UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

MODELO DE AUTENTICACIÓN DE ACCESO A SISTEMAS DE INFORMACIÓN MEDIANTE DINÁMICAS DE DIGITACIÓN

Tesis presentada por:
Bach. Buitrón Zúñiga Erik Alex.

Para Optar al Título Profesional de:
INGENIERO DE SISTEMAS

ASESOR:
Ing. Juan José Ore Cerrón

ANDAHUAYLAS – APURÍMAC
PERÚ
2015

PRESENTACIÓN

Señor Decano de la Facultad de Ingeniería de la Universidad Nacional José María Arguedas.

Señores miembros del jurado.

Al término de nuestros estudios profesionales y en cumplimiento con la normatividad establecida para optar por el Título Profesional de Ingeniero de Sistemas, pongo a vuestra consideración el presente trabajo de tesis intitulado "**Autenticación de acceso a sistemas de información mediante dinámicas de digitación**", con la finalidad de proponer una alternativa viable y económica para sistema de autenticación.

Esperando que los miembros del jurado eximan las deficiencias que pudieran presentarse y valoren el contenido desarrollado que ejecutara con el estudio y desarrollo tecnológico de nuestra sociedad.

Bach. Erik Alex Buitrón Zúñiga.

RESUMEN

Este trabajo de investigación realiza el estudio de los **"Patrones de Digitación"** y se propone un método alternativo de autenticación basado en estos, que puede ser aplicado en entornos escritorio y Web.

La Alternativa propuesta es el resultado del estudio de los patrones de Dinámica de Digitación, que nos permite diferenciar dos métodos, el primero que es ya bien conocido y llamamos **"Modelo Clásico",** que es un modelo que afirma que los Patrones de Digitación son Constantes en el tiempo, mientras que el segundo, es un modelo propio al cual llamamos **"Modelo Dinámico"** y sostiene que estos patrones cambian con el tiempo, en esta tesis se realiza un estudio comparativo de estos Modelos y se comprueba que el Modelo Dinámico resulta mejor que el modelo Clásico, ya que nos permite alcanzar mejores porcentajes de similitud entre las muestras y por lo tanto mejores niveles de seguridad. Además, producto de este estudio se propone los **"Parámetros de Operación"** del Modelo Dinámico.

Finalmente se implementa un prototipo de autenticación basado en el "Modelo Dinámico" para lo cual se hace uso del enfoque metodológico **"Cascada"**.

Palabras clave: patrones de digitación, autenticación, seguridad, modelo dinámico, modelo clásico, web, remoto.

ABSTRACT

This research is carried out to study the "**kind of works**" and proposes an alternative method of authentication based on these, applied in desk environments.

The alternative proposal is the result of the study of the dynamics of fingering patterns, which allows us to distinguish two methods, the first one is well known and called **"Classical Model"**, a model which claims that fingering patterns are constants in time, instead the second is a specific model know as **"Dynamic Model"** and argues that patterns change over time. In this thesis, we performs a comparative study of these models and we found that the dynamic model is better that the classical model, allowing us to achieve higher percentages of similarity between samples and therefore higher levels of security. Product of this study also proposes the **"Operating Parameters"** Dynamic Model.

Finally, a prototype is implemented based authentication "Dynamic Model" using **“Cascade Method”**

Keywords: Fingering Patterns, Authentication, Security, Dynamic Model, Classical Model, Web, Remotes.

INTRODUCCIÓN

La autenticación juega un papel importante en la seguridad informática, ya que si personal no autorizado accede a cierta información podría ser muy perjudicial para personas e incluso instituciones que manejan información confidencial, ésta situación nos hace reflexionar en lo valioso que es la información y las medidas de seguridad que se deben adoptar, para que únicamente las personas autorizadas tengan acceso a ella.

Existen gran cantidad de métodos de autenticación pero gran parte de ellos son inaplicables a entornos web o dispositivos remotos, dejando como única opción el método usuario-contraseña, que a pesar de su simplicidad y alta vulnerabilidad sigue siendo el más usado, este método hace uso de dos elementos, un elemento de identificación que vendría a ser el nombre del usuario y un elemento de autenticación que vendría a ser la contraseña del mismo, donde el usuario puede ser un nombre o algún tipo de objeto como una tarjeta de identificación y la contraseña es una palabra o texto escogido por la persona. Sin embargo este método presenta algunos inconvenientes debido a su simplicidad, puesto que los usuarios tienden a adoptar como contraseñas palabras obvias, como su nombre, sus iníciales, fecha de nacimiento, las cuales pueden ser fácilmente robadas; un intruso puede ver lo que digita el usuario en el momento de autentificarse ó mediante programas ejecutados en segundo plano, grabar lo que el usuario digita y así conocer su contraseña. De acuerdo a los puntos anteriores, nos damos cuenta que la contraseña no es suficiente para tener la certeza que el usuario es físicamente quien dice ser, bastaría tener el usuario y la contraseña para que exista accesos no autorizados a los recursos de sistemas ya sea en la web o dispositivos de seguridad electrónicos.

En este trabajo se plantea un modelo de autenticación para usuarios tomando como parámetro los patrones de digitación del usuario. El modelo de autenticación se basa en la comparación de registros, cada registro se conforma de los tiempos en el que cada usuario lleva a cabo los eventos pulsar, soltar una tecla, para la comparación de los registros se utilizara funciones estadísticas que nos permiten definir un porcentaje de similitud entre los registros guardados y los recién ingresados, comparando este porcentaje alcanzado, con un valor umbral de aceptación y así decidir la aceptación o rechazo de un usuario.

Para la mejor comprensión del desarrollo de la tesis, dividimos en capítulos, en la siguiente forma:

El Capítulo I: Referido a Aspectos Generales

Identifica el problema, objetivo, metas, limitaciones, justificación, y metodología de la Investigación así como la metodología de desarrollo del prototipo y los antecedentes del proyecto.

El Capítulo II: Referido al Marco teórico en el que se

Mencionan conceptos teóricos de las tecnologías implicadas para el desarrollo del prototipo, marco legal nacional e internacional, marco informático y un breve resumen de conceptos estadísticos.

El Capítulo III: Referido a la Panorámica de los mecanismos de autenticación de Usuarios

En este capítulo se describe los diferentes métodos de autenticación existentes en el mercado, así como sus ventajas y desventajas, además de un estudio comparativo de costos entre el uso de Tokens y el método de autenticación planteado en la presente tesis.

Capítulo IV: Patrones de la Dinámica de Digitación

En este capítulo se define los conceptos de los patrones de la dinámica de digitación, el modelo estático, modelo dinámico, así como el estudio realizado previo al planteamiento de la alternativa propuesta.

Capítulo V: Marco aplicativo.

En esta sección se describe la realización del prototipo, siguiendo el modelo de desarrollo en cascada, por lo cual se siguen las fases que este modelo exige que son: el análisis, el diseño, la implementación y prueba. A lo largo de las fases se presentan los diagramas que posibilitan la realización del prototipo a desarrollar.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1.

ASPECTOS GENERALES

1.1 EL PROBLEMA

1.1.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad se hace evidente la necesidad de desarrollar, nuevos y mejores mecanismos de autenticación, no obstante estos mecanismos implican la inversión de sumas de dinero considerables y tienden a ser dependientes de un hardware específico, lo que conlleva a hacer imposible su implementación en entornos web o aplicaciones remotas.

En la actualidad el método más extendido en entornos web y remotos es el Usuario-Contraseña, pero debido a su simplicidad es muy vulnerable ya que personas maliciosas valiéndose de herramientas tales como el uso de ingeniería social, keyloggers, troyanos, malwares, ataques de fuerza bruta, etc., pueden con facilidad obtener lo que se requiere y hacer una suplantación.

Surge la necesidad de investigar métodos de autenticación que puedan ser aplicados en entornos web y remotos, que no impliquen la inversión de grandes sumas de dinero, además de proveer niveles de seguridad mejores a los ofrecidos por el método Usuario-Contraseña.

1.1.2 FORMULACIÓN DEL PROBLEMA

Es posible encontrar algunos mecanismos de protección que pueda reforzar el proceso de autentificación de acceso a sistemas de información mediante dinámicas de digitación?

1.1.2.1 PROBLEMAS ESPECIFICOS

1. Se podrá obtener indicadores de porcentajes de error menores a 10 %.
2. Es posible desarrollar un prototipo de autenticación basada en patrones de dinámica de digitación bajo el modelo dinámico.

1.2 OBJETIVOS DE LA INVESTIGACIÓN

1.2.1 OBJETIVO GENERAL

Encontrar patrones de la dinámica de digitación y desarrollar un nuevo modelo de autentificación de acceso a sistemas de información mediante dinámica de digitación.

