasa de Falsa Aceptación de 0.2% y para la Tasa de Falso Rechazo 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 u 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. Los resultados que obtuvo fueron para la Tasa de Falsa Aceptación de 0% y para la Tasa de Falso Rechazo 35%.

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.

## 1.3.- PLANTEAMIENTO DEL PROBLEMA

Los problemas de seguridad informática han dejado de pertenecer sólo a los equipos de cómputo y han comenzado a reflejarse cada vez más en los teléfonos móviles. Los ataques están enfocados a robar información personal o corporativa.

Como se menciona en la introducción a esta tesis, el principal problema que actualmente los usuarios de un teléfono móvil tienen, es el del robo de su PIN, los ataques mediante el bluetooth de los cuales son víctimas muchas personas y la descarga de sitios wap infectados con malware[6].

Cuando un celular ingresa a un sitio wap infectado y descarga algún tipo de archivo para el dispositivo, es inmediatamente atacado por un virus con el único objetivo de obtener las contraseñas bancarias de los usuarios, esta vulnerabilidad se presenta en celulares desbloqueados y el ataque que se realiza se denomina "bluesniffing"[7], como lo menciona Andrés Velázquez [Audiencia Electrónica. 2009], director de investigaciones digitales del laboratorio de crímenes informáticos Mastica "Los teléfonos celulares han pasado de ser un dispositivo de comunicación más a ser el medio más personal que existe y ". Por lo que ser atacado por un virus o malwares no solo significa perder la libreta de direcciones, sino una serie de documentos que permiten saber todo acerca de una persona. Asimismo, el experto menciona que es muy importante que los celulares deban ser protegidos desde su punto más básico que es la inclusión de un PIN para evitar el acceso de cualquier otra persona que no sea el dueño.

[6] Malware o software de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya

[7] bluesniffing, técnica de hackeo donde se utiliza un dispositivo para sniffear conexiones entre otros dispositivos Hasta hace un tiempo esto se consideraba extremadamente complejo y que requería de hardware muy caro, pero ahora es posible

Si bien el bluetooth es una tecnología que permite la comunicación inalámbrica entre dos o más dispositivos celulares que posean la misma tecnología, la misma trae consigo una vulnerabilidad, que sucede al momento de transferir archivos durante el proceso de paring[8] o emparejamiento [Sallis, 2006], que es la intercepción al momento de dicho proceso, así en el momento de querer transferir algún archivo desde un celular hasta otro, en ambos casos los celulares deben introducir el número PIN como una forma de autenticación.

Los lugares más fáciles y preferidos en los cuales las persona ajenas eligen para obtener este tipo de información vital para los usuarios de los celulares son los lugares céntricos y estratégicos de una ciudad en donde el flujo de las personas es constante, así como el uso de los celulares también lo es, entre los principales lugares tenemos: en varios de los cines, en las plazas, en una biblioteca, en un centro comercial, en un stadium que es el lugar donde mayor cantidad de personas acude para ver un partido de futbol, en el minibus o algún medio de transporte y otros.

### 1.3.1 FORMULACIÓN DEL PROBLEMA

¿Es posible encontrar algún mecanismo de protección que pueda reforzar el proceso de autenticación en los teléfonos celulares mediante el ingreso del número PIN para poder evitar la intromisión de cualquier otra persona que no sea el usuario auténtico?

[8] Paring, proceso por el cual dos o más celulares se comunican mediante bluetooth y el cual genera un código de enlace almacenado en cada dispositivo enlazado

## 1.4.- OBJETIVOS

### 1.4.1 Objetivo General

- Encontrar patrones de tecleo en celulares mediante la dinámica de tecleo y asociarlos con características personales de autenticación para poder obtener indicadores de tasas de error cuyas medidas establezcan la aplicación del método mencionado en los teléfonos celulares.

### 1.4.2 Objetivos Específicos

- Evaluar las características biométricas del ritmo de tecleo de una persona.
- Obtener patrones de tiempo de presión que es el evento de presionar y soltar una tecla.
- Obtener patrones de tiempo de cambio que es el evento de presionar una tecla y presionar la siguiente tecla.
- Crear un modelo de clasificación de usuarios o perfil digital mediante su dinámica de tecleo.
- Desarrollar una aplicación que permita la autenticación del usuario, así como la creación y adaptación del perfil digital.

## 1.5.- JUSTIFICACIÓN

Debido a los problemas que se suscitan con respecto a la problemática planteada anteriormente y que afecta a la sociedad, es que la presente tesis va orientada al desarrollo de una aplicación para la autenticación de usuarios de celulares haciendo uso de la dinámica de tecleo como una técnica de autenticación biométrica, el cual viene a ser un complemento o un aditamento al control de seguridad de las credenciales de autenticación, en el caso de los celulares, los usuarios únicamente utilizan el PIN para poder acceder al celular.

A diferencia de los demás sistemas biométricos, que muchos de ellos requieren de dispositivos adicionales para los procesos de captura o registro y verificación, lo que a la vez también significa un costo adicional que en la mayoría de los casos es muy alto, la dinámica de tecleo hasta el momento es el único sistema biométrico que no necesita de un dispositivo adicional para el proceso de captura o registro y verificación, lo que en materia de costo significa un nivel bajo [Aguilar, Lizama, 2006], ya que solo se requiere de un teclado convencional.

El beneficio principal del desarrollo de la aplicación, traería consigo un nivel de confianza incremental en los usuarios de celulares, mismos que no tendrían que preocuparse por el robo o pérdida de su PIN.

A parte del beneficio principal, también se debe considerar el aporte significativo que brindará la actual investigación, ya que durante mucho tiempo la dinámica de tecleo ha sido ignorada como una técnica para el uso en la autenticación biométrica, además de crear inquietud en la investigación de sistemas biométricos diferentes a los ya conocidos hasta la actualidad.

## 1.6.- HIPÓTESIS

Hi: La incorporación de la dinámica de tecleo como un método de autenticación biométrico de comportamiento permite brindar seguridad a los usuarios de celulares, obteniendo como indicadores de tasas de error a la Tasa de Falsa Aceptación (TFA), a la Tasa de Falso Rechazo (TFR) y a la Tasa de Error de Cruce (TEC) cada uno con porcentajes menores o iguales al 10%.

### 1.6.1 Identificación de variables

a) Variable independiente

- El patrón de tiempo de presión.
- El patrón de tiempo de cambio.

b) Variable dependiente

- Perfil digital personal.

c) Variables perturbadoras

- El estado de ánimo de una persona al momento de autenticarse en el celular mediante su número PIN.
- La alteración de los usuarios por lesiones sufridas en las manos, o impedimento por la pérdida de las manos en algún accidente.
- El tiempo de adecuación de las personas con respecto al uso de un celular.
- El tipo de teclado que posee el celular.
- La longitud del número PIN asociada al usuario del teléfono celular.
- La inestabilidad difusa del prototipo en el proceso de la captura de datos.

### 1.6.2 Definición de variables

a) Variable independiente

El patrón de tiempo de presión es el tiempo que transcurre cuando el usuario presiona y suelta la misma tecla, como se observa en la figura 1.

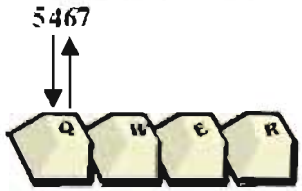



Figura 1. Evento pulsar-soltar.

Fuente: [Aguilar, 2006]

El patrón de tiempo de cambio es el tiempo que transcurre cuando el usuario presiona una tecla y a continuación presiona la siguiente tecla, como se observa en la figura 2.

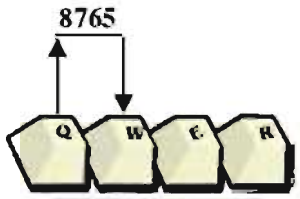



Figura 2. Evento presionar una tecla y presionar la siguiente tecla.

Fuente: [Aguilar, 2006]

b) Variable dependiente

El perfil digital personal de un usuario es creado a partir de los tiempos generados por las variables independientes y luego procesadas por clasificadores basados en modelos estadísticos, para su posterior aplicación en la autenticación del usuario.

Se manejarán dos perfiles: uno denominado perfil digital de referencia que será creado y almacenado la primera vez que el usuario ingrese al celular, y el otro denominado perfil digital de prueba que será generado al momento de que el usuario realice un intento de ingreso al celular, y el cual será comparado con el perfil digital de referencia para comprobar la autenticidad del usuario.

## 1.7.- ALCANCES Y LIMITACIONES

Debido a que en el mercado actual existe una diversidad de marcas y modelos de celulares, el desarrollo del prototipo para el estudio la presente tesis se desarrolló en un celular de la marca Sony Ericsson modelo F305 con las siguientes características:

- Tamaño: 3.8 x 1.9 x 0.6 pulgadas.
- Peso: 97.5gr.
- Pantalla 176x220 pixels.
- Memoria Phone memory 10MB * Memory Stick Micro™ (M2™) (hasta 4GB).

Teniendo en cuenta las características del celular y también tomando en cuenta las variables perturbadoras que se mencionaron anteriormente, en el desarrollo mismo de la investigación y la construcción del prototipo se tomarán en cuenta las siguientes observaciones:

- La contraseña es la medida que se toma en cuenta para la autenticación de un usuario en un sistema, en el caso de los celulares esta medida está dada por el número PIN que debe ser ingresado al momento de ingresar al celular, mismo que está compuesto de 4 a 8 dígitos, todos de carácter numérico, por lo consiguiente el análisis de dígrafos para crear el perfil digital del usuario fue tomado en cuenta con la principal característica del PIN.
- Como en muchos de los trabajos acerca de la dinámica de tecleo y en muchos de estos estudios se toma en cuenta el análisis de las letras mayúsculas y minúsculas, para nuestro objeto de estudio no fue tomado en cuenta por la razón misma de que el PIN solo esta compuesto de números.
- Actualmente se están lanzando en el mercado muchos celulares con teclado táctil, para la realización de esta investigación el celular Sony Ericsson F305 posee un teclado alfanumérico corriente, es decir que no se

está tomando en cuenta el estudio de esta tesis a los nuevos celulares con teclado táctil.

- El desarrollo de aplicaciones bajo la plataforma J2ME en el celular Sony Ericsson F305 tiene como límite un tamaño de 150 KB, por lo consiguiente para el desarrollo del prototipo se tuvo que utilizar la menor cantidad de recursos de código de programación para evitar un posible rechazo por parte del celular al momento de instalar la aplicación.

# 2.- MARCO TEÓRICO

## 2.1 SEGURIDAD Y AUTENTICACIÓN

### 2.1.1 Introducción

Mantener un sistema de información funcionando correctamente y sin ningún tipo de problemas es a menudo 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.

El surgimiento de la palabra "seguridad" se da a necesidad y 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.

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.

Algunos hechos importantes que ocurrieron en diferentes fechas se muestran a continuación [Sanchez, Gorrotxategi, Garaizar] esto como prueba del hecho que: ¿por qué alguien tendría que amenazarme si no tengo nada importante? o ¿Quién va a querer atacarme si no tengo nada importante?, es verdad, las amenazas surgen por la posesión de algo muy valioso y vital que si es develado, nos daría un gran problema.

### 2.1.2 ¿QUÉ ES SEGURIDAD?

Existen muchos conceptos para poder definir la seguridad, entre ellos tenemos: "Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro" [Wikipedia, 2007].

Borghello [Borghello, Fabian, 2001] afirma "La seguridad se define como la interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global".

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

Debemos considerar que la seguridad implica además otros conceptos muy importantes, también conocidos como la triada de la seguridad [Wikipedia, 2006] [Borghello, Fabian, 2001]: Confidencialidad, Integridad y Disponibilidad (figura 3).


Figura 3. Triada de la seguridad.
Fuente: Elaboración propia

Actualmente esta triada ha sido modificada y se le han añadido 2 elementos: Control y la Autenticidad [Borghello, Fabian, 2001].

### 2.1.2.1.- Confidencialidad

La confidencialidad de la información también es conocida como privacidad y consiste en que toda la información solo sea de conocimiento para aquellas personas que están autorizadas [Borghello, Fabian, 2001].

Cuando por alguna razón nuestra información ha sido accesada u obtenida por medio de una persona no autorizada [Wikipedia, 2006], se presenta una ruptura en la confidencialidad del sistema. Por ejemplo puede suceder que alguien este espiando sobre nuestros hombros mientras nosotros tenemos información vital en nuestro monitor. En este caso la pérdida de confidencialidad puede traer muchos problemas al dueño, ya que información vital como los números PIN de sus tarjetas de créditos pueden ser utilizadas para hacer un sin fin de transacciones en bancos de manera descontrolada.

### 2.1.2.2.- Integridad

La integridad de la información se refiere a que la información que ha sido almacenada en un sistema, no debe de ser alterada en su contenido a menos que se tenga una autorización a un grupo de personas para hacerlo [Wikipedia, 2006]. Un atacante no debe ser capaz de sustituir información legítima por falsa.

Si por alguna razón o por algún medio la información es alterada, modificada o eliminada, se presenta un pérdida en la integridad de la información, esta alteración en la información puede ser de manera parcial, que se da cuando un empleado modifica una cierta región de la información y de manera total que se da cuando algún programa por alguna razón decide eliminar todo el contenido de la información.

### 2.1.2.3.- Disponibilidad

La disponibilidad de la información se refiere a que cuando una persona autorizada desee hacer uso de la información, la misma este disponible en cualquier momento, para su posterior tratamiento. Esto requiere que la información esté almacenada correctamente con el hardware y el software funcionando perfectamente [Borghello, Fabian, 2001].