1.2.2 OBJETIVOS ESPECÍFICOS

1. Determinar y validar el umbral de aceptación y de sobre escritura en la autenticación de usuarios en aplicaciones de un cajero automático, mediante los patrones de la dinámica de digitación basada en el modelo dinámico.
2. Desarrollar una aplicación de autenticación basada en los patrones de la dinámica de digitación bajo el modelo dinámico.

1.3 METAS

1. Documento técnico de los patrones de la dinámica de digitación
2. Implementar una aplicación de autenticación, mediante los patrones de digitación.

1.4 LIMITACIONES

1. La contraseña utilizada para cada usuario en el proceso de autenticación, será un número de 8 dígitos que varía entre 00000000 y 99999999.
2. Los patrones de la dinámica de digitación está ligada al estado físico de la tecla en donde se realizara el proceso de muestreo y los procesos de autenticación.
3. El proceso de muestreo y de autentificación de usuarios se debe realizar en el mismo tipo teclado.

1.5 JUSTIFICACIÓN

Los accesos no autorizados a redes sociales, cuentas bancarias, sistemas informáticos, robos a dispositivos electrónicos como por ejemplo cajeros automáticos, por falta de sistemas de seguridad es un problema que afecta a la sociedad, siendo la orientación de esta tesis, el planteamiento de un mecanismo para la autenticación de usuarios de sistemas no solo informáticos sino también de sistemas electrónicos, haciendo uso de dinámica de digitación como una técnica de autenticación conductual, la cual viene a ser un complemento al control de seguridad.

A diferencia de gran parte de los métodos a autenticación existentes, que requieren de dispositivos adicionales para su funcionamiento, la dinámica de digitación, no requiere de ningún dispositivo adicional ya que opera con un teclado que está disponible en todos los equipos de cómputo o equipos electrónicos, lo que implica un costo mínimo en cuanto a equipamiento. El principal beneficio que traería consigo la implementación del método de dinámica de digitación seria el hecho de elevar el nivel de confianza de los usuarios en los diferentes sistemas informáticos y electrónicos.

1.6 METODOLOGÍA

El tipo de metodología a usar en la tesis, será la investigación cuasi experimental, ya que permitirá caracterizar y describir los patrones de la dinámica de digitación, indicando sus rasgos más peculiares o diferenciadores, siendo el objetivo de la investigación experimental; llegar a conocer las situaciones, usos y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas.

1.7 ANTECEDENTES

A lo largo de la historia el ser humano desarrolló varios métodos con el fin de poder autentificarse, gracias a la biometría se tienen el timbre de voz, la forma del rostro, las huellas dactilares, entre otros. Así también el uso de contraseñas, tarjetas de acceso. Son ejemplos de los intentos por encontrar métodos de identificación confiables. El objetivo de esta identificación es permitir a una

persona el acceso a algún recurso físico o informático, con el fin de evitar la suplantación de identidad de personal autorizado.

- **Titulo**: Identificación de usuarios por dinámica de tecleo

  Autor: Licenciado José Guadalupe Aguilar Hernández

  Año: 2007

  País: México

  Resumen: En la investigación "Identificación de usuarios por dinámica de tecleo", realizada en la Universidad Politécnica del Centro en México en el 2007, el Licenciado José Guadalupe Aguilar Hernández, plantea un método para la autenticación de usuarios tomando como parámetro la dinámica de tecleo del usuario. El modelo de autenticación se basa en la comparación de plantillas, cada plantilla se toma de los tiempos en el que cada usuario lleva a cabo los eventos pulsar, soltar tecla y soltar, pulsar tecla entre teclas, dichos tiempos se manejan con una precisión de cuatro cifras, para la comparación de similitud de plantillas se utilizaron funciones estadísticas de dispersión, obteniendo un porcentaje de aceptación (PA) comparado con un porcentaje de similitud (PS). Se decide la aceptación o rechazo de un usuario. Durante las pruebas se calcularon los errores de falsa aceptación y falso rechazo obteniendo 0.0% para el primero

- **Titulo**: Autenticación Personal por Dinámica de Tecleo Basada en Lógica Difusa

  Autor: Livia Cristina Freire Araujo, Miguel Gustavo Lizárraga, Luis Humberto Rabelo Sucupira, João Baptista Tadanobu y Luan Ling Lee

  Año: 2003

  País: Brasil

  Resumen: En la investigación "Autenticación Personal por Dinámica de Tecleo Basada en Lógica Difusa" realizada en Universidad Estatal de Campinas, ubicado en el estado de São Paulo, Brasil en el 2003, Livia Cristina Freire Araujo, Miguel Gustavo Lizárraga, Luis Humberto Rabelo Sucupira, João Baptista Tadanobu y Luan Ling Lee presentaron un método biométrico de autenticación para acceso a sistemas informáticos basado en el

reconocimiento del patrón de tecleo de sus usuarios. El método emplea cuatro características de tecleo: el tamaño de la contraseña a digitar, dos tipos de tiempos entre pulsaciones de teclas consecutivas y el tiempo que cada tecla permanece presionada. Siete experimentos fueron realizados utilizando las características de la secuencia de caracteres en conjunto con un clasificador difuso. Los resultados de los experimentos son evaluados en tres situaciones: usuario legítimo, impostor e impostor especialista. Como resultado de los experimentos se obtuvo tasas de errores de falso rechazo de 3.4 % y de falsa aceptación de 2.9 %.

- **Titulo**: Identificación de Usuarios Basado en el Reconocimiento de Patrones de Tecleo

  Autor: Acevedo Daniel, Glemarys Hernández y Eugenio G. Scalise P

  Año: 2000

  País: Venezuela

  Resumen: En trabajo el trabajo denominado "Identificación de Usuarios Basado en el Reconocimiento de Patrones de Tecleo", realizado por Acevedo Daniel, Glemarys Hernández y Eugenio G. Scalise P, en la Universidad Central de Venezuela, Facultad de Ciencias en el 2000, se plantea un método para la identificación de usuarios basado en el reconocimiento patrones de tecleo utilizando una Red de Base Radial. Para la realización de las pruebas de reconocimiento se tomaron datos generados por los eventos de teclado de una aplicación de mensajería instantánea por Internet. Durante el entrenamiento del modelo se utilizaron datos de tecleo de diecisiete usuarios de habla hispana. Tales datos están conformados por el tiempo transcurrido entre pares de letras tecleadas consecutivamente y el par de letra tecleado por el usuario. Estos pares fueron tomados de una lista de cuarenta pares seleccionados durante el estudio. Como resultado se obtuvo un módulo de reconocimiento de patrones de tecleo con resultados de reconocimiento aceptables

- **Titulo**: Sistema de Protección de Datos usando Dinámica de Tecleo

  Autor: Acevedo Francisco Diego Acosta Escalante, Alejandra Lilí Torres Jiménez

Año: 2005

País: México

Resumen: En el trabajo “Sistema de Protección de Datos usando Dinámica de Tecleo” realizado por Francisco Diego Acosta Escalante, Alejandra Lilí Torres Jiménez en la Universidad Juárez Autónoma de Tabasco en el 2005 se usa la dinámica de tecleo, para medir los tiempos de retardo que cada usuario tiene al dactilografiar. Para ello se propone una metodología basada en la dinámica dactilar en conjunción con dos modelos estocásticos para mejorar la seguridad de la autenticación, uno basado en el comportamiento de los tiempos del usuario y el otro basado en el comportamiento de la totalidad de los tiempos de todos los usuarios

- **Titulo**: Sistema de Autenticación para Dispositivos Móviles basado en Biometría de comportamiento de Tecleo

  Autor: Gerardo Iglesias Galvan

  Año: 2007

  País: México
- **Resumen**: En la tesis titulada “Sistema de Autenticación para Dispositivos Móviles basado en Biometría de comportamiento de Tecleo” para optar grado de: Ingeniero en Sistemas Computacionales en El Instituto Tecnológico Departamento de Sistemas y Computación en México, D.F. en junio del 2007, presentado por Gerardo Iglesias Galvan, refiere que el objetivo de la tesis es 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. los resultados obtenidos una vez concluido la fase de experimentación, 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.

CAPÍTULO 2.
MARCO TEORICO

2.1 MARCO INFORMÁTICO

2.1.1 AUTENTICACIÓN

Es el acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores [11].

2.1.2 MÉTODOS DE AUTENTICACIÓN

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en cuatro categorías

A. **Algo que el usuario es** (ejemplo, la huella digital o el patrón retiniano), la secuencia de ADN (hay definiciones clasificadas de cuál es suficiente), el patrón de la voz (otra vez varias definiciones), el reconocimiento de la firma, las señales bio-eléctricas únicas producidas por el cuerpo vivo, u otro identificador biométrico) [7].

B. **Algo que el usuario tiene** (ejemplo, tarjeta de identificación, símbolo de la seguridad, símbolo del software o teléfono celular) [7].

C. **Algo que el usuario sabe** (ejemplo, una contraseña, una frase o un número de identificación personal (el PIN del paso) [7].