Poder garantizar que la información este disponible en todo momento puede ser muchas veces dificultosa, ya que se cuenta con factores perjudiciales que son inherentes al sistema, como un corte de luz u otros [Wikipedia, 2006].

### 2.1.2.4.- Control

El control de la información se refiere a que la misma cuando es requerida para su procesamiento debe ser válida y sobre todo que pueda ser utilizado en un tiempo, forma y distribución determinados [Borghello, Fabian, 2001].

### 2.1.2.5.- Autenticidad

La autenticidad de la información se refiere a que debe ser posible para un usuario establecer el origen de la información [Wikipedia, 2006], es decir que el usuario esta en la necesidad de saber si el origen de la información es un componente seguro y de fiar. Un atacante no debe tener la capacidad de hacerse pasar por otro usuario.

## 2.1.3 ¿Qué debemos proteger?

Cuando nos realizamos esta pregunta, lo primero que se nos viene a la cabeza son: los datos, el software, el hardware. Todo en su conjunto conforma un sistema informático [Borghello, Fabian, 2001], pero de todo ese conjunto lo que más nos interesa sin duda son los datos, ya que los mismos conforman el activo en una empresa, así como es de gran importancia para un usuario de un banco.

Podemos entender el concepto de datos como al conjunto de información lógica que es administrada por el software y el hardware [Borghello, Fabian, 2001].

Los 5 elementos que conforman la seguridad de la información, los cuales mencionaba anteriormente entran y juegan un papel muy importante en la protección de los datos.

## 2.1.4 ¿De quién debemos protegernos?

Como se menciono en la parte introductoria a la seguridad, existen muchas amenazas que pueden afectar la seguridad de un sistema. Una de estas amenazas [Borghello, Fabian, 2001] esta conformada por personas, que pueden ser desde una sola hasta un grupo de varias. Podemos denominar a este tipo de personas atacante(s) o intruso(s).

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

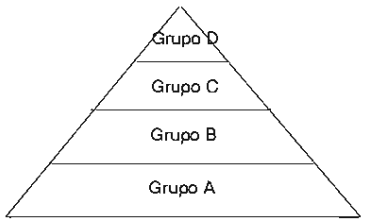



Figura 4. Clasificación de intrusos
Fuente: [Borghello, Fabian, 2001]

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.

De la anterior clasificación también es necesario mencionar la clasificación de las amenazas existentes: interceptación, interrupción, modificación y fabricación [Jerez, 2002].

### 2.1.4.1.- Interceptación

Estos ataques se realizan cuando una persona no autorizada accede a un elemento del sistema mientras un flujo de información fluye a través del sistema dentro de una organización (figura 5).

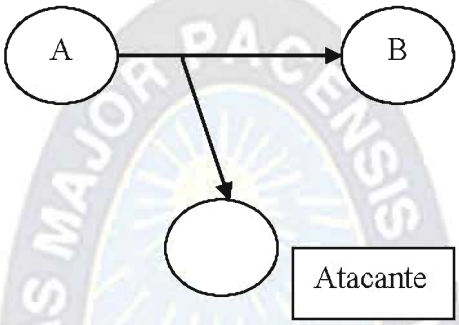



Figura 5. Ataque de Interceptación

Fuente: Elaboración propia

### 2.1.4.2.- Interrupción

Estos ataques se realizan cuando una persona no autorizada o intruso logra que un elemento del sistema se pierda mientras un flujo de información estaba fluyendo a través del sistema de la organización (figura 6). Este tipo de ataques pueden ser confundidos con "caídas del sistema".

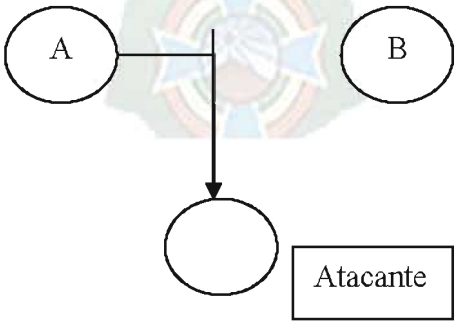



Figura 6. Ataque de Interrupción

Fuente: Elaboración propia

### 2.1.4.3.- Modificación

Estos ataques se realizan cuando una persona no autorizada logra una interrupción en el sistema, pero además logra modificar el elemento que estaba siendo transmitido por el flujo de información dentro de la organización (figura 7).

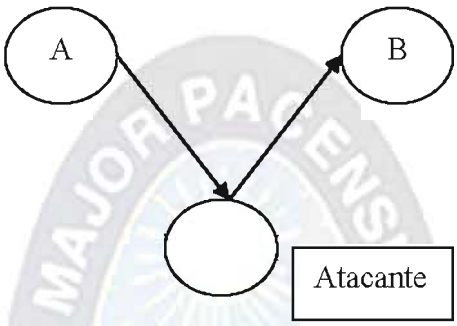



Figura 7. Ataque de Modificación

Fuente: Elaboración propia

### 2.1.4.4.- Fabricación

Un ataque de fabricación se da cuando el intruso logra crear un objeto el cual es difícil de distinguir si es un elemento genuino (figura 8). A este tipo de ataques también se los llama phishing[12].

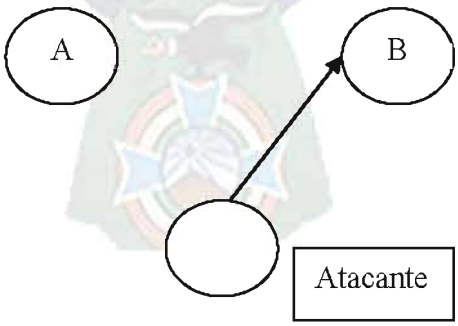



Figura 8. Ataque de Fabricación

Fuente: Elaboración propia

[12] phishing, El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes

### 2.1.5 Autenticación de Usuarios

Actualmente muchos de los sistemas de información orientados a la web utilizan un mecanismo de control para el acceso a diferentes recursos que los mismos pueden ofrecer, este tipo de control se lo denomina "autenticación" que proviene del griego "Autentikos" que significa verdadero o genuino, y "authentes" que significa el autor o dueño [Online Etymology Dictionary, 2001].

Pero en realidad que significa autenticar a un usuario en un sistema de información, entre muchas de las definiciones encontramos que autenticar a un usuario es: "el acto de establecimiento o confirmación de una persona que a menudo consiste en verificar su identidad. [Wikipedia, 2005]".

A menudo los métodos de autenticación a través de los cuales un usuario se puede autenticar se dividen en: algo que el usuario conoce, algo que el usuario posee y algo que el usuario es [Red Iris, 2002].

Antes de entrar con la clasificación de los métodos de autenticación, es necesario realizar una aclaración entre los términos identificación y autenticación. Por un lado la identificación es el medio por el que un usuario afirma su identidad a un sistema, mientras que la autenticación es el medio para poder establecer la validez de esta afirmación [Red Iris, 2002]. Para aclarar mejor el panorama, tomamos como ejemplo el esquema básico de control que utiliza el mecanismo de logueo conformado por el ID y el passwords del usuario. En nuestro caso el login o ID vendría a ser el medio por el cual un usuario de identifica en el sistema, pero la manera en que el usuario se autentica en el mismo es mediante su password.

#### 2.1.5.1.- Autenticación basada en algo que el usuario conoce

Uno de los mecanismos básicos de control de usuarios que utilizan los sistemas de información es el del logueo, conformado por el ID y el passwords. Este tipo de

mecanismo lleva mucho tiempo como preferencial de los sistemas de autenticación. Entre las principales ventajas que se toma en cuenta, la familiarización de los usuarios y el bajo costo que significa su implementación.

Desgraciadamente entre sus desventajas son: que muchos de los usuarios utilizan como password o contraseña, palabras demasiado fáciles como sus propios nombres o nombres de conocidos, y otra desventaja que podemos encontrar es que muchas veces los usuarios escogen contraseñas de longitud muy corta, lo cual hace que hackers[13] puedan utilizar programas de fuerza bruta[14] para poder acceder a sistemas de manera inautorizada.

A continuación se muestran algunas estadísticas de las tendencias de 13.787 usuarios al momento de escoger su contraseña en términos de longitud y tipo de Caracteres.

Tabla 1. Elección de contraseña en base a longitud.

Fuente: [Sparfford, 1992]

| Longitud de contraseña (caracteres) | Número de usuarios |
|---|---|
| 1 | 55 |
| 2 | 87 |
| 3 | 212 |
| 4 | 449 |
| 5 | 1260 |
| 6 | 3035 |
| 7 | 2917 |
| 8 | 5772 |

[13] hackers, experto en varias o alguna rama técnica relacionada con la informática
[14] programas de fuerza bruta, ataque en el que se intenta cada posible contraseña, una por una, hasta lograr encontrar la contraseña correcta

Tabla 2. Composición de contraseñas.

Fuente: [Sparfford, 1992]

| Tipo de caracteres | Número de usuarios | Porcentaje |
|---|---|---|
| Solamente minúsculas | 3988 | 28.9% |
| May/min mezcladas | 5259 | 38.1% |
| Algunas mayúsculas | 5641 | 40.9% |
| Dígitos | 4372 | 31.7% |
| Meta caracteres | 24 | 0.2% |
| Caracteres de control | 188 | 1.4% |
| Espacios y/o tabuladores | 566 | 4.1% |
| . , ; | 83 | 6.1% |
| - _ + = | 222 | 1.6% |
| ¡ # $ % & () | 654 | 4.4% |
| Otros no alfanuméricos | 229 | 1.7% |

Todos los mecanismos de autenticación basados en algo que el usuario conoce (ejemplo el PIN), trabajan de la siguiente forma: una clave que es compartida por 2 objetos, el cual se debe mantener en secreto, de manera que cuando se habilita una sesión de comunicación entre ambos objetos, una de ellas necesita verificar la clave que la otra debe proporcionar. Sería suficiente que una de ellas revelara la clave a un tercero para que se rompa uno de los principios fundamentales de la seguridad como es la confidencialidad [Huidobro, 2006].

### 2.1.5.2.- Autenticación basada en algo que el usuario posee

Este tipo de métodos se basa en que lo habitual que usa un usuario como: tarjetas inteligentes[15], token[16], otros. Son muy pocos los sistemas de autenticación basados únicamente en algo que el usuario posee, ya que en la actualidad se han combinado con algo que el usuario conoce, y los pocos que quedan solo se utilizan para realizar autenticaciones con acceso físico.

Este tipo de dispositivos como los tokens y demás, utilizan un microprocesador miniaturizado integrado en un trozo de plástico y funcionan mediante un lector de contactos.

Este tipo de mecanismos es aceptado por lo usuarios por ser: fiable, rápido y utilizar la criptografía para almacenar los datos [Huidobro, 2006]. Entre las desventajas podemos encontrar es que muchos de ellos como los tokens se pueden extraviar con facilidad.

### 2.1.5.3.- Autenticación basada en algo que el usuario es

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.

[15] Tarjetas Inteligentes, es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada
[16] Token, es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación

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 ultimo las cuestiones religiosas [Woodward, 2001].

## 2.2 BIOMETRÍA

### 2.2.1 Definición

Características propias que identifican a una persona de otra nos hace pensar que de alguna forma podemos reconocer a personas conocidas con solo escuchar su voz, o identificar a un delincuente con solo realizar un análisis de las huellas dactilares que el mismo haya dejado sobre la escena de crimen, o como en muchos bancos, el solo hecho de que una persona realice el trazo de su firma es una característica para su identificación.

La palabra biometría proviene del griego "bios" que significa vida y "metron" que significa medida [Muñoz, 2007].

Podemos definir biometría como el estudio de los métodos para el reconocimiento de las características cuantitativas mediante el estudio matemático y estadístico [Wikipedia. 2004].

Como características propias de las personas que se pueden utilizar para los sistemas biométricos podemos encontrar la geometría de la mano, los rasgos faciales, el iris, la retina, la voz, el ritmo de tecleo de las personas, la forma de caminar de la personas, la firma.

Todas las características anteriormente descritas están clasificadas en dos grupos: Biometrías estáticas y dinámicas. En la tabla 3 se muestra la evaluación a varias tecnologías biométricas en base a diferentes criterios, donde A,M, y B son "Alto", "Bajo" y "Medio".

Tabla 3. Comparación entre varias tecnologías biométricas.

Fuente: [Anil , Arun , Salil, 2004]

| | Universalidad | Unicidad | Permanencia | Recolectabilidad | Desempeño | Aceptabilidad | Facilidad de engaño |
|---|---|---|---|---|---|---|---|
| Cara | A | B | M | A | B | A | B |
| Huella digital | M | A | A | M | A | M | A |
| Geometría de la mano | M | M | M | A | M | M | M |
| Dinámica de tecleo | B | B | B | M | B | M | M |
| Venas de la mano | M | M | M | M | M | M | A |
| Iris | A | A | A | M | A | B | A |
| Retina | A | A | M | B | A | B | A |
| Firma | B | B | B | A | B | A | B |
| Voz | M | B | B | M | B | A | B |
| Termograma facial | A | A | B | A | M | A | A |
| ADN | A | A | A | B | A | B | B |

### 2.2.2 Funcionamiento

La comodidad que brindan los sistemas biométricos a un usuario se sintetiza en que el mismo no tiene la necesidad de portar consigo un token o crear y recordar una contraseña, puesto que únicamente la primera vez que utilice el sistema tendrá que presentar su credencial o en este caso su rasgo característico y medible al sistema para que este pueda crear su perfil y sea almacenado. Ya en una segunda oportunidad el usuario solo tendrá que presentar su credencial y este será comparado contra el perfil creado.

En la figura 9 se presenta un esquema básico del funcionamiento de un sistema biométrico

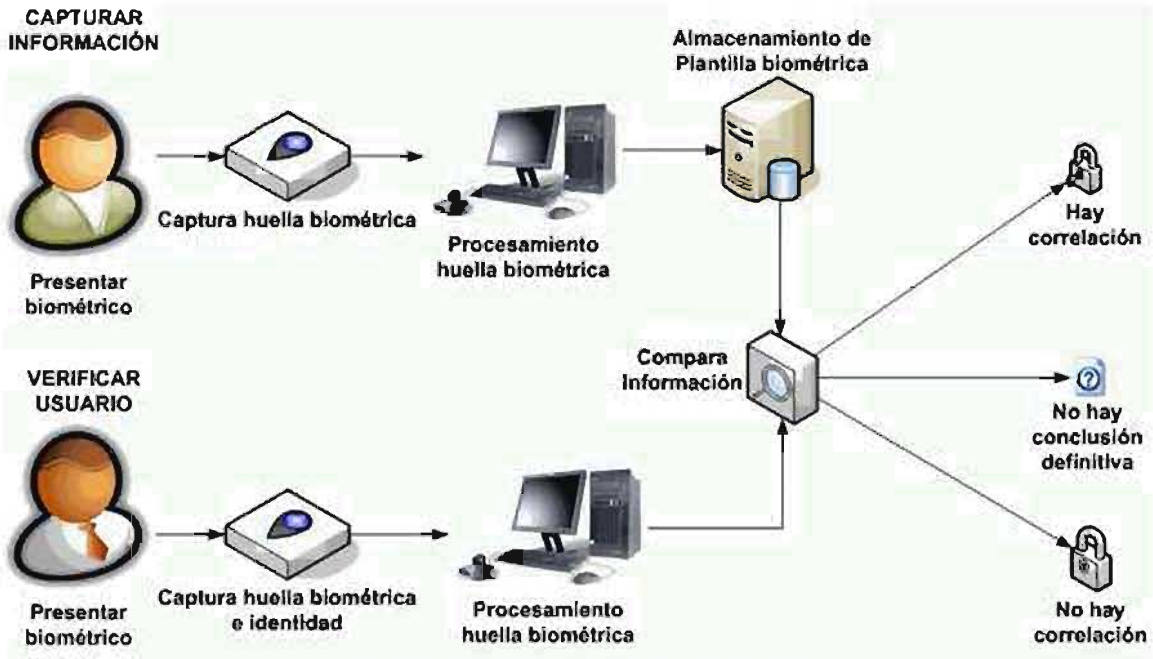



Figura 9. Proceso de registro y verificación en un sistema biométrico

Fuente: extraído de la página web:

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

Cuando un usuario hace uso del sistema, el mismo captura su rasgo fisiológico o conductual. Dicha captura luego es procesada por un algoritmo numérico para poder 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 [Anil , Arun , Salil, 2004].

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 positivos.

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 el celular, denegando el acceso a u usuario que es legítimo. Dentro de la Estadística este error se conoce como falsos negativos.

Se considera que la TFR es mas elevada que la TFA, ya que al producirse un error de este tipo se rompe el esquema de seguridad. En la figura 10 se muestra una gráfica de la TFR contra la TFA, de la cual de puede obtener una nueva medida denominada TEC o EER (del inglés Equal Error Rate – tasa de error de cruce). Se dice que mientras mas bajo sea el TEC, más exacto será el sistema [Ashbourn, 2000].

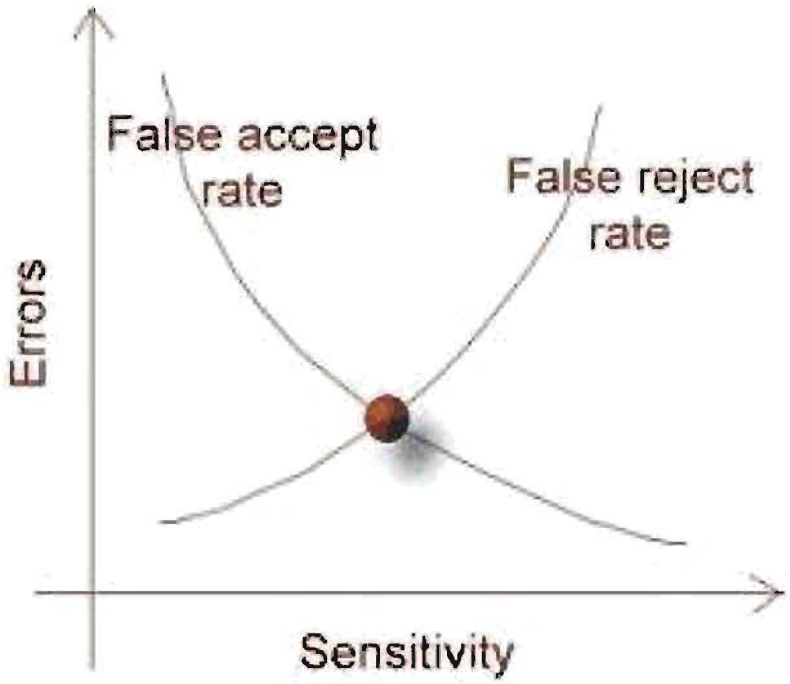



Figura 10. Medida de desempeño de un sistema biométrico
Fuente: extraído de la página web: http://es.wikipedia.org/wiki/Biometr%C3%ADa

### 2.2.3 Biometría Estática

Son aquellas características fisiológicas[17] 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.

#### 2.2.3.1.- 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].

Los problemas que presentan estos sistemas están relacionados a factores de condición del ambiente en el momento de la adquisición de la muestra, como pueden ser la iluminación, el fondo, el ángulo en que se toma la imagen [Matthew , Alex, 1991].

#### 2.2.3.2.- 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

[17] fisiológico, Relacionado con las funciones y características propias del cuerpo humano

localizan las terminaciones de crestas, bifurcaciones, puntos y cruces (todos estos elementos se denominan minucias, podemos ver un ejemplo en la Figura 11), 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].

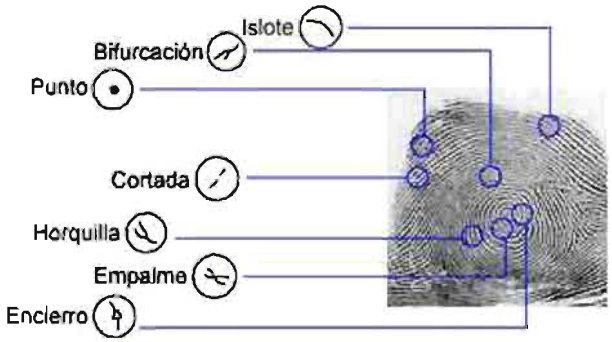



Figura 11. Minucias en una huella digital

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

### 2.2.3.3.- Geometría de la mano

Para usar la geometría de la mano como rasgo biométrico se coloca la mano sobre una superficie y se toman dos imágenes, una de la vista lateral y otra de la superior. A partir de estas imágenes (Figura 12) se medirán la forma y tamaño de la palma y el largo y ancho de los dedos [Muñoz, 2007].

Tiene como desventaja que los lectores suelen ser de gran tamaño, lo que complica la incorporación en dispositivos móviles.

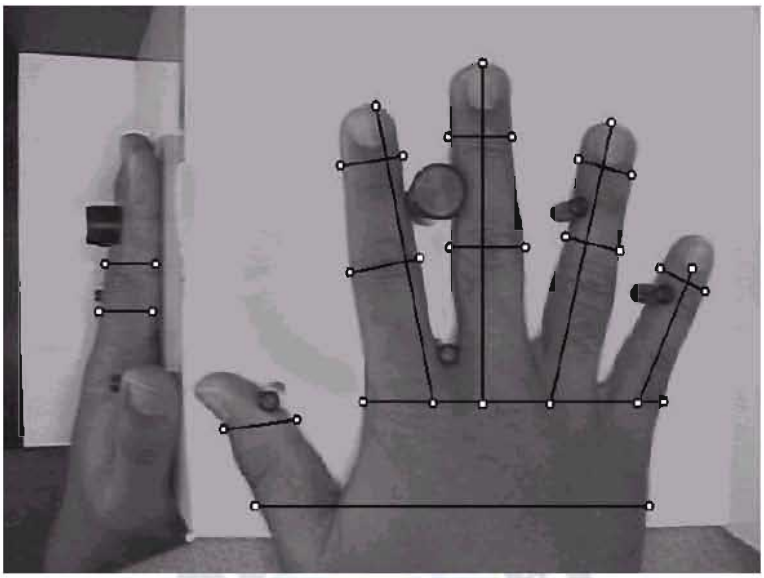


Figura 12. Medición de la geometría de la mano.
Fuente: extraído de la página web:
http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node120.html

### 2.2.3.4.- Iris

El iris es la parte del ojo que tiene el color, y está formado por un tejido con una textura compleja con un patrón único. El iris se forma durante el desarrollo fetal y se estabiliza en los primeros dos años de vida. La imagen del ojo es adquirida por una pequeña cámara infrarroja, para después identificar el iris y segmentarlo en bordes (Figura 13) y convertir sus características en datos numéricos (llamado IrisCode) [Yau Wei Y, 2002].

Se considera que las sistemas que usan el iris son los más confiables de todos los sistemas biométricos que se han propuesto [Muñoz, 2007], pero a pesar de ser un sistema muy rápido y confiable, no existen muchas implementaciones hoy en día debido a su alto costo [Yau Wei Y, 2002].

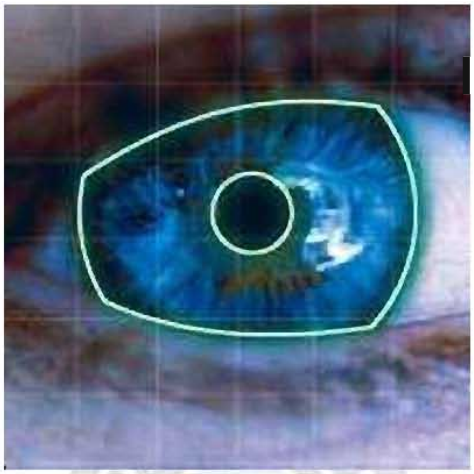


Figura 13. Adquisición de las características del Iris.

Fuente: extraído de la página web: http://www.biometriaaplicada.com

### 2.2.3.5.- Retina

Los vasos sanguíneos de la retina poseen una estructura rica y única (Figura 14). El funcionamiento de los sistemas que hacen uso de la retina es muy similar al de aquellos que usan el iris [Muñoz, 2007]. Un aspecto por el que no logran gran aceptación entre los usuarios es que las lecturas pueden revelar la existencia de ciertas enfermedades.

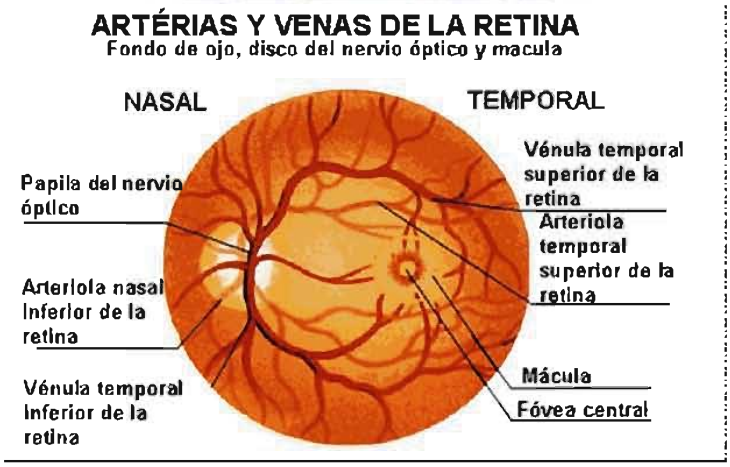



Figura 14. Imagen de vasculatura retinal

Fuente: extraído de la página web: http://www.e-oftalmologia.com/area_formacion/anatomia/retina.html

### 2.2.4 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.

Estos rasgos presentan desventajas generales de que no son estables en el tiempo y que pueden verse afectados por factores ambientales y de estado emocional [Ruud, Connell, Pakanti, 2003].

#### 2.2.4.1.- Voz

En los sistemas de autenticación por voz, el usuario emplea un micrófono para grabar sus voz, ya sea repitiendo un texto dado por el sistema o hablando libremente. Después la voz es digitalizada para poder extraer de ella algunas características únicas y generar el perfil. La extracción de las características puede lograrse a través de plantillas estocásticas o de plantillas modelo. En las plantillas estocásticas se usan técnicas de igualación probabilísticas como el Modelo Escondido de Markov, el cual produce una medida de similitud del modelo [Yau Wei Y, 2002].

En las plantillas modelo se emplean técnicas de igualación determinísticas, que suponen que la muestra es similar al perfil, pero con alguna distorsión. A partir de aquí se mide la distancia de error mínimo, empleando algoritmos como envolvimiento de tiempo dinámico, cuantización de vectores y vecinos más cercanos [Muñoz, 2007].