D. **Algo que el usuario hace** (ejemplo, reconocimiento de voz, firma, o el paso) [7].

2.1.2.1 CARACTERÍSTICAS DE LA AUTENTICACIÓN

Cualquier método de identificación debe poseer determinadas características para ser viable:

- **Universalidad**: Si las características se pueden extraer de cualquier usuario o no. Por ejemplo, la universalidad de rostro es muy alta [7].

- **Unicidad**: La probabilidad de que no existan dos sujetos con las mismas características. Por ejemplo, la unicidad de mano y rostro son medias, mientras que las de iris o retina son muy altas [7].

- **Estabilidad**: Si las características que se extraen permanecen inalterables con relación a diversos parámetros (tiempo, edad, ritmo de trabajo, enfermedades, etc.). Por ejemplo, la voz tiene una estabilidad relativamente baja, mientras que el iris y la retina presentan una estabilidad muy alta [7].

- **Facilidad de captura:** Si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto. Por ejemplo, tanto como voz y mano presentan una gran facilidad de captura pues usan un simple micrófono o una cámara de fotos. Por otro lado, las técnicas basadas en retina o en DNA, utilizan sistemas muy complejos [7].

- **Rendimiento:** Denominado también tasas de acierto y error. iris, DNA, retina y algunos métodos de huella presentan unas tasas realmente buenas, mientras que técnicas como oreja o voz presentan tasas bastante bajas [7].

- **Aceptación por los usuarios:** Se trata de un parámetro habitualmente olvidado y sin embargo es el que puede considerarse más importante para un verdadero éxito del sistema. Si los usuarios no aceptan con agrado el sistema, se pueden llegar a negar a usarlo o, lo que puede llegar a ser peor, a usarlo con desidia, falseándose los resultados. Ejemplos característicos de problemas ocurridos por mala aceptación, son retina, por el método de captura de los datos biológicos, y en algunos entornos huella, por su connotación policial o judicial [7].

- **Robustez frente a la burla del sistema:** Si la técnica puede reconocer el falseamiento de los datos capturados (por ejemplo, uso de fotos, dedos de látex, etc.). Esta característica normalmente viene mejorada por técnicas colaterales para detectar sujeto vivo. En el caso de huella, se puede detectar el flujo sanguíneo, o en el caso de voz, cambiando el mensaje a pronunciar por parte del sujeto a reconocer [7].

- **Coste:** Por supuesto a la hora de implantar cualquier tipo de sistema, hay que tener en cuenta el coste del mismo, ya que un excesivo coste puede no estar justificado para el nivel de seguridad que se pretende conseguir. Las técnicas basadas en iris o retina tienen un coste muy elevado, mientras que las basadas en voz presentan uno muy bajo [7].

2.1.2.2 MECANISMO GENERAL DE AUTENTICACIÓN

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable de quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos [14].

El primer elemento necesario (y suficiente estrictamente hablando) para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único. Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como login.

El proceso general de autenticación consta de los siguientes pasos:

1° El usuario solicita acceso a un sistema.

2° El sistema solicita al usuario que se autentique.

3° El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.

4° El sistema valido según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

2.1.3 TECLADO

Dispositivo que integra una gran cantidad de teclas, semejantes a las de una máquina de escribir mecánica. También tiene una serie de botones extras que realizan otras funciones específicas. A través del tiempo, este dispositivo es de los que menos modificaciones han sufrido, ya que por excelencia es el periférico de entrada más común de las computadoras y de los más indispensables, los teclados y computadoras de escritorio, reemplazaron del mercado el uso de las máquinas de escribir mecánicas y máquinas de escribir eléctricas [12].

Figura 0.1 : Teclado convencional alfanumérico.
Fuente [13]

2.1.3.1 DISPOSICIÓN FÍSICA DE LAS TECLAS

La disposición de un teclado actual es la siguiente:

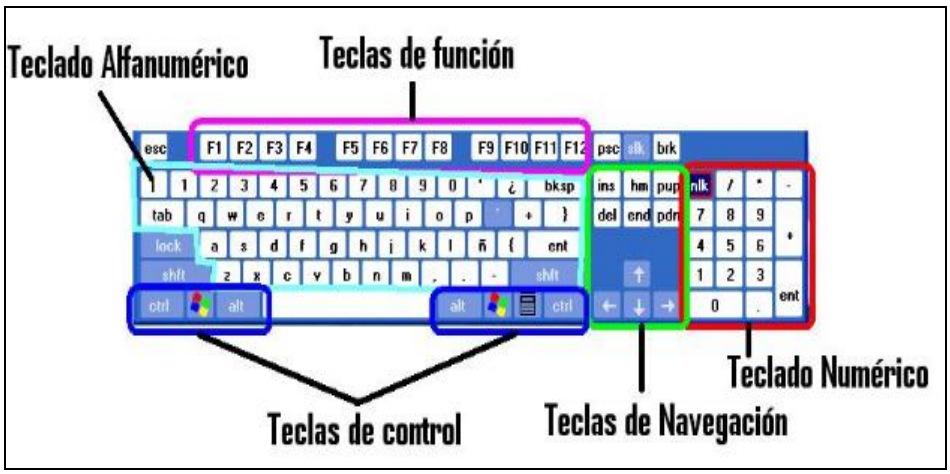


Figura 0.2 : Disposición de teclas.
Fuente **[11]**

- **Teclas de función:** tienen diferentes aplicaciones dependiendo cada programa, ejemplo: F1 comúnmente es para activar la ayuda.
- **Teclado Alfanumérico:** se trata de las mismas teclas que integra una máquina de escribir mecánica.
- **Teclas de Navegación:** se emplean para realizar movimientos del cursor en pantalla.
- **Teclado Numérico:** llevan a cabo operaciones con números, incluyendo símbolos matemáticos. Se debe de activar con el botón "Bloq Num".
- **Teclas de control:** Permiten la realización de operaciones especiales.

2.1.3.2 TIPOS DE TECLADO

Se clasifican de acuerdo a tres criterios principales, el primero de ellos se refiere a la estructura del teclado, el segundo al tipo de pulsador utilizado y el tercero al tipo de aplicación. Existe la posibilidad de combinar las dos estructuras con los distintos tipos de pulsador.

2.1.3.2.1 DE ACUERDO A SU ESTRUCTURA

2.1.3.2.1.1 TECLADOS TIPO SÁNDWICH

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

Figura 0.3 : Teclado tipo sándwich.
Fuente [12]

2.1.3.2.1.2 TECLADOS DE PERFIL BAJO

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

Figura 0.4 : Teclado de Perfil Bajo.
Fuente [8]

2.1.3.2.2 DE ACUERDO AL TIPO DE PULSADOR

2.1.3.2.2.1 TECLADOS DE MEMBRANA

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

- Fabricadas en acero inoxidable (con contactos dorados de forma opcional).

- Diferentes formas y dimensiones para adaptarse a las particularidades de cada diseño, permitiendo crear teclas cuadradas, circulares o rectangulares.
- Diferentes fuerzas de actuación en función del ámbito de funcionamiento.

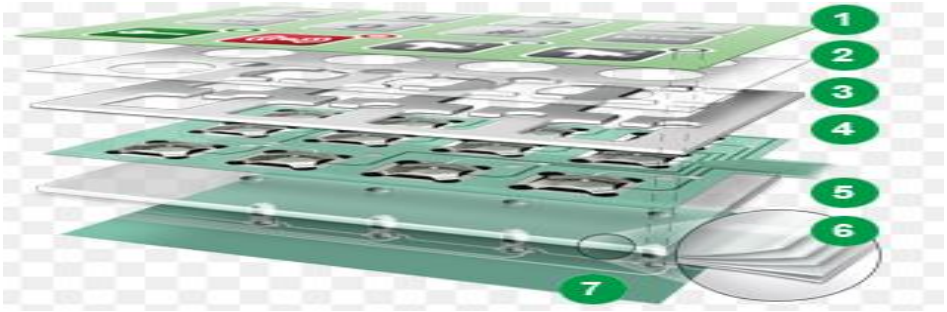


Figura 0.5 : Teclado de Membrana.
Fuente [9]

2.1.3.2.2.2 TECLADOS SENSITIVOS

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

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

Figura 0.6 : Teclado Sensitivo.
Fuente [4]

2.1.3.2.2.3 TECLADOS PIEZOELÉCTRICOS

Los teclados piezoeléctricos están construidos con pulsadores cuyo funcionamiento se basa en el efecto piezoeléctrico. Si se aplica una fuerza a un cuerpo piezoeléctrico, se inducen cargas superficiales por el desplazamiento dieléctrico, por lo tanto se crea un campo eléctrico. Si el cuerpo piezoeléctrico tiene electrodos este campo puede ser transformado en una tensión eléctrica. En un interruptor basado en piezoeléctricos la tensión eléctrica generada es amplificada y acondicionada para producir un impulso eléctrico corto, el cual se usa para producir el cierre de un contacto momentáneo de entre 10 y 1000 ms de duración, dependiendo de la fuerza y velocidad de pulsación.

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

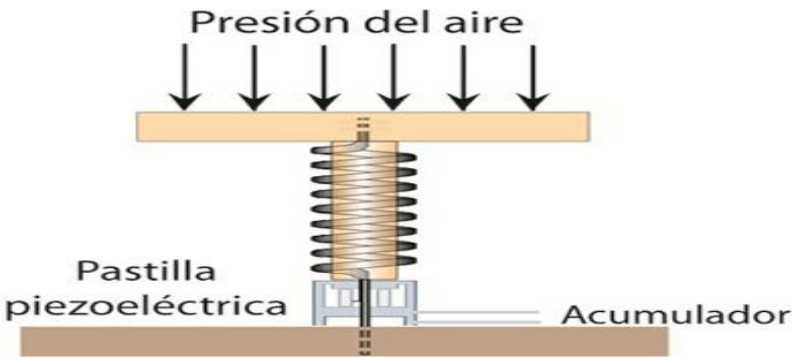


Figura 0.7 : Tecla Piezoeléctrica.
Fuente [10]

2.1.3.2.3 DE ACUERDO A LA APLICACIÓN

2.1.3.2.3.1 TECLADOS ESTANDAR TIPO PC

Se denominan teclados estándar tipo PC, con unas dimensiones y disposición de teclas predefinidas. Estos teclados son conectables a sistemas tipo PC, ya que incorporan un codificador compatible. Entre este tipo de teclado el más común es el QWERTY es la distribución de teclado más común. Fue diseñado y patentado por Christopher Sholes en 1868 y vendido Remington en 1873.

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

Figura 0.8 : Teclado Estándar Tipo PC.
Fuente [1]

2.2 MARCO LEGAL NACIONAL

2.2.1 DE LA PROTECCIÓN DE DATOS PERSONALES

En Perú existe la ley 29733, denominada **Ley de protección de datos personales,** fue aprobada en el 2010 por el Consejo de Ministros y se presentó en la segunda mitad de ese mismo año ante el Parlamento. Debatiéndose a inicios de marzo del 2011 y a finales de abril la ley fue aprobada por la Comisión de Justicia y en junio por el Pleno. El 3 de julio es firmada por el presidente Alan García, esta ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de un adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. Es así, que el fin de esta ley es orientar una **protección efectiva del derecho de la intimidad**, **protección de datos personales** y **bases de datos** que contenga información concerniente a una persona física determinada o determinable", en el blog de "García Sayán abogados", se comenta que esta Ley de Protección de Datos Personales, tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, previsto en la Constitución Política del Perú. Esta Ley regula los datos contenidos o destinados a ser contenidos en Bancos de Datos Personales de administración pública y de administración privada. En ese sentido, ésta Ley no

será aplicable en los casos en que los datos personales estén destinados a ser contenidos en Banco de Datos Personales creados por personas naturales para fines exclusivamente relacionados con su vida o a los contenidos y destinados que forman parte de un Banco de Datos de Administración Pública. Esto sólo se producirá en el caso de que su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas (Defensa Nacional, Seguridad Pública y para el desarrollo de actividades en materia penal para la investigación y represión de delitos). Finalmente, en caso exista una vulneración a los derechos de los titulares, éstos pueden recurrir ante la Autoridad Nacional de Protección de Datos Personales, a través de una reclamación, o ante el Poder Judicial, a través de una Acción de Habeas Data. En ese sentido, la Autoridad Nacional de Protección de Datos Personales tiene a cargo desarrollar las acciones correspondientes para cumplir lo establecido en la Ley, gozando de potestad sancionadora en casos de infracciones, con multas que van desde las 0,5 hasta 100 UIT. Asimismo, tiene a su cargo el Registro Nacional de Protección de Datos Personales [10].

La Constitución Política del Perú, regula el estado de derecho del país. Es el más alto nivel en normas legales y de allí se desarrollan las demás leyes; los temas legales con respecto a la informática son novedosos en el país, a pesar que en países más avanzados ya existen gran cantidad de normas, Aquí se analizan los artículos insertados en la constitución que están relacionados a la informática y que nos pueden guiar para comprender el derecho informático.

En la constitución vigente desde el año de 1993, encontramos los siguientes artículos:

1) En los **DERECHOS FUNDAMENTALES DE LA PERSONA** en el **Artículo 1 de la constitución política** se reconoce a la persona humana como el ente máximo de la sociedad; y dispone todo el poder del estado y de la sociedad para su **protección y respeto**. Los demás artículos tienen que lograr esta finalidad. Aquí no se hace mención a tecnologías específicas, porque está plasmando de manera general que todas las actividades humanas, ya sea utilizando o no **la informática nunca deben ir en contra**

de la dignidad de la persona, y el Estado es que defenderá su cumplimiento [10].

2) En los **DERECHOS FUNDAMENTALES DE LA PERSONA** en el **Artículo 2°, en el numeral 4 se contempla sobre** el **derecho al acceso a la información pública es un derecho humano**. Es decir que por nuestra simple condición de seres humanos, todos nosotros lo poseemos. Por ello, **recibe especial protección por parte del Estado**. Pero este derecho no sólo está garantizado en este artículo, sino que nuestra Constitución también contempla la Acción de **Hábeas Data.** Ésta es una acción de garantía; es decir, un proceso constitucional que tiene por objeto la tutela jurisdiccional de derechos constitucionales tales como el acceso a la información. **El Hábeas Data es entonces el mecanismo a través del cual podemos solicitar judicialmente que se garantice nuestro derecho de acceso a la información cuando consideramos que éste está siendo vulnerado**, es así que el **derecho al acceso a la información pública está regulado por la Ley N° 27806, ley de Transparencia y Acceso a la Información Pública y el Reglamento de la ley aprobado por Decreto Supremo 072-2003-PCM** [10]**.**

3) En los **DERECHOS FUNDAMENTALES DE LA PERSONA** en el **Artículo 2°, en el numeral 5, se menciona** sobre; **hasta qué punto la información personal se puede compartir o distribuir**, no depende del tipo de institución, ya que es igual para las públicas y privadas. La controversia es ¿Cuando se puede decir que afectan la intimidad personal o familiar? El dar el nombre, la dirección, el correo electrónico, el centro de trabajo, etc. Para distintas personas afectará de diferente manera esta información [10].

4) En los **DERECHOS FUNDAMENTALES DE LA PERSONA** en el **Artículo 2°, en los numerales 9 y 10, se puede interpretar que** con la tecnología actual, se va a hablar muy poco del domicilio físico**, y más del domicilio virtual o web.** Como el artículo es general**, también se restringen los ingresos a estos sin el consentimiento del propietario. En el caso de las correspondencias, se debe seguir manteniendo,** como una

forma de **asegurar que los correos electrónicos o mensajes a través de la red, no sean interceptados y utilizados por personas ajenas.** Sólo la autoridad competente puede revisar la correspondencia, pero respetando la intimidad de la persona [10]**.**

2.2.2 DEL CONCEPTO DE DELITO INFORMÁTICO Y RELACIÓN CON OTRAS FIGURAS DELICTIVAS

De manera general, **se puede definir el delito informático como aquél en el que, para su cometido, se emplea un sistema automático de procesamiento de datos o de transmisión de datos**. En la legislación Peruana esta figura se encuentra descrita en el artículo 186°, inciso 3, segundo párrafo, del Código Penal. Este hecho merece ser resaltado puesto que en **otros países se habla de delito informático en sentido de lege ferenda** ya que **carecen de una tipificación expresa de estos comportamientos**. La aparición de estas nuevas conductas merece, no obstante, determinar si las figuras delictivas tradicionales contenidas en el Código Penal son suficientes para dar acogida al delito informático [10].

2.2.2.1 DELITO DE ESTAFA

Entre las conductas defraudatorias cometidas mediante computadora y las defraudaciones en general, dentro de las cuales se encuentra la estafa existe una afinidad o proximidad en los conceptos. Pero al examinar más exhaustivamente los elementos típicos de la estafa, **se acaba concluyendo que el fraude informático y el delito de estafa prácticamente sólo tienen en común el perjuicio patrimonial que provocan**, en donde las secuencia o fases de maniobras o **manipulación** para delinquir es en primer lugar la fase de entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros, o bien se omiten o suprimen datos, estas operaciones tienen un tratamiento informático mediante un programa, este produce una salida de datos ya procesados, la manipulaciones a distancia, en las cuales se opera desde una computadora fuera de las instalaciones informáticas afectadas, a las que se accede tecleando el código secreto de acceso, con la ayuda de un modem, líneas telefónicas, etc.