### 2.2.4.2.- Manera de Caminar

La biometría basada en la manera de caminar es un método espacial-temporal complejo, que se logra a través de filmaciones que analizan varios movimientos de cada articulación, es por esto que requieren un alto costo computacional. La manera de caminar puede parecer un rasgo no muy distintivo, pero es lo suficientemente discriminatorio como para permitir autenticaciones en ambientes de baja seguridad [Anil , Arun , Salil, 2004] como en los bancos, para de esa manera poder determinar personas sospechosas de realizar un acto delictivo.

### 2.2.4.3.- Firma

Una firma desarrollada de forma natural representa el acto de escritura más frecuente y habitual, y aunque dos firmas nunca serían iguales, siempre la mantenemos dentro de ciertos límites, los cuales representan de manera única a cada individuo. La firma ha sido aceptada como método de autenticación en transacciones legales y comerciales [Joyce, Gupta, 1990].

### 2.2.4.4.- Dinámica de tecleo

Cuando una persona se sienta frente a una computadora y comienza a teclear, la misma no teclea de una manera caótica, sino que teclea por un momento, se detiene para reunir ideas, se detiene para descansar, continúa tecleando y así sucesivamente [Carl, Moran, 1980]. Este comportamiento único nos brinda las bases para desarrollar un esquema de autenticación; las características que nos interesarán para el análisis del comportamiento están relacionadas con eventos de las pulsaciones de las teclas, y son: el tiempo de presión (dwell time) y tiempo de cambio (flight time). Los mismos que son mostradas en la Figura 15.


Figura 15. Eventos en el cálculo de dinámica de tecleo.
Fuente: [Aguilar, 2006]

El tiempo de presión es el tiempo que transcurre desde que se presiona una tecla hasta que se libera. El tiempo de cambio corresponde al tiempo que pasa desde que se suelta una tecla hasta que se presiona la siguiente [Aguilar, Lizama, 2006].

El punto central para el cálculo de perfiles 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.

# 3.- MARCO APLICATIVO

## 3.1.- Diseño Metodológico

En el marco del plan de trabajo a la presente tesis se aplicó el método científico, enmarcándose en un diseño cuasi-experimental:

### 3.1.1.- Método Cuantitativo

#### 3.1.1.1.- Población

Como el tamaño de la población de usuarios de teléfonos celulares en Bolivia [ABI,2008] es de aproximadamente 4,4 millones, el trabajo actual está orientada a la población estudiantil y administrativa de la Universidad Mayor de San Andrés con una población cercana a las 80.000 personas de las cuales se toma como tamaño de muestra representativa a un total de 80 personas, cantidad calculada a partir de la formula (A), quienes han sido divididos en tres grupos de personas, de las cuales se deberá tomar en cuenta que tengan como mínimo un año, respecto al tiempo de adecuación en el manejo de celulares y que se describen a continuación:

1. Grupo de 40 personas denominado "Grupo de Perfil de muestras de Universitarios": el cual estará conformado por 30 estudiantes de la carrera de Informática de la Universidad Mayor de San Andrés, de los cuales se crearán sus respectivos perfiles digitales, que serán utilizados para poder hallar la TFR (Tasa de Falso Rechazo).
2. Grupo de 40 personas denominado "Grupo de Perfil de muestras de Varios": el cual estará conformado por 30 personas comunes que no se encuentren en la Universidad Mayor de San Andrés, de los cuales se crearán sus respectivos perfiles digitales, que serán utilizados para poder hallar la TFR (Tasa de Falso Rechazo). Lo que se buscará con este grupo es probar si la aplicación biométrica es capaz de reconocer a cualquier persona.

3. Grupo de 10 personas denominado "Grupo de Personificadores": el cual estará conformado por personas de los dos anteriores grupos a quienes se les proveerá los números PIN de personas registradas en el prototipo, para que puedan realizar el proceso de autenticación haciéndose pasar como usuarios legítimos y de esa manera poder hallar la TFA (Tasa de Falsa Aceptación).

**Cálculo del tamaño muestral:**

$$\text{Tamaño muestral} = N * z^2 * p * q / (i^2 * (N-1) + z^2 * p * q) \qquad (A)$$

Donde:

- N: tamaño de la población
- z: Valor de z: 1,96 para un $\propto = 0,05$
- p: es la prevalencia esperada del parámetro a evaluar.
- q: q = 1 – p
- i: es el error que se prevé cometer.

### 3.1.1.2.- Desarrollo del Prototipo

En el presente capítulo se detallan las diferentes partes o módulos que se integraron para el desarrollo del prototipo (figura 19) propuesto en esta tesis, el cual fue programado en su totalidad usando la platadorma J2ME, la elección de la misma fue debido a la facilidad de integración que se tiene con el desarrollo de aplicaciones móviles para el celular Sony Ericcson serie F305.

El prototipo funciona a partir de un nombre de usuario y un password, ambos elegidos de manera libre, siendo esta sobre la cual se hará el cálculo de la dinámica de tecleo del usuario.

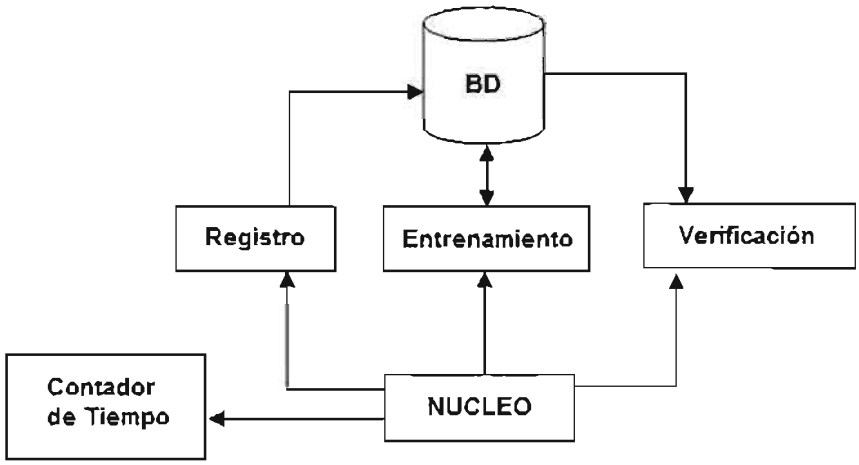



Figura 19. Diseño Modular del prototipo

Fuente: Elaboración propia

### 3.1.1.3.- Núcleo

El módulo principal, o núcleo es el encargado de interactuar con el usuario, y a partir de ahí llama a los demás módulos que se encargan de otras tareas. Es necesario aclarar que se tuvo la necesidad de utilizar la clase Canvas propia del lenguaje de programación Java, para poder capturar las muestras necesarias del password que el usuario introducirá a través del teclado convencional del celular, ya que la herramienta de introducción de texto "TextField" dentro de un "Form", ambos propios del J2ME, no nos provee la funcionalidad de captura de eventos de teclado (KeyPress y KeyReleased).

### 3.1.1.4.- Registro y Verificación

Aunque en la figura 19 el registro y la verificación se muestran como dos módulos distintos, aquí se explican de manera conjunta debido a que en esencia ambos módulos realizan la misma tarea: obtener el perfil digital del usuario a partir de sus tiempos.

Durante el proceso de registro el usuario escoge e introduce de manera libre un nombre de usuario y un password (representando el número PIN) para de esa

manera poder almacenarlos en el celular (figura 20), y poder pasar a los módulos de entrenamiento y verificación.

Durante el proceso de verificación el usuario cuyos datos de autenticación (nombre de usuario y password) y perfil digital que han sido almacenados en el celular de manera previa (figura 21), debe introducir nuevamente su nombre de usuario y password para de esa manera poder crear el perfil digital de prueba como se menciona y detalla en el capítulo 8 apartado del método de análisis.

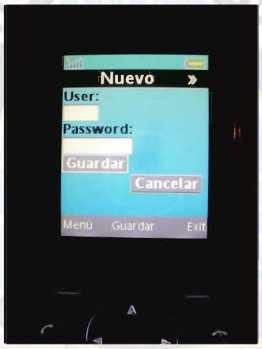



Figura 20. Formulario de Registro antes de iniciar el entrenamiento

Fuente: Elaboración propia

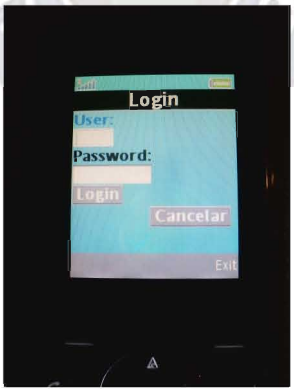



Figura 21. Formulario de Verificación para la autenticación

Fuente: Elaboración propia

### 3.1.1.5.- Contador de Tiempo

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 password y posterior almacenamiento.

Existe una función que nos permite calcular tiempos al momento de lanzarse los eventos KeyPress y KeyReleased, la función getTime() de la clase Date propia del lenguaje de programación Java, la misma nos devuelve el tiempo en milisegundos.

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.

### 3.1.1.6.- Entrenamiento

Este módulo es la parte esencial del prototipo, ya que es durante esta fase que el usuario ingresa de manera consecutiva cinco muestras del password que eligió de manera aleatoria durante la fase de registro. Este módulo también integra el módulo de contador de tiempo para poder capturar los tiempos (KeyPress y KeyReleased).

### 3.1.1.7.- Recolección de Datos

El esquema básico para la recolección de datos se muestra en la figura 16 mismos que se inician a partir de la captura de los patrones de tiempo de presión y de cambio.


Figura 16. Esquema básico para recolección de datos y posterior verificación.
Fuente: Elaboración propia

La recolección de los datos se realizará mediante el prototipo, previamente instalado en el celular Sony Ericsson F305, que en una primera instancia serán almacenados en el celular para luego ser utilizados en cada proceso de autenticación del usuario.

El prototipo deberá capturar los eventos de key presses y key released mismos que serán utilizados para capturar los tiempos de tiempo de presión y de cambio a medida que usuario vaya ingresando su password. Estos tiempos se representan de la siguiente manera:

Tiempo de presión = TiempoKeyReleased(i) – TiempoKeyPressed(i) (1)

Tiempo de cambio = TiempoKeyPressed(i+1) – TiempoKeyReleased(i) (2)

Donde i es la i-esima tecla que el usuario presiona al ingresar su PIN.

### 3.1.1.8.- Método de Análisis

Una vez finalizado la fase de recolección de datos es necesario utilizar algún método para poder crear los dos tipos de perfiles digitales personales como anteriormente se mencionaba. Como en muchos de los trabajos realizados previamente a esta tesis, existen muchos métodos para el análisis entre los cuales podemos mencionar: Modelo de Markov Oculto y Modelo Gaussiano de la Teoría estadística de Aprendizaje utilizados en el trabajo realizado por Cheng-Huang Jiang, Shiupyng Shieh y Jen-Chien Liu [Cheng-Huang, Shiupyng, Jen-Chien, 2006], modelos difusos [Marino, 2000], clasificadores de redes en función de base radial (RBF) y clasificadores basados en modelos estadísticos [Aguilar, Lizama, 2006] [Monrose, Aviel, 2000].

Para nuestro trabajo se utilizó los clasificadores basados en modelos estadísticos. Debemos tomar en cuenta que para la creación del perfil digital de referencia es necesario que durante la fase experimental se le pida a cada persona que ingrese su número PIN de tamaño 4 a 8 dígitos, en 5 reiteradas ocasiones, con el objetivo de que con estas 5 muestras, que son extraídas por cada usuario, podamos encontrar una media, haciendo un total de 400 muestras para las 80 personas que son parte de la experimentación, el cual estaría representado por un vector de tiempos medios de la siguiente forma:

$$M = \{ m_1, m_2, m_3, \ldots , m_{2n-1} \}$$

$$M = \{ TP, TC \}$$

$$TP = \{ tp_1, tp_2, tp_3, \ldots, tp_n \} \text{ y } TC = \{ tc_1, tc_2, tc_3, \ldots, tc_{n-1} \}$$

Donde:

- M es el vector de tiempos medios de las 5 muestras conformado por los tiempos de presión medios y tiempos de cambio medios.
- $m_i$ es el i-ésimo tiempo medio.

- TP es el vector de tiempos de presión medios.
- $tp_i$ es el i-ésimo tiempo de presión de una tecla.
- TC es el vector de tiempos de cambio medios.
- $tc_i$ es el i-ésimo tiempo de cambio entre 2 teclas.
- n es el tamaño del número PIN del usuario, con 4<=n<=8.

Tabla 4. Tabla de muestras para la creación del perfil digital del usuario
Fuente: Elaboración propia

| Tiempos | $TP_1$ | $TC_1$ | $TP_2$ | $TC_2$ | $TP_3$ | $TC_3$ | $TP_4$ | $TC_4$ | $TP_5$ | $TC_5$ | $TP_6$ | $TC_6$ | $TP_7$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Teclas presionadas | 5 | 5-9 | 9 | 9-9 | 9 | 9-1 | 1 | 1-7 | 7 | 7-1 | 1 | 1-0 | 0 |
| Muestra 1 | 38 | 484 | 58 | 478 | 38 | 199 | 72 | 492 | 54 | 185 | 27 | 324 | 56 |
| Muestra 2 | 62 | 485 | 52 | 504 | 41 | 259 | 81 | 407 | 56 | 191 | 37 | 266 | 76 |
| Muestra 3 | 54 | 451 | 59 | 456 | 46 | 192 | 74 | 456 | 18 | 211 | 29 | 306 | 56 |
| Muestra 4 | 51 | 418 | 31 | 462 | 32 | 195 | 80 | 463 | 35 | 192 | 21 | 341 | 45 |
| Muestra 5 | 71 | 443 | 40 | 446 | 42 | 177 | 77 | 440 | 52 | 187 | 26 | 271 | 74 |

Una vez que se obtiene M (tabla 4), se lo debe de almacenar en el celular para su posterior uso.

También debemos calcular la variabilidad que existe entre los diferentes tiempos de las muestras, para esto utilizaremos el cálculo de las desviaciones estándares para cada dato obtenido en la recolección de datos, el cual estará almacenada en un vector de la siguiente forma:

$$S = \{ s_1, s_2, s_3, \ldots, s_{2n-1} \}$$

Donde:

$$s_i = \sqrt{\frac{\sum (x - \bar{x})^2}{n-1}} \quad (3)$$

- x es cada uno de los tiempos de la muestras para un evento.
- $\bar{x}$ son los tiempos medios de presión y cambio.

- n es el número de muestras tomadas para el perfil.

También calculamos las distancias de los vectores M con respecto a los TC y TP de las 5 muestras tomadas utilizando para tal efecto el método de métricas de distancia "Manhattan city block distance metric with standard deviation" definido de la siguiente forma:

$$D(X,Y) = \sum_{i=1}^{n} \frac{|X_i - Y|}{\sigma_i} \qquad (4)$$

Donde:

- Y representa el vector de tiempos de presión y cambio medios o como lo hemos denominado M.
- X representa al vector de tiempo de presión y cambio de una de las 5 muestras tomadas.
- $\sigma_i$ son las desviaciones estándares de las cinco muestras o como lo hemos denominado S.

Este cálculo de la distancia D, nos servirá para poder determinar el umbral sobre el cual el prototipo deberá comparar, cuyo valor deberá ser mínimo para poder aceptar a un usuario o rechazarlo cada vez que el mismo intente ingresar al celular.

Para el proceso de verificación se le pedirá al usuario que ingrese su número PIN con el cual se había registrado la primera vez, y el proceso de creación del perfil digital de prueba es similar al del proceso de creación del perfil digital de referencia, con la diferencia de que para el de prueba solo se requiere que la persona ingrese una sola vez su número PIN y lo podemos representar de la siguiente forma:

$$L = \{ L_{PIN} \} = \{ I_1, I_2, I_3, \ldots, I_{2n-1} \}$$

Donde:

- L representa el perfil digital de prueba para un usuario.

Una vez que se ha obtenido L, solo nos queda calcular la distancia que existe entre el vector L y el vector M (figura 17), es decir debemos calcular D(L,M) utilizando nuevamente el método "Manhattan city block distance metric with standard deviation" definido en (4) ,cuyo resultado será analizado para determinar si se encuentra dentro del umbral, finalmente de acuerdo al número de aceptaciones y rechazos durante la fase de experimentación, podremos determinar las tasas de errores Tasa de Falsa Aceptación y Tasa de Falso Rechazo, y de la gráfica de ambos también podremos determinar la Tasa de Error de Cruce.

Se utilizo el método "Manhattan city block distance metric with standard desviation" definido en (4), ya que la misma nos permite calcular la distancia entre los perfiles tanto de referencia como el de prueba y poder determinar que tan cercanos o lejanos se encuentran ambos, de tal forma que durante el proceso de autenticación el prototipo sea capaz de dar o no acceso a los recursos del celular al usuario.

El umbral es una medida porcentual que pueda ser calculada en términos de medida de distancias, para esto debemos utilizar la siguiente fórmula:

$$U_D = ( PD * \%Aceptación) / U_{\%} \quad (5)$$

Donde:

- $U_D$ es el umbral en términos de distancia.
- %Aceptación es el porcentaje de aceptación (valores entre 1 a 100).
- $U_{\%}$ es el umbral en términos de porcentaje.
- PD es el promedio de distancia.

Es importante mencionar que un valor pequeño para $U_{\%}$ arroja un valor grande para $U_D$, y por otro lado un valor grande para $U_{\%}$ arroja un valor pequeño para $U_D$.

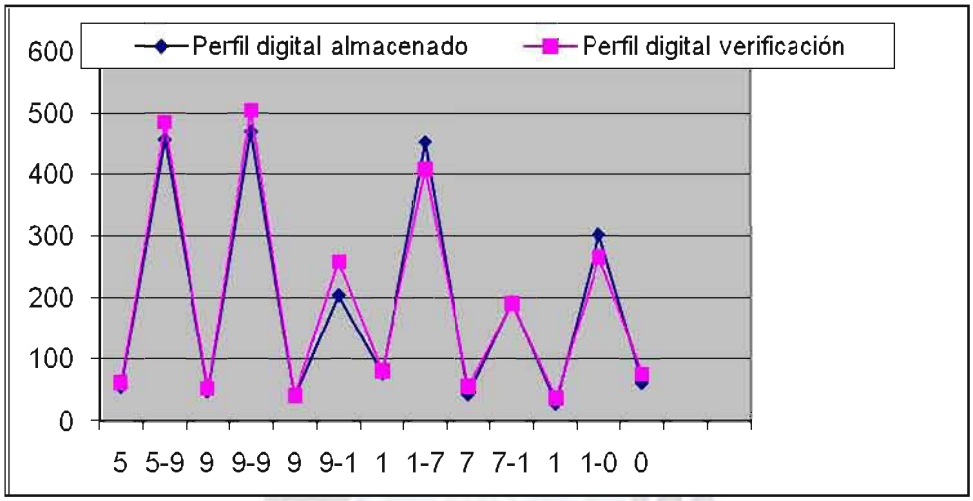



Figura 17. Distancia entre el perfil digital almacenado y el perfil digital de verificación

Fuente: Elaboración propia

### 3.1.2.- Prueba Experimental

Para probar la hipótesis planteada en la presente tesis, se realizó un experimento de acuerdo con la población especificada, las personas fueron seleccionadas en base a que contaran con un buen manejo de celulares durante al menos 1 año. Las pruebas se llevaron a cabo a lo largo de un período de siete días.

Los usuarios podían elegir libremente la contraseña a usar, pero se les hacía la recomendación de que usarán un número con el que estuvieran familiarizados y que fuera de al menos cuatro dígitos hasta un máximo de ocho dígitos.

Con las pruebas se pretendía medir la tasa de falso rechazo (TFR), la tasa de falsa aceptación (TFA) y la tasa de error de cruce (TEC), por lo que el experimento se dividió en dos dinámicas. En la primera fase se les pidió a los usuarios de los dos primeros grupos de personas que ingresaran su nombre de usuario y password para que posteriormente trataran de autenticarse reuniendo un total de 80 perfiles. En la segunda fase se proporcionó los 80 nombres de usuarios y passwords registrados en el prototipo al tercer grupo de personas y se pidió a los mismos que intentaran verificarse, haciendo un total de 80 ataques de personificación.

El prototipo desarrollado guardaba los tiempos de todos los intentos llevados a cabo por las personas que participaron en el estudio, esto con la intención de que después pudiéramos analizar con mayor detalle el comportamiento. Dicho análisis consistió en comenzar a ejecutar simulaciones del mismo experimento, proporcionando al prototipo como entrada los mismos tiempos que habían generado los usuarios previamente, pero cambiando en cada ejecución el valor del $U_{\%}$ en intervalos de 5%, comenzando en un 5% y llevándolo hasta el 100%.

### 3.1.3.- Resultados

Como resultados de los experimentos realizados con las personas que interactuaron directamente con el prototipo, de los 80 intentos de autenticación que hubo por parte de usuarios legítimos, el prototipo rechazó de manera equivocada un total de 7 usuarios, lo que se transforma en una Tasa de Falso Rechazo (TFR) de 8.75%. Respecto a los intentos de falsificación de identidad, de los 80 únicamente 4 de ellos fueron exitosos, entregando una Tasa de Falsa Aceptación (TFA) con un valor del 5%.

Las simulaciones que se hicieron, nos ayudaron a calcular las curvas de la Tasa de Falso Rechazo (TFR) y la Tasa de Falsa Aceptación (TFA), adicionalmente nos permite calcular la Tasa de Error de Cruce (TEC) que nos indica el umbral óptimo de sensibilidad del sistema.

En la Figura 18 podemos observar que la TEC se encuentra en un Umbral de alrededor de 45, que hace que el prototipo funcione con una TFR y una TFA de 8%.

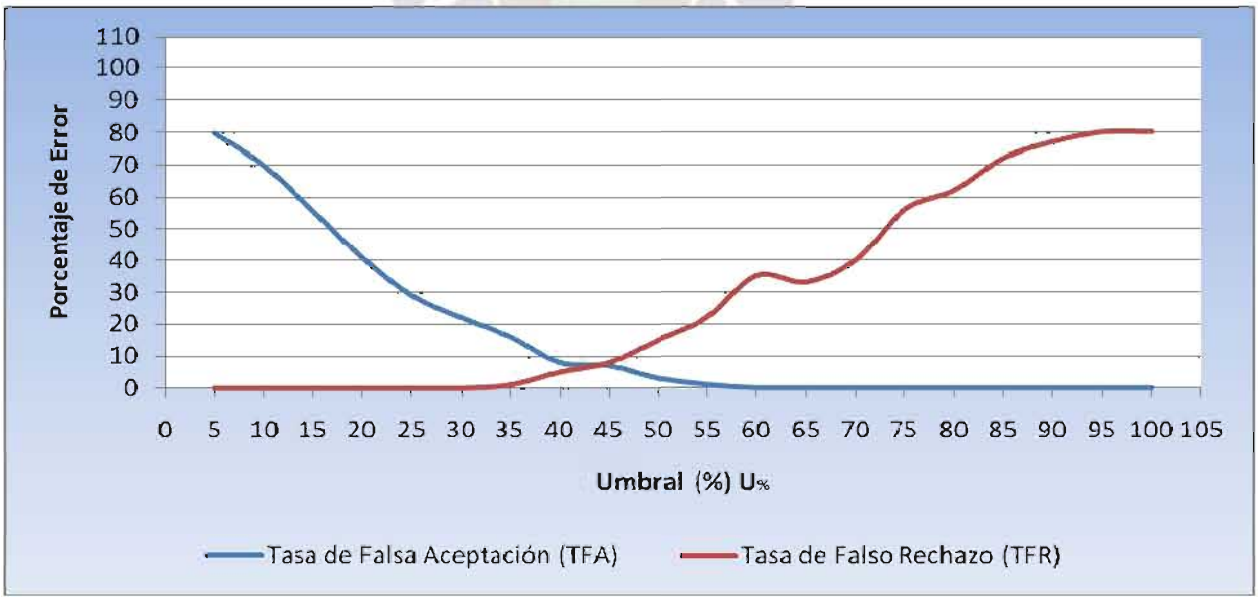



Figura 18. Gráfico de datos Umbral (%) Vs Porcentaje de error

Fuente: Elaboración propia

Las siguientes observaciones fueron hechas de acuerdo con los experimentos realizados:

- Aunque un impostor observe como un usuario legitimo teclea su clave, esto no significa que el impostor obtendrá éxito al intentar pasar por ese usuario.
- Si se escoge una secuencia de dígitos que posea un tamaño de entre 6 y 8 y además que sean no correlativos aumenta la dificultad de autenticación de un impostor.
- La familiaridad de la secuencia de dígitos para el usuario tiene un impacto bastante significativo.
- El empleo de una sesión de cinco intentos durante el entrenamiento disminuye significativamente la tasa TFR.

# DISCUSIÓN DE RESULTADOS

Como se puede observar en la Figura 18 existe un pequeño desfase en la curva que representa la Tasa de Falso Rechazo entre el rango de datos 60 y 65 para el eje que representa el Umbral en términos de porcentaje y en el rango de datos 30 y 40 para el eje que representa el porcentaje de error, esto se debe a la intromisión de algunas variables perturbadoras durante el proceso de cálculo para el valor de la Tasa de Error de Cruce, mostrando una clara disminución de precisión del prototipo.

En teoría este tipo de desfases no debería existir como se muestra en la Figura 22. Ya que la curva que representa la Tasa de Falsa Aceptación empieza en un valor alto y después tiende a declinarse hasta llegar a un valor bajo, por el contrario la curva que representa la Tasa de Falso Rechazo empieza en un valor bajo y después tiende a aumentar hasta llegar a un valor alto.

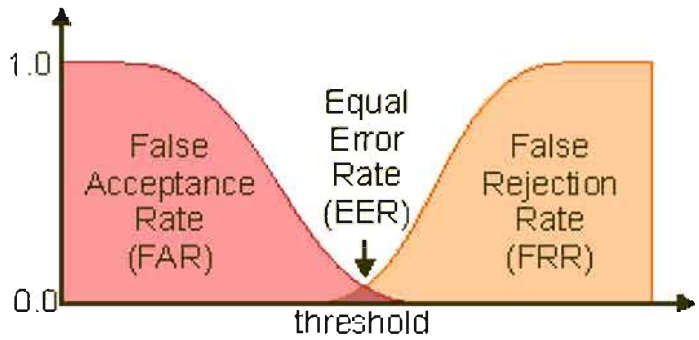



Figura 22. Gráfico de representación de las curvas TFA, TFR y TEC
Fuente: http://support.bioid.com/sdk/docs/About_EER.htm

En la Figura 23 se puede apreciar un ajuste de las curvas, mediante el método de mínimos cuadrados, tanto de la Tasa de Falso Rechazo como de la Tasa de Falsa Aceptación, aclarando que se realizo dicho ajuste para tratar de igualar las medidas teóricas reales que se muestran en la Figura 22.