El punto medular de la **delincuencia informática es la manipulación de la computadora**. La conducta consiste en **modificaciones de datos**, practicados especialmente por empleados de las empresas perjudicadas, con el fin de obtener un enriquecimiento personal, por ejemplo, el pago de sueldos, pagos injustificados de subsidios, manipulaciones en el balance, etc. **El delito de estafa, previsto en el art. 196° CP, se define como el perjuicio patrimonial ajeno, causado mediante engaño, astucia, ardid u otra forma fraudulenta, induciendo o manteniendo prendida por el delito de estafa**.

En primer lugar, y en cuanto al engaño que se requiere en la estafa, éste se refiere de manera directa a una persona física, persona jurídica. Sin embargo, **el problema principal estriba en si la introducción de datos falsos en una máquina equivale al engaño sobre una persona**. **En realidad, para que exista engaño, es requisito la participación de dos personas.** Es indudable que en algunas conductas de **manipulación** fraudulenta sí se podrá configurar el delito de estafa, por ejemplo, cuando el **delincuente informático engaña mediante una computadora a otra persona que se encuentra en el otro terminal**; en este caso, **al haber dos personas, podrá sustentarse el engaño**, en donde el medio empleado para conseguirlo es una computadora. También en la actualidad **se puede plantear el engaño a una persona jurídica, como en el caso en que se solicita un préstamo al banco**, falseando la situación económica real, o en el que ante una compañía de seguros se miente sobre el verdadero estado de salud de la persona. Desde el punto de vista del Derecho Penal, se niega la posibilidad de engañar a una máquina. En este sentido, la computadora es sólo una máquina, un instrumento creado por el hombre. En cuanto al error, como elemento de la estafa, se requiere la concurrencia de dos personas, lo cual se deduce de la descripción del tipo en el art. 196° CP, donde se indica "induciendo o manteniendo en error al agraviado mediante engaño". Además, el error es entendido como el estado psíquico que padece el agraviado como consecuencia del engaño. Por estas razones es que en **la manipulación de computadoras, tal y como está concebida y establecida en el Código Penal, no es posible sustentar que existe un engaño**. De otro lado, no puede sostenerse que la computadora incurre en un error, dado que actúa conforme a

los datos de las instrucciones manipuladas. Por tanto, **no hay estafa en los casos de manipulación de máquinas automáticas**, pues no se puede hablar **ni de error ni de engaño**; sólo podrá plantearse hurto en el caso que se obtenga un bien mueble, pero será un hecho impune cuando se trata de prestación de servicios. Un problema semejante tiene lugar con la manipulación de computadoras a través de la introducción y alteración de programas. En referencia al acto de disposición patrimonial en el delito de estafa, éste ha de realizarlo la persona engañada, quien se encuentra en una situación de error, de ahí que siempre se entienda en la estafa que el acto de disposición es un acto humano, es decir, realizado por una persona. En el caso de las manipulaciones informáticas fraudulentas el acto de disposición lo realiza la computadora, con lo cual se rompe el esquema planteado en el delito de estafa. Finalmente, en cuanto al perjuicio en el delito de estafa, éste no ofrece mayor problema para comprenderlo dentro de la manipulación de una computadora, puesto que en ambos casos normalmente se causa un perjuicio a la persona. **En conclusión, en la legislación peruana, la casi totalidad de supuestos de manipulación de computadoras no puede acogerse dentro del delito de estafa. La única manera sería creando un tipo especial defraudatorio donde se prescinda de los elementos básicos de la estafa, el engaño a una persona y la subsiguiente provocación del error** [10].

2.2.2.2 DELITO DE DAÑOS

El delito de daños se encuentra tipificado en el art. 205° CP. El comportamiento consiste en dañar, destruir o inutilizar un bien. **En el sistema informático, el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito**. Es importante precisar que, si los daños se producen de manera negligente, quedarán impunes dado que el delito de daños sólo puede cometerse de manera dolosa. Estos **hechos se conocen como "sabotaje",** hechos que resultan ser favorecidos gracias a la concentración de información en un mínimo espacio. **La destrucción total de programas y datos puede poner en peligro la estabilidad de una empresa e incluso de la economía**

nacional. El modus operandi de estos actos se viene perfeccionando con el tiempo; en primer lugar, se realizaban con la causación de incendios, posteriormente, con la introducción de los denominados "programas crasch", virus, time bombs (la actividad destructiva comienza luego de un plazo), cáncer roudtine (los programas destructivos tienen la particularidad de que se reproducen por sí mismos), que borran grandes cantidades de datos en un cortísimo espacio de tiempo.

Es indudable que estos **comportamientos producen un daño en el patrimonio** de las personas, por lo que no hay inconveniente en **sancionar penalmente dichas conductas**. Pero es necesario indicar que con el **delito de daños sólo se protege un determinado grupo de conductas que están comprendidas en el delito informático, quedando fuera otras, como por ejemplo, el acceso a una información reservada sin dañar la base de datos**. De ahí que el delito de daños será de aplicación siempre que la conducta del autor del hecho limite la capacidad de funcionamiento de la base de datos [10].

2.2.2.3 EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL PERUANO

La **criminalidad informática en el Código Penal peruano se encuentra recogida de manera expresa como una agravante del delito de hurto en el art. 186°, inciso 3, segundo párrafo**. De esta manera, **el legislador penal** opta por **tipificar esta modalidad delictiva como una forma de ataque contra el patrimonio**, por cuanto éste se configura en el bien jurídico protegido en el delito de hurto, entendiéndose el patrimonio en un sentido jurídico-económico. Por tanto, cabe concluir que se protege un bien jurídico individual. Si bien, es posible que en algunos casos las referidas conductas afecten, además del patrimonio, a la intimidad de las personas, al orden económico, etc. [10].

2.2.2.4 ANÁLISIS DE LA CONDUCTA TÍPICA EN EL DELITO DE HURTO

El comportamiento típico del delito de hurto se encuentra tipificado en el art. 185° Código Penal. La conducta consiste **en apoderarse ilegítimamente de un bien mueble**, total o parcialmente ajeno, sustrayéndolo del lugar donde se

encuentra. En esta conducta estaremos ante un **delito informático si el sujeto activo, para apoderarse del bien mueble, emplea la utilización de sistemas de transferencia electrónica de fondos**, de la telemática en general, o la **violación** del empleo de **claves secretas** [10].

2.2.2.4.1 CARACTERÍSTICAS PARTICULARES DEL DELITO DE HURTO DESDE EL PUNTO DE VISTA DE LA CRIMINALIDAD INFORMÁTICA

1) **EL OBJETO MATERIAL DEL DELITO.-** El objeto material del delito de hurto ha de ser un bien mueble, y por tal interpreta la doctrina un bien corporal o material, aprehensible, tangible, entre otras cosas, porque sólo así es posible la sustracción. Si se parte de la base de que en el uso de computadoras en realidad se trabaja con datos archivados y se maneja únicamente información, se suscita un grave problema a la hora de poder definir dicha información con las mismas características que tradicionalmente se exigen en el bien mueble a los efectos del delito de hurto.

   Es evidente que la **información en sí misma no es algo tangible**; esto no impide que pueda llegar a adquirir corporeidad en **aquellos casos en los que se archiva o grava en medios tangibles** como puede ser una cinta, un disco, disquete, etc. En cuyo caso no se plantearía problema alguno puesto que ya **habría un concreto bien mueble corpóreo** susceptible de ser aprehendido. Por tanto, en cuanto al concepto de bien mueble, se requiere una ampliación de los estrictos límites marcados por un concepto materialista de bien mueble. En base a esto, no habría inconveniente en admitir a **la información computarizada como bien mueble** y, por lo tanto, **objeto material del delito de hurto**, en cuanto sea susceptible de gozar de un **determinado valor económico** en el mercado [10].

2) **LA CONDUCTA TÍPICA.-** En el delito de hurto, el comportamiento típico consiste en apoderarse de un bien mueble mediante sustracción del lugar en el que se encuentra. Por lo tanto, y según esta descripción, sería precisa la concurrencia de un desplazamiento físico del bien

mueble. **En el ámbito de la criminalidad informática es posible, sin embargo, sustraer información sin necesidad de proceder a un desplazamiento físico o material**. Es por ello que la noción de desplazamiento físico se ha espiritualizado, bastando con que el bien quede de alguna forma bajo el control del sujeto activo. Sin embargo, **en la sustracción de información**, **el apoderamiento puede realizarse con una simple lectura o memorización de datos**, de cuya utilización, por lo demás, no queda excluido el titular; de ahí que muchos autores consideren que en este delito, lo que **se lesiona es el derecho al secreto de los datos almacenados**, el derecho exclusivo al control, o un hipotético derecho a negar el acceso a terceros fuera de los que él decida [10].