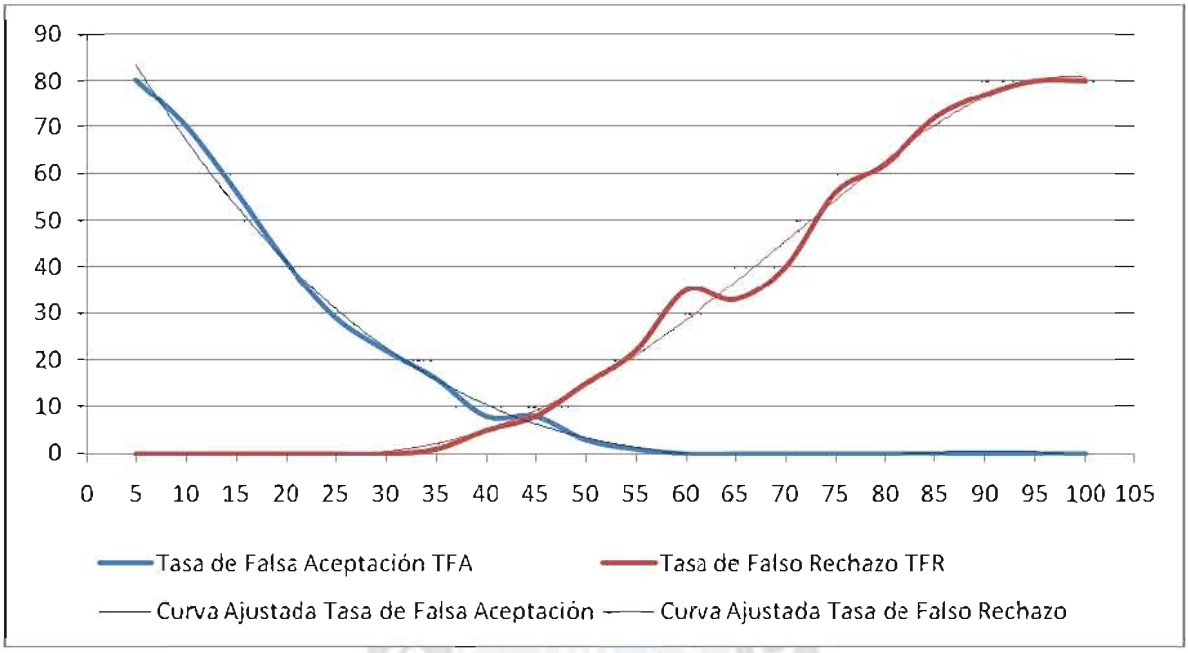



Figura 23. Gráfico de ajustes a las curvas TFA y TFR

Fuente: Elaboración propia

**Ecuaciones Polinómicas de representación a las curvas ajustadas**

**Curva de la Tasa de Falsa Aceptación**

$y = 0{,}0002x^3 + 0{,}0506x^2 - 3{,}9754x + 101{,}94$

**Curva de la Tasa de Falso Rechazo**

$y = 0{,}0009x^3 - 0{,}0341x^2 + 0{,}401x - 1{,}278$

# CONCLUSIONES GENERALES

Esta tesis tuvo por objetivo lograr encontrar patrones de tecleo en celulares mediante la dinámica de tecleo a través del prototipo desarrollado y asociarlos con características personales de autenticación para poder obtener indicadores de tasas de error cuyas medidas establezcan la aplicación del método mencionado en los celulares. Al ser este trabajo la primera implementación de este método para celulares, los resultados fueron satisfactorios y prometedores, ya que nos permiten ver que las medidas de seguridad en el proceso de autenticación en un celular pueden evolucionar con el tiempo y ser confiables para los usuarios al aplicar dicho método.

La metodología propuesta en este trabajo es de bajo costo, pues usa un teclado convencional para la adquisición de las muestras biométricas y no es invasiva pues el usuario utiliza el acceso clásico a sistemas informáticos del tipo usuario/clave.

La principal ventaja que se encontró en el actual método biométrico es que provee una segunda capa de seguridad, fortaleciendo los sistemas basados en el número PIN; otra ventaja es, que actúa de manera transparente para el usuario durante la etapa de autenticación. La desventaja que se presentó radica en la etapa de registro de usuario durante la fase de experimentación, ya que para algunas de las personas llegó a ser tedioso el escribir en repetidas ocasiones su contraseña y también el hecho mismo de que las mismas personas alegaban el no estar familiarizados con el celular Sony Ericsson F305.

# TRABAJOS FUTUROS

Existen varios puntos importantes sobre los cuales enfocarse, el primero de ellos consiste en probar la dinámica de tecleo en otros sistemas basados en números PIN como ser los cajeros automáticos de las empresas bancarias, o de celulares de última generación que llevan consigo una pantalla táctil, este último es importante ya que el trabajo en la captura de las latencias de tecleo son más complicadas.

En un segundo punto se trataría acerca del prototipo desarrollado el cual se debería modificar 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 dispositivos móviles o sistemas que tengan como base el número PIN.

Por último es necesario aplicar los criterios de evaluación biométrica para que de esa manera la dinámica de tecleo sea aplicada al proceso de autenticación en los celulares como una segunda capa de seguridad y de manera estándar.

# ANEXOS

A continuación se presentan los formularios que se utilizaron en la fase experimental de la presente tesis.

**Universidad Mayor de San Andrés**
**Facultad de Ciencias Puras y Naturales**
**Carrera de Informática**

**Formulario de Datos**
**(Fase de Experimentación)**

**Tesista: Univ.** Alvaro Javier Medina Balboa
**Tema:** Autenticación Biométrica para usuarios de celulares mediante Dinámica de Tecleo

GRUPO UNIVERSITARIOS

| Nro | Nombres y Apellidos | Carrera | Edad | Firma | Uso de celular (años) | PIN elegido | Estado |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |
| 13 | | | | | | | |
| 14 | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **15** | | | | | | | |
| **16** | | | | | | | |
| **17** | | | | | | | |
| **18** | | | | | | | |
| **19** | | | | | | | |
| **20** | | | | | | | |
| **21** | | | | | | | |
| **22** | | | | | | | |
| **23** | | | | | | | |
| **24** | | | | | | | |
| **25** | | | | | | | |
| **26** | | | | | | | |
| **27** | | | | | | | |
| **28** | | | | | | | |
| **29** | | | | | | | |
| **30** | | | | | | | |

Alvaro Javier Medina Balboa
CI 5991710 LP

**Universidad Mayor de San Andrés**
**Facultad de Ciencias Puras y Naturales**
**Carrera de Informática**

**Formulario de Datos**
**(Fase de Experimentación)**

**Tesista: Univ.** Alvaro Javier Medina Balboa
**Tema:** Autenticación Biométrica para usuarios de celulares mediante Dinámica de Tecleo

GRUPO VARIOS

| Nro | Nombres y Apellidos | Profesión | Firma | Uso de celular (años) | PIN elegido | Estado |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |
| 12 | | | | | | |
| 13 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **14** | | | | | | |
| **15** | | | | | | |
| **16** | | | | | | |
| **17** | | | | | | |
| **18** | | | | | | |
| **19** | | | | | | |
| **20** | | | | | | |
| **21** | | | | | | |
| **22** | | | | | | |
| **23** | | | | | | |
| **24** | | | | | | |
| **25** | | | | | | |
| **26** | | | | | | |
| **27** | | | | | | |
| **28** | | | | | | |
| **29** | | | | | | |
| **30** | | | | | | |

Alvaro Javier Medina Balboa
CI 5991710 LP

**Universidad Mayor de San Andrés**
**Facultad de Ciencias Puras y Naturales**
**Carrera de Informática**

**Formulario de Datos**
**(Fase de Experimentación)**

**Tesista: Univ.** Alvaro Javier Medina Balboa
**Tema:** Autenticación Biométrica para usuarios de celulares mediante Dinámica de Tecleo

GRUPO PERSONIFICADORES

| Nro | Nombres y Apellidos | Profesión | Firma | Uso de celular (años) | PIN elegido | Estado |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |

Alvaro Javier Medina Balboa
CI 5991710 LP

Ejemplo de Perfil digital de un usuario usando la tabla de datos que se almacena en el teléfono celular.

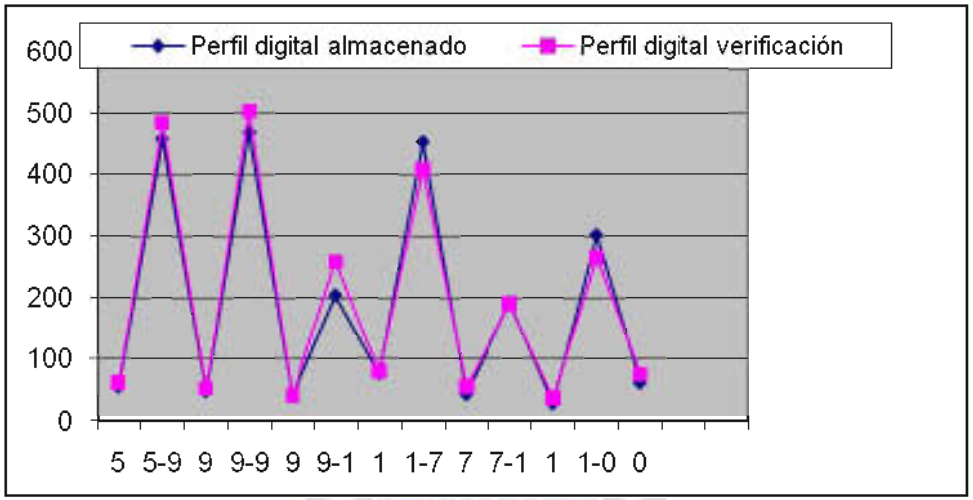
| | 5 | 5-9 | 9 | 9-9 | 9 | 9-1 | 1 | 1-7 | 7 | 7-1 | 1 | 1-0 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Muestra 1 | 38 | 484 | 58 | 478 | 38 | 199 | 72 | 492 | 54 | 185 | 27 | 324 | 56 |
| Muestra 2 | 62 | 485 | 52 | 504 | 41 | 259 | 81 | 407 | 56 | 191 | 37 | 266 | 76 |
| Muestra 3 | 54 | 451 | 59 | 456 | 46 | 192 | 74 | 456 | 18 | 211 | 29 | 306 | 56 |
| Muestra 4 | 51 | 418 | 31 | 462 | 32 | 195 | 80 | 463 | 35 | 192 | 21 | 341 | 45 |
| Muestra 5 | 71 | 443 | 40 | 446 | 42 | 177 | 77 | 440 | 52 | 187 | 26 | 271 | 74 |
| | | | | | | | | | | | | | |
| MEDIAS | 55,2 | 456,2 | 48 | 469,2 | 39,8 | 204,4 | 76,8 | 451,6 | 43 | 193,2 | 28 | 301,6 | 61,4 |
| Des Est | 12,35718415 | 28,56046218 | 12,1449578 | 22,65391798 | 5,215361924 | 31,63542318 | 3,834057903 | 31,24579972 | 16,2788206 | 10,35374328 | 5,830951895 | 32,7001529 | 13,2211951 |
| | Estos son los datos obtenidos en la autenticación estos se pueden modificar | | | | | | | | | | | | |
| Mu Test | 62 | 485 | 52 | 504 | 41 | 259 | 81 | 407 | 56 | 191 | 37 | 266 | 76 |

Utilizando el metodo de Manhattan city block distance metric with standard deviation

$$D(X,Y) = \sum_{i=1}^{n} \frac{|X_i - Y_i|}{\sigma_i}$$

X es el vector de tiempos Muestra Test
Y es el vector de tiempo MEDIAS

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0,550287179 | 1,008387043 | 0,32935479 | 1,536158117 | 0,230089497 | 1,725913375 | 1,095445115 | 1,427391854 | 0,798583652 | 0,212483538 | 1,543487266 | 1,08867992 | 1,10428746 |
| Distancia | 12,65054881 | | | | | | | | | | | | |
| Umbral | ACCEPT | | | | | | | | | | | | |
| % Aceptación | 100 | | | | | | | | | | | | |



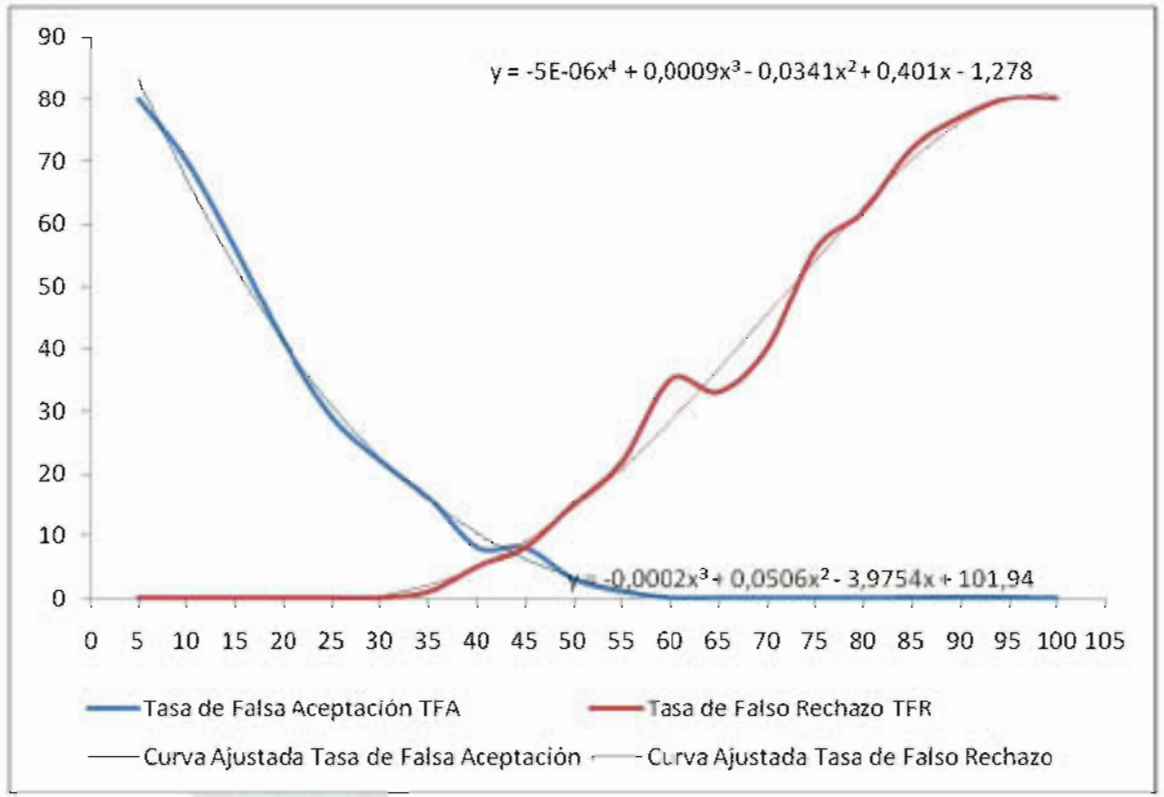

Estas son las distancias de la media con respecto a las muestras

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1,391902864 | 0,973373604 | 0,82338697 | 0,388453777 | 0,345134245 | 0,170694729 | 1,251937274 | 1,292973787 | 0,675724629 | 0,791984095 | 0,171498585 | 0,68501209 | 0,40843509 |
| Distancia 1 | 9,370511735 | | | | | | | | | | | | |
| | 0,550287179 | 1,008387043 | 0,32935479 | 1,536158117 | 0,230089497 | 1,725913375 | 1,095445115 | 1,427391854 | 0,798583652 | 0,212483538 | 1,543487266 | 1,08867992 | 1,10428746 |
| Distancia 2 | 12,65054881 | | | | | | | | | | | | |
| | 0,097109502 | 0,182069883 | 0,90572567 | 0,582680665 | 1,188795733 | 0,391965675 | 0,730296743 | 0,140818927 | 1,535737792 | 1,719184986 | 0,171498585 | 0,13455595 | 0,40843509 |
| Distancia 3 | 8,188875193 | | | | | | | | | | | | |
| | 0,339883257 | 1,337513369 | 1,39975785 | 0,317825817 | 1,495581728 | 0,29713527 | 0,83462485 | 0,364849039 | 0,491436093 | 0,115900111 | 1,200490096 | 1,20488733 | 1,24043249 |
| Distancia 4 | 10,6403173 | | | | | | | | | | | | |
| | 1,278608445 | 0,462177395 | 0,65870958 | 1,024105412 | 0,421830744 | 0,866117701 | 0,052164053 | 0,371249899 | 0,552865605 | 0,598817242 | 0,34299717 | 0,93577544 | 0,95301521 |
| Distancia 5 | 8,51843389 | | | | | | | | | | | | |

| | | | |
|---|---|---|---|
| | 19,74747477 | Umbral de acuerdo al Porcentaje | |
| Prom Dist | 9,873737387 | Este es la media de las distancias | Porcentaje de Umbral 50% |

## Tabla resumen Tasa de Falso Rechazo, Tasa de Falsa Aceptación y Tasa de Error de Cruce

| Umbral U% | % error TFA | % error TFR |
|---|---|---|
| 5 | 80 | 0 |
| 10 | 70 | 0 |
| 15 | 56 | 0 |
| 20 | 41 | 0 |
| 25 | 29 | 0 |
| 30 | 22 | 0 |
| 35 | 16 | 1 |
| 40 | 8 | 5 |
| 45 | 8 | 8 |
| 50 | 3 | 15 |
| 55 | 1 | 22 |
| 60 | 0 | 35 |
| 65 | 0 | 33 |
| 70 | 0 | 40 |
| 75 | 0 | 56 |
| 80 | 0 | 62 |
| 85 | 0 | 72 |
| 90 | 0 | 77 |
| 95 | 0 | 80 |
| 100 | 0 | 80 |

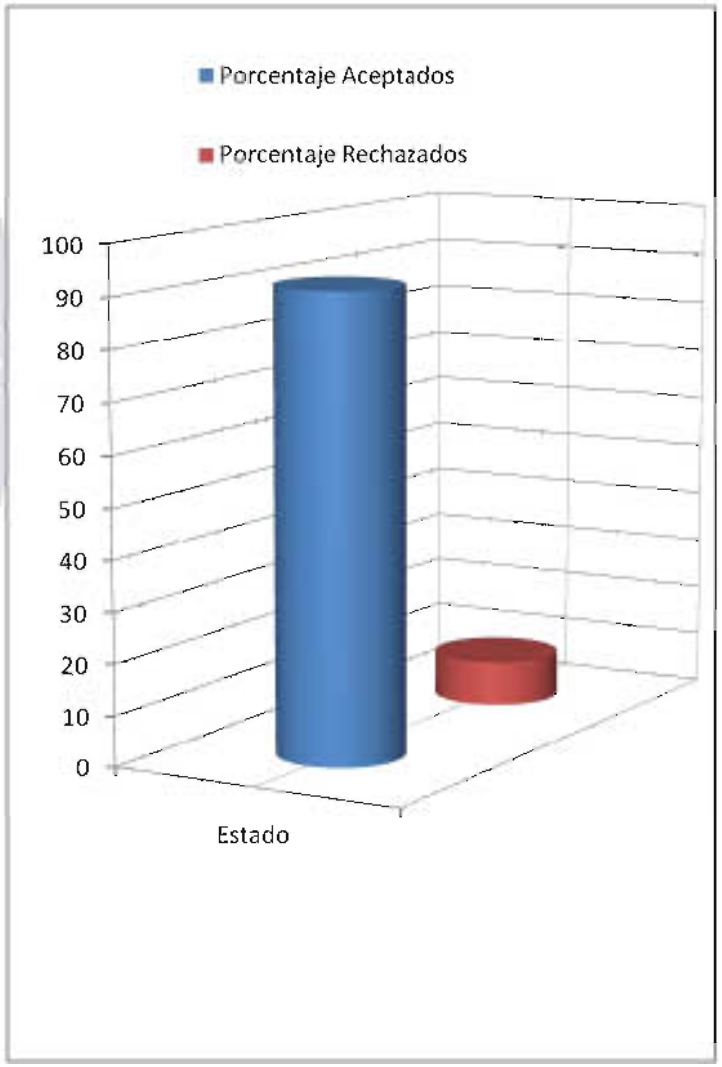


**Primera dinámica** **Objetivo:** medir la Tasa de Falso Rechazo

**Umbral** 45

| Nro | Usuario | PIN | Tamaño Número PIN | Estado |
|---|---|---|---|---|
| 1 | javier2387 | 5991710 | 7 | Aceptado |
| 2 | alvaro | 6767788 | 7 | Aceptado |
| 3 | gareve | 4869203 | 7 | Aceptado |
| 4 | caja18 | 70533418 | 8 | Aceptado |
| 5 | jesus | 6768427 | 7 | Aceptado |
| 6 | ad | 2382385 | 7 | Aceptado |
| 7 | ron | 6725894 | 7 | Aceptado |
| 8 | alejandro | 6097436 | 7 | Aceptado |
| 9 | joseluis | 69498533 | 8 | Aceptado |
| 10 | elva | 70162636 | 8 | Aceptado |
| 11 | CSALINAS | 495001 | 6 | Aceptado |
| 12 | israel | 4091987 | 7 | Aceptado |
| 13 | nadathor | 11111111 | 8 | Rechazado |
| 14 | rafa | 12345678 | 8 | Aceptado |
| 15 | gricel | 6139325 | 7 | Aceptado |
| 16 | valeria | 694748 | 6 | Aceptado |
| 17 | edurcc | 6901043 | 7 | Aceptado |
| 18 | bart | 4652391 | 7 | Aceptado |
| 19 | maria | 5994785 | 7 | Rechazado |
| 20 | roberto007 | 171183 | 6 | Aceptado |
| 21 | lisseth | 54774 | 5 | Aceptado |
| 22 | joel | 54875574 | 8 | Aceptado |
| 23 | nikolass | 12548 | 5 | Aceptado |
| 24 | 2pacftw | 4512154 | 7 | Aceptado |
| 25 | alpha | 54123 | 5 | Aceptado |
| 26 | aaruh | 25484 | 5 | Aceptado |

| | Cantidades | Porcentajes |
|---|---|---|
| **Total Aceptados** | 73 | 91,25 |
| **Total Rechazados** | 7 | 8,75 |



| | | | | |
|---|---|---|---|---|
| 27 | achuracr | 548789 | 6 | Aceptado |
| 28 | adan | 5454578 | 7 | Aceptado |
| 29 | iruzki | 6698577 | 7 | Aceptado |
| 30 | admin1116 | 4111541 | 7 | Aceptado |
| 31 | adrre | 2585587 | 7 | Aceptado |
| 32 | agustin | 554542 | 6 | Rechazado |
| 33 | floresta | 215487 | 6 | Aceptado |
| 34 | alamn | 54565 | 5 | Aceptado |
| 35 | AlanNtojED | 2212586 | 7 | Aceptado |
| 36 | alansakehnn | 72589654 | 8 | Aceptado |
| 37 | AleCrov | 999857 | 6 | Aceptado |
| 38 | shinazu | 7258584 | 7 | Aceptado |
| 39 | alexisbart | 758487 | 6 | Aceptado |
| 40 | Ergo | 5555 | 4 | Rechazado |
| 41 | Amazing | 7895847 | 7 | Aceptado |
| 42 | appletw | 59987485 | 8 | Aceptado |
| 43 | archienm | 58744874 | 8 | Aceptado |
| 44 | ardox | 25888547 | 8 | Aceptado |
| 45 | argmax50 | 72584578 | 8 | Aceptado |
| 46 | mario | 72584785 | 8 | Aceptado |
| 47 | DavidMacat | 589587 | 6 | Aceptado |
| 48 | davidssen | 558748 | 6 | Aceptado |
| 49 | davo | 150689 | 6 | Aceptado |
| 50 | ddiego | 558958 | 6 | Rechazado |
| 51 | deakerr | 72589658 | 8 | Aceptado |
| 52 | demolition | 7258748 | 7 | Aceptado |
| 53 | demolitioooo | 78542598 | 8 | Aceptado |
| 54 | depredavot | 5663587 | 7 | Aceptado |
| 55 | destroyer64 | 5987454 | 7 | Aceptado |
| 56 | Dietw | 45877484 | 8 | Aceptado |
| 57 | dnzkovic | 21455478 | 8 | Aceptado |

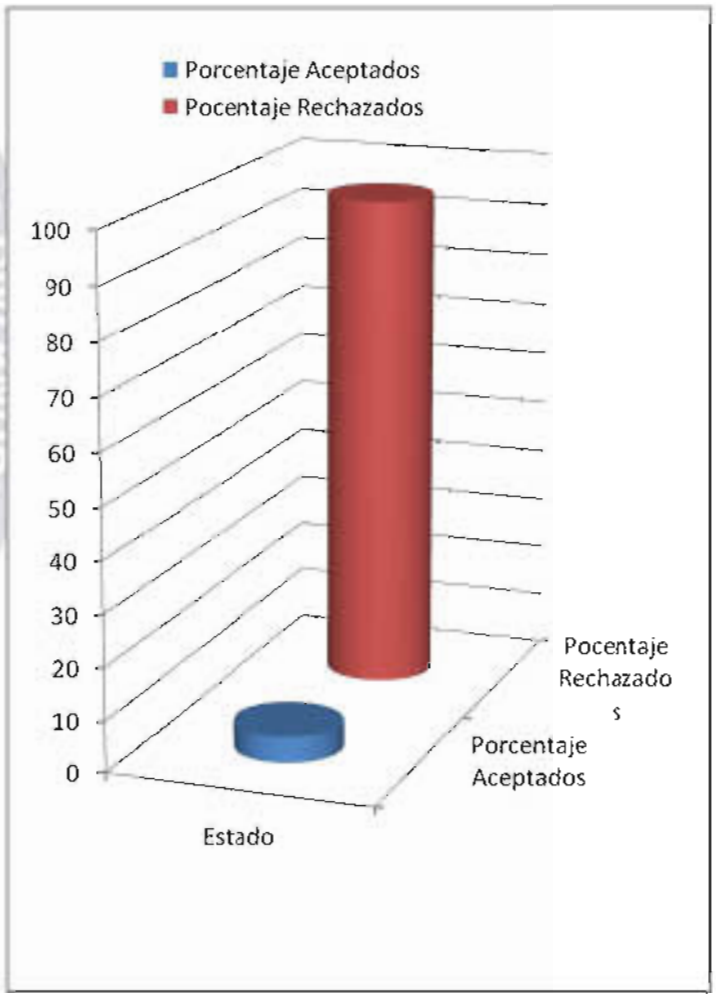
| | | | | |
|---|---|---|---|---|
| 58 | domen01234 | 987654 | 6 | Aceptado |
| 59 | luci | 1234 | 4 | Aceptado |
| 60 | ronis | 59987487 | 8 | Aceptado |
| 61 | driscoll | 58874784 | 8 | Aceptado |
| 62 | dymension | 21457445 | 8 | Aceptado |
| 63 | ekurasko | 22547841 | 8 | Aceptado |
| 64 | elbiotopo | 4445 | 4 | Rechazado |
| 65 | alcapone | 24545478 | 8 | Aceptado |
| 66 | elevar | 4585784 | 7 | Aceptado |
| 67 | elgabye | 11245785 | 8 | Aceptado |
| 68 | elhandless | 12324578 | 8 | Aceptado |
| 69 | elnico | 77895487 | 8 | Aceptado |
| 70 | emiih | 44578754 | 8 | Aceptado |
| 71 | Frox | 12215487 | 8 | Aceptado |
| 72 | emmu | 1125487 | 7 | Aceptado |
| 73 | eqlqe | 559854 | 6 | Aceptado |
| 74 | ericx697 | 559587 | 6 | Aceptado |
| 75 | ermaac | 22255 | 5 | Rechazado |
| 76 | miltton) | 71554874 | 8 | Aceptado |
| 77 | Jorge | 73025847 | 8 | Aceptado |
| 78 | evltn998 | 55487484 | 8 | Aceptado |
| 79 | miky | 71548745 | 8 | Aceptado |
| 80 | antonio66 | 72564785 | 8 | Aceptado |