3) **FORMAS DE EJECUCIÓN DE LA CONDUCTA TÍPICA.-** Como hemos indicado anteriormente, **el delito informático en el Código Penal es un delito de hurto agravado**, y se configura como tal en base a los **medios que emplea el sujeto activo**. Tales son:

   a) **Utilización de sistemas de transferencia electrónica de fondos:** La **transferencia electrónica** de fondos queda definida como aquélla que es iniciada a través de un terminal electrónico, instrumento telefónico o computadora, para autorizar un crédito, o un débito, contra una cuenta o institución financiera Según esta definición, este sistema está referido a la colocación de sumas de dinero de una cuenta en otra, ya sea dentro de la misma entidad bancaria, ya a una cuenta de otra entidad, o entidad de otro tipo, sea pública o privada [10].

   b) **Utilización de sistemas telemáticos:** La telemática es definida como la información a distancia, entendiendo por informática el **tratamiento de información**. A este tipo de conductas se les denomina **"hurto de información",** que se produciría mediante la sustracción de información de una empresa con la finalidad de obtener un beneficio económico. Si en estos casos, la sustracción se produce con la intención de demostrar una simple habilidad, podría constituirse un delito de hurto de uso (art. 187° CP). Si se

destruyen los datos contenidos en el sistema, habría un delito de daños (art. 205° CP) [10].

c) **Violación de claves secretas**: En la violación de claves secretas se protege la obtención de claves por medios informáticos, para su posterior empleo accediendo a estos sistemas. Este es un medio que normalmente concurrirá cuando una persona tiene acceso al password de otro, con lo cual logra ingresar a la base de datos correspondiente y realizar transferencia de dinero o sustraer información. Por tanto, es un medio que mayormente se empleará para configurar las conductas anteriores, sea de transferencia electrónica de fondos o la utilización de la telemática. Si bien, habrá conductas que no emplearán la violación de claves secretas, como los casos del empleado de la empresa que valiéndose de su password accede al sistema realizando las conductas anteriormente señaladas [10].

2.3 MARCO LEGAL INTERNACIONAL

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales, Bajo esta perspectiva, los organismos internacionales que integran el engranaje de la Comunidad Mundial, realizan mancomunados esfuerzos en aras de viabilizar una serie de proyectos que en coordinación con la voluntad de los Estados Nacionales pueden materializarse en un período corto cargado de optimismo.

Según Oliver Hance en su libro “Leyes y Negocios en Internet”, existen tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos: **Acceso no autorizado**, actos dañinos o circulación de material dañino e intercepción no autorizada. Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos **han tipificado y penado y penalizado** estos tres tipos **de comportamiento, ilícito**.

Muchos autores han abordado el tema con singular pasión, clasificando a los delitos informáticos sobre la base de dos criterios: como instrumento o medio, o como fin u objetivo.

Casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos? La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común. Es decir, hay que **unificar criterios**: difícil será actuar contra un **delito que sí lo es en un país y no en otro**. En este sentido está trabajando, por ejemplo, la Unión Europea. Es cierto, de todas formas, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio. Lo que ocurre es que no sólo es eso. Además el avance que está sufriendo Internet en número de usuarios, que parece que vaya a colapsarse en cualquier momento, y en broma se hable ya del ciberespacio, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella: con el aumento de la ciber población, aumentan los posibles delincuentes y los posibles objetivos.

Muchas empresas que en un principio no querían conectarse a Internet, precisamente por los posibles problemas de seguridad, ahora no quieren quedarse atrás, ya que se ha convertido en una cuestión o de pura necesidad o de imagen, y ahora se conectan a marchas forzadas, lo que hace que muchas no tomen las precauciones necesarias y se conviertan automáticamente en jugosos y fáciles objetivos. Internet no estaba pensada y desarrollada para lo que está ocurriendo: su propio diseño no está basado sobre protocolos híper-seguros y, tan es así, que hoy día se estima que no existe un sólo servidor en el mundo que no haya sufrido un ataque contra su seguridad por parte de hackers y crackers. Desde el punto de vista de la seguridad también es preocupante el uso de la criptología por parte de los delincuentes, tanto para ocultar sus mensajes haciéndolos ininteligibles, como para ocultar sus propios movimientos en un sistema informático, haciendo que incluso aunque sean detectados no se pueda saber exactamente qué es lo que estaban haciendo, al estar encriptados los archivos descubiertos. En este sentido,

actualmente es muy inquietante la utilización de cripto-virus (programas con código vírico encriptados). Lógicamente, no es que la criptología sea mala en sí (presenta más ventajas que desventajas): el problema surge cuando es utilizada por malas manos.

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de **aplicar y armonizar en el plano internacional las leyes penales**, a fin de luchar **contra el problema del uso indebido de los programas de computación**. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo **principal problema es la falta de una legislación unificada** que, facilita la comisión de los delitos. En 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales. En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos. En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos [2].

2.4 MARCO TECNOLÓGICO

2.4.1 MICROSFT VISUAL BASIC

Microsoft Visual Basic es un lenguaje de programación desarrollado por el aleman Alan cooper para. El lenguaje de programación es un dialecto de BASIC0, con importantes agregados. Su primera versión fue presentada en 1991, con la intención de simplificar la programación utilizando un ambiente de desarrollo completamente gráfico que facilitara la creación de interfaces gráficas y, en cierta medida, también la programación misma. Desde el 2001 Microsoft

ha propuesto abandonar el desarrollo basado en la API Win32 y pasar a trabajar sobre un framework o marco común de librerías independiente de la versión del sistema operativo, .NET Framework, a través de Visual Basic .NET (y otros lenguajes como C Sharp (C#) de fácil transición de código entre ellos).

Visual Basic (Visual Studio) constituye un IDE (entorno de desarrollo integrado o en inglés Integrated Development Enviroment) que ha sido empaquetado como un programa de aplicación, es decir, consiste en un editor de código (programa donde se escribe el código fuente), un depurador (programa que corrige errores en el código fuente para que pueda ser bien compilado), un compilador (programa que traduce el código fuente a lenguaje de máquina), y un constructor de interfaz gráfica o GUI (es una forma de programar en la que no es necesario escribir el código para la parte gráfica del programa, sino que se puede hacer de forma visual). [13].

2.4.1.1. CARACTERISTICAS

Visual Studio permite a los desarrolladores crear aplicaciones, sitios y aplicaciones web, así como servicios web en cualquier entorno que soporte la plataforma .NET (a partir de la versión .net 2002, se incorpora la versión Framework 3.5 y Framework 4.0 para las ediciones 2005, 2008 y 2010). Así se pueden crear aplicaciones que se intercomuniquen entre estaciones de trabajo, páginas web y dispositivos móviles. Cabe destacar que estas ediciones son iguales al entorno de desarrollo comercial de Visual Studio Professional pero sin características avanzadas. Las ediciones que hay dentro de cada suite son:

Visual Basic Express Edition.

Visual C# Express Edition.

Visual C++ Express Edition.

Visual J# Express Edition (Desaparecido en Visual Studio Express 2008).

Visual Web Developer Express Edition:

Para programación con lenguaje ASP.NET. Está orientado a la programación y diseño web, incluyendo un editor visual WYSIWYG y otro HTML con autocompletado de código (IntelliSense), coloración de sintaxis y validación. Aparte de ASP.NET, también soporta Visual Basic .NET y C Sharp (C#). También tiene un servidor web local para realizar pruebas en ASP.NET, un depurador para ubicar errores en el código fuente y una herramienta de publicación en línea de sitios creados.

2.5 MARCO ESTADÍSTICO

2.5.1 DESVIACION ESTÁNDAR

La desviación estándar (o desviación típica) es una medida de dispersión para variables de razón (ratio o cociente) y de intervalo, de gran utilidad en la estadística descriptiva. Es una medida (cuadrática) de lo que se apartan los datos de su media, y por tanto, se mide en las mismas unidades que la variable. Para conocer con detalle un conjunto de datos, no basta con conocer las medidas de tendencia central, sino que necesitamos conocer también la desviación que representan los datos en su distribución, con objeto de tener una visión de los mismos más acorde con la realidad a la hora de describirlos e interpretarlos para la toma de decisiones [1].

La formula de la desviación estándar es:
Donde:

$$s_i = \sqrt{\frac{(x-\overline{x})^2}{n-1}}$$

- x, es cada uno de los tiempos de la muestra para un evento.
- $\overline{x}$, es el promedio de los tiempos de presión y de cambio.
- n, es el número de muestras tomadas para el perfil.

2.5.2 COEFICIENTE DE VARIACIÓN

En estadística, cuando se desea hacer referencia a la relación entre el tamaño de la media y la variabilidad de la variable, se utiliza el coeficiente de variación.

Su fórmula expresa la desviación estándar como porcentaje de la media aritmética, mostrando una mejor interpretación porcentual del grado de variabilidad que la desviación típica o estándar. Por otro lado presenta problemas ya que a diferencia de la desviación típica este coeficiente es variable ante cambios de origen. Por ello es importante que todos los valores sean positivos y su media sea, un valor positivo. A mayor valor del coeficiente de variación mayor heterogeneidad de los valores de la variable; y a menor C.v, mayor homogeneidad en los valores de la variable. Suele representarse por medio de las siglas C.v [1].

Exigimos que: $\bar{x} > 0$, Se calcula:

$$C_V = \frac{\sigma}{|\bar{x}|},$$

Donde σ es la desviación típica. Se puede dar en tanto por ciento calculando:

$$C_V = \frac{\sigma}{|\bar{x}|} \cdot 100$$

2.5.3 FUNCION DE SCORING

La función de scoring es una función exponencial que se encarga de relacionar los valores de la media y desviación estándar y de esta manera tendremos un vector de valores score, esta función nos indica que tan parecidos o el grado de similitud que existe entre dos conjuntos de datos, con parámetros iguales [9].

La función de scoring es la siguiente:

Donde:

$$\mathbf{S_{(i)} = e^{-\frac{1}{2}Si(Xi-Pi)}}$$

- $S_{(i)}$, function de scoring.
- s_i, es la desviación estándar para cada usuario.
- x_i, es el tiempo de presión y de cambio en un intento de autenticación
- P_i, promedio de los tiempos del perfil conductual de un usuario.

2.5.4 INDICE DE CORRELACION R2

R2, en cualquier modelo de regresión lineal indica que tanta relación hay entre las variables, es decir, que tanto se ve afectado el resultado Y al modificar X, en una ecuación lineal cuando se efectúa la regresión lineal de una ecuación cualesquiera, por consiguiente, si R2 es baja, el modelo no es confiable porque no existe una fuerte relación entre X y Y. Siempre te da un valor de 0 a 1, donde 0 indica que no existe ninguna relación entre X y Y. siendo 1, la máxima relación [1].

2.6 MARCO DE LA METODOLOGÍA

Investigación Cuasi Experimental.

Por medio de este tipo de investigación podemos aproximarnos a los resultados de una investigación experimental en situaciones en las que no es posible el control y manipulación absolutos de las variables.

- Es apropiada en situaciones naturales, en que no se pueden controlar todas las variables de importancia.
- Su diferencia con la investigación experimental es más bien de grado, debido a que no se satisfacen todas las exigencias de ésta, especialmente en cuanto se refiere al control de variables.

Los pasos a seguir para cumplir con el objetivo y las metas de la presente tesis serán las siguientes:

1° Desarrollar el marco teórico, técnico y legal del método de autenticación e identificación mediante los patrones de la dinámica de digitación.

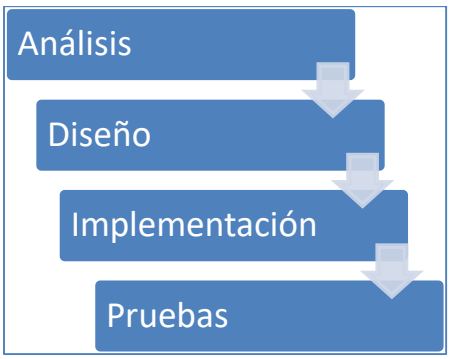
2° Analizar e interpretar los tiempos de los patrones de la dinámica de digitación de un determinado usuario bajo el modelo clásico y el modelo dinámico, mediante la recolección de datos, procesamiento de datos y comparación de gráficas, obtenido al procesar el número de intentos de autenticación y la dispersión de las plantillas del perfil conductual y del último intento de autenticación.

3° Validar los resultados del análisis e interpretación en el modelo propuesto en la presente tesis (modelo dinámico), mediante el ataque de usuarios no

autorizados al prototipo de autenticación e identificación mediante patrones de la dinámica de digitación.

4° Documentar la metodología utilizada para el desarrollo e implementación del prototipo.

5° En la implementación del aplicativo se utiliza el ciclo de vida cascada que es un enfoque metodológico que ordena rigurosamente las etapas del proceso de desarrollo de software, de tal forma que el inicio de cada etapa debe esperar a la finalización de la etapa anterior.



.

Figura 2.90: Fases de la metodología en cascada.
Fuente elaboración propia.

- **Análisis**

  En esta fase se analizan las necesidades de los usuarios finales del software para determinar qué objetivos debe cubrir. Es importante, señalar que en esta etapa se debe consensuar todo lo que se requiere del sistema y aquello que seguirá en las siguientes etapas, no pudiéndose requerir nuevos resultados a mitad del proceso de elaboración del software.

- **Diseño**

  El proceso de diseño del sistema divide los requerimientos en sistemas y establece la arquitectura completa del sistema. El diseño del software identifica y describe las abstracciones fundamentales del sistema software y sus relaciones.

- **Implementación**

  Durante esta etapa, el diseño de software se lleva a cabo como un conjunto o unidades de programas. La prueba de unidades implica verificar que cada una cumpla su especificación.

- **Prueba**

  Los elementos, ya programados, se ensamblan para componer el sistema y se comprueba que funciona correctamente y que cumple con los requisitos, antes de ser entregado al usuario final.

CAPÍTULO 3.
PANORÁMICA DE LOS MECANISMOS DE AUTENTICACIÓN DE USUARIOS

3.1 INTRODUCCIÓN

De una forma constante y casi sin darse cuenta, una persona realiza durante todo el día múltiples identificaciones: reconoce a los componentes de su familia y a sus compañeros de trabajo simplemente viéndolos en persona o en fotografía, a clientes y amigos según se habla con ellos por teléfono, o incluso reconociendo quien ha podido escribir un determinado texto por la caligrafía utilizada. De una forma menos habitual, se puede llegar a identificar a una persona mediante el olor, el tacto o el comportamiento. Y todo esto, y mucho más, lo realiza el cerebro con tal sencillez y velocidad, que lo hace pasar inapreciable. Pero todas estas formas de identificación suponen un previo conocimiento de la persona [9].

Sin embargo, si dos personas que no se han encontrado nunca se encuentran en una situación en la que, al menos una de ellas, necesita autenticar su identidad, se tiene que recurrir a medios alternativos. Imaginemos dos situaciones:

Situación 1: Dos comerciantes se encuentran en una reunión del sector. Ambos se presentan mutuamente, y para constatar su identidad, aparte de transmitir otra información más, como la empresa para la que trabajan, se intercambian unas tarjetas de papel, que comúnmente se denominan tarjetas de visita o tarjetas de empresa.

Situación 2: Un turista quiere coger un avión para irse de vacaciones. Ha comprado un billete con su nombre y para ir a recoger su tarjeta de

> embarque ha de pasar por un mostrador, donde un empleado de la compañía necesita comprobar la identidad de dicho turista, de forma que esté seguro de que le está entregando la tarjeta de embarque al cliente que realmente corresponde. Una vez pasado este trámite, el turista debe pasar por un control de accesos, de forma que xm policía atestigüe que la persona que va a entrar en un avión no es, por ejemplo, un terrorista. Para ambos casos, el turista mostrará un documento acreditativo de su identidad, emitido por una entidad de solvencia reconocida (normalmente un Estado), y que suele ser denominado Pasaporte, o en otros casos, por ejemplo. Documento Nacional de Identidad (DNI).

En estos dos ejemplos queda palpable una de las características más importantes al tratar la identificación de una persona: los requisitos de exactitud de la identificación dependen de la seguridad que se le quiera dar al sistema. Es decir, en el primer caso quedaría demasiado riguroso el que los dos comerciantes se enseñaran el DM, puesto que sólo quieren identificarse para conocerse, compartir un café y, con un poco de suerte, plantear futuras relaciones entre las empresas. En el segundo caso no se admitiría nunca la utilización de una tarjeta de visita, ya que ésta puede ser fácilmente falsificable, y se tiene que asegurar el importe pagado por el cliente, por un lado, y la seguridad del resto de los pasajeros, por otro.

En todos los casos comentados hasta ahora, están siempre presentes los dos actores en el proceso de identificación: el que requiere la identificación y el que se identifica. Sin embargo, con la expansión de las redes telemáticas y la proliferación de distintas soluciones en las que nunca se encuentran cara a cara los dos actores, complican de gran manera el proceso de identificación.

Imaginemos el caso de un Cajero Automático. En este caso, el cliente del sistema quiere obtener un dinero, pero el propietario del Cajero, el Banco, tiene que estar seguro de que el dinero lo saca de la cuenta del cliente apropiado y se lo entrega realmente a dicho cliente. Por tanto el Cajero tiene que realizar un proceso de identificación del usuario, en el que se asegure:

- Un correcto funcionamiento del proceso.

- Un cierto grado de seguridad frente al fraude.

Estas necesidades se plantean cada vez más en los nuevos sistemas que aparecen. Los sectores en los que se requiere una identificación electrónica ya no se limitan instalación bien localizadas y que requieran un número pequeño de sensores, la tendencia es que esta autenticación sea llevada a entornos web y remotos, donde muchos de los mecanismos de autenticación son imposibles de aplicar debido a ciertas limitaciones de la tecnología.