**Segunda dinámica** **Objetivo:** medir la Tasa de Falsa Aceptación

**Umbral** 45

| Nro | Usuario | PIN | Tamaño Número PIN | Estado |
|---|---|---|---|---|
| 1 | javier2387 | 5991710 | 7 | Rechazado |
| 2 | alvaro | 6767788 | 7 | Rechazado |
| 3 | gareve | 4869203 | 7 | Rechazado |
| 4 | caja18 | 70533418 | 8 | Rechazado |
| 5 | jesus | 6768427 | 7 | Rechazado |
| 6 | ad | 2382385 | 7 | Rechazado |
| 7 | ron | 6725894 | 7 | Rechazado |
| 8 | alejandro | 6097436 | 7 | Rechazado |
| 9 | joseluis | 69498533 | 8 | Rechazado |
| 10 | elva | 70162636 | 8 | Rechazado |
| 11 | CSALINAS | 495001 | 6 | Rechazado |
| 12 | israel | 4091987 | 7 | Rechazado |
| 13 | nadathor | 11111111 | 8 | Rechazado |
| 14 | rafa | 12345678 | 8 | Rechazado |
| 15 | gricel | 6139325 | 7 | Rechazado |
| 16 | valeria | 694748 | 6 | Rechazado |
| 17 | edurcc | 6901043 | 7 | Rechazado |
| 18 | bart | 4652391 | 7 | Rechazado |
| 19 | maria | 5994785 | 7 | Rechazado |
| 20 | roberto007 | 171183 | 6 | Rechazado |
| 21 | lisseth | 54774 | 5 | Rechazado |
| 22 | joel | 54875574 | 8 | Rechazado |
| 23 | nikolass | 12548 | 5 | Rechazado |
| 24 | 2pacftw | 4512154 | 7 | Rechazado |
| 25 | alpha | 54123 | 5 | Rechazado |
| 26 | aaruh | 25484 | 5 | Rechazado |
| 27 | achuracr | 548789 | 6 | Rechazado |

| | Cantidades | Porcentajes |
|---|---|---|
| **Total Aceptados** | 4 | 5 |
| **Total Rechazados** | 76 | 95 |



| | | | | |
|---|---|---|---|---|
| 28 | adan | 5454578 | 7 | Rechazado |
| 29 | iruzki | 6698577 | 7 | Rechazado |
| 30 | admin1116 | 4111541 | 7 | Rechazado |
| 31 | adrre | 2585587 | 7 | Rechazado |
| 32 | agustin | 554542 | 6 | Rechazado |
| 33 | floresta | 215487 | 6 | Rechazado |
| 34 | alamn | 54565 | 5 | Rechazado |
| 35 | AlanNtojED | 2212586 | 7 | Rechazado |
| 36 | alansakehnn | 72589654 | 8 | Rechazado |
| 37 | AleCrov | 999857 | 6 | Rechazado |
| 38 | shinazu | 7258584 | 7 | Rechazado |
| 39 | alexisbart | 758487 | 6 | Rechazado |
| 40 | Ergo | 5555 | 4 | Aceptado |
| 41 | Amazing | 7895847 | 7 | Rechazado |
| 42 | appletw | 59987485 | 8 | Rechazado |
| 43 | archienm | 58744874 | 8 | Rechazado |
| 44 | ardox | 25888547 | 8 | Rechazado |
| 45 | argmax50 | 72584578 | 8 | Rechazado |
| 46 | mario | 72584785 | 8 | Rechazado |
| 47 | DavidMacat | 589587 | 6 | Rechazado |
| 48 | davidssen | 558748 | 6 | Rechazado |
| 49 | davo | 150689 | 6 | Rechazado |
| 50 | ddiego | 558958 | 6 | Rechazado |
| 51 | deakerr | 72589658 | 8 | Rechazado |
| 52 | demolition | 7258748 | 7 | Rechazado |
| 53 | demolitioooo | 78542598 | 8 | Rechazado |
| 54 | depredavot | 5663587 | 7 | Rechazado |
| 55 | destroyer64 | 5987454 | 7 | Rechazado |
| 56 | Dietw | 45877484 | 8 | Rechazado |
| 57 | dnzkovic | 21455478 | 8 | Rechazado |
| 58 | domen01234 | 987654 | 6 | Rechazado |

| | | | | |
|---|---|---|---|---|
| 59 | luci | 1234 | 4 | Aceptado |
| 60 | ronis | 59987487 | 8 | Rechazado |
| 61 | driscoll | 58874784 | 8 | Rechazado |
| 62 | dymension | 21457445 | 8 | Rechazado |
| 63 | ekurasko | 22547841 | 8 | Rechazado |
| 64 | elbiotopo | 4445 | 4 | Aceptado |
| 65 | alcapone | 24545478 | 8 | Rechazado |
| 66 | elevar | 4585784 | 7 | Rechazado |
| 67 | elgabye | 11245785 | 8 | Rechazado |
| 68 | elhandless | 12324578 | 8 | Rechazado |
| 69 | elnico | 77895487 | 8 | Rechazado |
| 70 | emiih | 44578754 | 8 | Rechazado |
| 71 | Frox | 12215487 | 8 | Rechazado |
| 72 | emmu | 1125487 | 7 | Rechazado |
| 73 | eqlqe | 559854 | 6 | Rechazado |
| 74 | ericx697 | 559587 | 6 | Rechazado |
| 75 | ermaac | 22255 | 5 | Aceptado |
| 76 | miltton) | 71554874 | 8 | Rechazado |
| 77 | Jorge | 73025847 | 8 | Rechazado |
| 78 | evltn998 | 55487484 | 8 | Rechazado |
| 79 | miky | 71548745 | 8 | Rechazado |
| 80 | antonio66 | 72564785 | 8 | Rechazado |

# BIBLIOGRAFIA

## Artículos científicos consultados


1. Aguilar, H. J. G., Lizama P. L. A. "Autenticación Biométrica por dinámica de tecleo". División Académica de Informática y Sistemas. México. 2006.
2. Anil K. J., Arun R., Salil P. "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology .2004.
3. Araujo C. "Autentificación Personal por Dinámica de Tecleo Basada en Lógica Difusa", Brazil. 2004.
4. Ashbourn J. "Biometrics: Advanced Identity Verification". Spring. 2000.
5. Carl S., Moran T., "The Keystroke level model for User Performance time with interactive system", 1980.
6. Cheng-Huang J., Shiupyng S., Jen-Chien L., "Keystroke Statistical Learning Model for Web".National Chiao Tung University. Taiwan. 2006.
7. Huidobro J M. "Técnicas de Seguridad Biométricas". Perspectiva Empresarial. 2006.
8. Jerez L. C. A. "Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet". 2002.
9. Joyce R., Gupta G., "Identity Authentication base on keystroke latencies". In Communications of the ACM. Vol. 33. 1990.
10. Marino T. M., "Biometría de tecleo, autenticación de usuarios", Ingeniería Informática, Universidad Autónoma de Madrid, 2000.
11. Matthew A. T., Alex P. P. "Face Recognition Using Eigenfaces". 1991.
12. Monrose F., Aviel D. R. "Keystroke dynamics as a biometric for authentication". Future Generation Computer Systems. 2000.
13. Muñoz. V. N. "Tecnologías Biométricas". EDUBOTS. Robótica Educativa. Chile. 2007.
14. Ruud B., Connell J., Pakanti S. "Guide to Biometrics". Springer. 2003.
15. Sparfford E. "Observing Reusable Password Choices". Technical report. Department of Computer Sciences, Purdue University. 1992.

16. Umphress D., Williams G. "Verifying identity via keyboard characteristics". Academic Press. 1985.
17. Woodward D. J, "Army Biometric Applications: identifying and Addressing Sociocultural Concerns", RAND Corp, 2001.
18. Yau Wei Y. "The '123' of Biometric Technology". Information Technology Standars Committee. 2002.

**Páginas web consultadas**

1. AdmitOneSecurity. 2009. Software AdminteOne Security Suite. Disponible en: http://www.admitonesecurity.com/. Consultado en fecha: 11 de Marzo del 2009.
2. Allmysoft. 2007. Software BioKeyLogon. Disponible en: http://www.allmysoft.com/download-biokeylogon-software.html. Consultado en fecha: 10 de Marzo del 2009.
3. Bowers J. Hansen B. 2006. "How to match on a Mahalanobis distance". Disponible en: http://cran2.arsmachinandi.it/doc/vignettes/optmatch/mahalanobisMatching.pdf. Consultado en fecha: 10 de Marzo del 2009.
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 2009.
5. Gaines SR. Lisowsky W. Press JS. Shapiro N. 1980. "Authentication by keystroke timing: some preliminary results". Disponible en: http://www.rand.org/pubs/reports/2006/R2526.pdf. Consultado en fecha: 5 de Marzo del 2009.
6. Garcia J. 1986. "Personal identification apparatus". Disponible en: http://www.freepatentsonline.com/4621334.html. Consultado en fecha: 6 de Mayo del 2009.

7. 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 2009.
8. Mundo Virtual. 2008. "El celular cumple 35 años". Disponible en: http://tumundovirtual.wordpress.com/2008/04/15/el-celular-cumple-35-anos/. Consultado en fecha: 2 de Marzo del 2009.
9. Online Etymology Dictionary. 2001. "Autenticación". Disponible en: http://www.etymonline.com. Consultado en fecha: 16 de Marzo del 2009.
10. Red Iris. 2002. "Autenticación de usuarios". Disponible en: http://www.rediris.es/cert/doc/unixsec/node14.html#SECTION05510000000000000000. Consultado en fecha: 18 de Marzo del 2009.
11. Sallis E. 2006. "Bluetooth, la amenaza azul". Disponible en: http://www.infobaeprofesional.com/notas/25041-Bluetooth-la-amenaza-azul.html?cookie. Consultado en fecha: 4 de Marzo del 2009.
12. 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 2009.
13. Spaltro JL. 2007. "Inteligencia Biométrica". Disponible en: http://www.info-resumendeseguridad.blogspot.com/2007/08/inteligencia-biomtrica.html. Consultado en fecha: 4 de Marzo del 2009.
14. Wikipedia. 2004. "Biometría". Disponible en: http://es.wikipedia.org/wiki/Biometr%C3%ADa. Consultado en fecha: 18 de Marzo del 2009.
15. Wikipedia. 2005. "Autenticación". Disponible en: http://es.wikipedia.org/wiki/Autenticaci%C3%B3n. Consultado en fecha: 16 de Marzo del 2009.
16. Wikipedia. 2006. "Seguridad de la Información". Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. Consultado en fecha: 13 de Marzo del 2009.

17. Wikipedia. 2007. "Seguridad Informática". Disponible en: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica. Consultado en fecha: 11 de Marzo del 2009.
18. Wikipedia. 2008. "Código Morse". Disponible en: http://es.wikipedia.org/wiki/C%C3%B3digo_Morse. Consultado en fecha: 4 de Marzo del 2009.
19. Wikipedia. 2009. "El Telégrafo". Disponible en: http://es.wikipedia.org/wiki/Tel%C3%A9grafo. Consultado en fecha: 4 de Marzo del 2009.
20. Audiencia Electrónica. 2009. "Celulares: vulnerable a virus". Disponible en: http://www.audienciaelectronica.net/2009/11/25/los-celulares-vulnerables-a-virus/
21. ABI. "En Bolivia la telefonía móvil tiene más de 4 millones de abonados". http://www.abi.bo/

**Tesis consultadas**

1. Borghello A. S. S., Fabian C. "Seguridad Informática: Sus implicancias e Implementación" (tesis licenciatura). Argentina: Universidad Tecnológica Nacional; 2001.

**Revistas Consultadas**

1. Instituto Nacional de Tecnologías de la Comunicación (INTECO). ,"Guía para proteger y usar de forma segura su móvil". España. 2009.