En este capítulo daremos un alcance a los diferentes métodos de autenticación existentes así como las limitaciones que estos tienen al aplicarse a contextos web y remotos, además de los conceptos que se consideran necesarios y finalmente se expondrá a detalle los mecanismos que puedan ser haciendo un estudio comparativo entre estos.

3.2 IDENTIFICACIÓN VS AUTENTICACIÓN

La identificación y la autenticación son conceptos bastante confundidos, pero sus definiciones distan mucho la una de la otra, más que eso, la identificación precede en orden a la autenticación.

En el proceso de autenticación los registros ingresados se comparan solamente con los de un patrón ya guardado, este proceso se conoce también como uno-para-uno. Este proceso implica conocer presuntamente la identidad del individuo a autenticar, por lo tanto, dicho individuo ha presentado algún tipo de credencial, que después del proceso de autenticación será validada o no.

En el proceso de identificación los registros ingresados se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos. Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de este proceso es la identidad del individuo, mientras que en el proceso de autenticación es un valor verdadero o falso.

3.3 MECANISMOS DE AUTENTICACIÓN

3.3.1 MECANISMOS DE AUTENTICACIÓN BIOMÉTRICOS

3.3.1.1 MECANISMOS DE AUTENTICACIÓN BIOMÉTRICOS ESTÁTICOS

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

3.3.1.1.1 HUELLA DIGITAL

Las huellas digitales son el método de identificación de personas más antiguo. Las huellas digitales están formadas por patrones de valles y crestas en las yemas de los dedos, los cuales se forman durante los primeros siete meses de vida del feto. Existen dos técnicas para la identificación de huellas dactilares, en la primera se localizan las terminaciones de crestas, bifurcaciones, puntos y cruces (todos estos elementos se denominan minucias, podemos ver un ejemplo en la Figura 3.1), 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 [9].

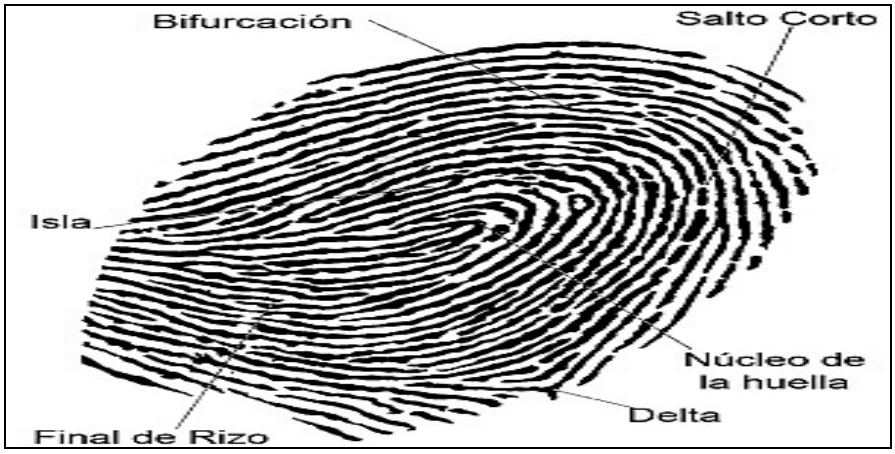


Figura 0.1 : Minucias en una huella digital.
Fuente [3]

La identificación basada en huella dactilar es la más antigua de las técnicas biométricas y ha sido utilizada en un gran número de aplicaciones puesto que la mayoría de la población tiene huellas dactilares únicas e inalterables.

Es el rasgo biométrico más utilizado para autenticación y presenta la mayor gama de tecnologías de captura con distintas características de funcionamiento, asimismo, tiene como ventajas su alta tasa de precisión y que, habitualmente, los usuarios tienen conocimientos suficientes sobre su utilización.

El método utilizado para el análisis de las huellas dactilares comienza a partir de la toma de una imagen de la huella, concluyendo el proceso con la consecución de un registro de ésta, por último, indicar que las huellas dactilares de una pequeña fracción de la población pueden no ser adecuadas para la identificación automática debido a factores genéticos, envejecimiento, medio ambiente, o por motivos profesionales (obreros con un gran número de cortes y contusiones que hacen que sus huellas digitales vayan cambiando).

Ventajas

- Elevado ratio de eficacia.
- Puede llevar a cabo comparaciones 1 a N (Identificación).
- Equipo relativamente económico.
- Facilidad de uso (muestra fácil de tomar y mantener).
- Muy desarrollado e investigado dado su uso desde hace tiempo [9].

Desventajas

- Las imágenes reales de la huella no pueden recrearse a partir de la plantilla.
- Los usuarios relacionan esta técnica con investigaciones policiales y actividades de tipo criminal [9].
- **No apropiado para entornos web y remotos.**

3.3.1.1.2 GEOMETRÍA DE LA MANO

Ofrecen un buen balance entre la velocidad del análisis de las plantillas y son ideales para uso masivo, como control de asistencia y acceso de entradas. Su uso se ha incrementado en los últimos años [9].

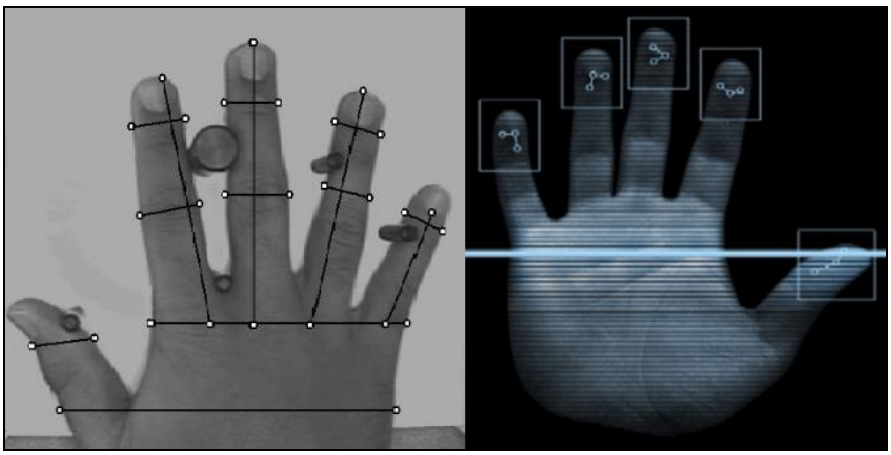


Figura 0.2 : Geometría de la mano con ciertos parámetros extraídos. Fuente [7]

Los sistemas de reconocimiento basados en la geometría de la mano se fundamentan en una serie de medidas tomadas de la mano, incluyendo su forma, tamaño de la palma, longitudes y anchuras de los dedos. Comercialmente se han instalado en todo el mundo cientos de sistemas de verificación basados en la geometría de la mano, La técnica es sencilla, relativamente fácil de usar y de bajo costo. Los factores ambientales como la sequía o anomalías individuales como la piel seca, no parecen tener efectos negativos en la validación del reconocimiento de estos sistemas. Por otra parte, la geometría de la mano no es una característica completamente exclusiva de un individuo, en consecuencia, los sistemas de reconocimiento basados en ella no pueden ser ampliados a sistemas que requieran la identificación de un individuo dentro de una población grande, ya que está presente la variación de la morfología y geometría de la mano a lo largo de la vida. Además, la información geométrica de la mano es variable durante el período de crecimiento, ya sea por causa del uso de joyas (anillos) o ciertas enfermedades (artritis). Esto puede plantear nuevos retos en la correcta extracción de la información [9].

Otro punto a nombrar es el tamaño físico de un sistema basado en este carácter biométrico; se trata de un sistema grande y no puede integrarse en determinados dispositivos portátiles. Existen, no obstante, sistemas de verificación que se basan en mediciones de algunos de los dedos (por lo general el índice medio), en lugar de toda la mano. Estos dispositivos son más pequeños que los utilizados para la geometría de la mano, pero aun así mucho más grandes que los que se utilizan para otros caracteres biométricos (por ejemplo: huellas dactilares, geometría de la cara, voz, etc.).

Ventajas

- Cómodo para usuarios poco acostumbrados a uso de sistemas biométricos dado su fácil uso. (Superficie guiada).
- Apropiado en bases de datos de muchos usuarios dado su poca información almacenada.
- Facilidad de integración en otros sistemas y procesos de control [9].

Desventajas

- Elevado coste de hardware relacionado.
- Gran espacio ocupado por el sistema.
- Variación de la morfología y geometría de la mano a lo largo de la vida.
- Falta de información para realizar la identificación.
- **No apropiado para entornos web y remotos** [9]**.**

3.3.1.1.3 RETINA

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

ingles como intrusive). Para que el lector pueda realizar su trabajo, el usuario no debe tener lentes puestos. [3]

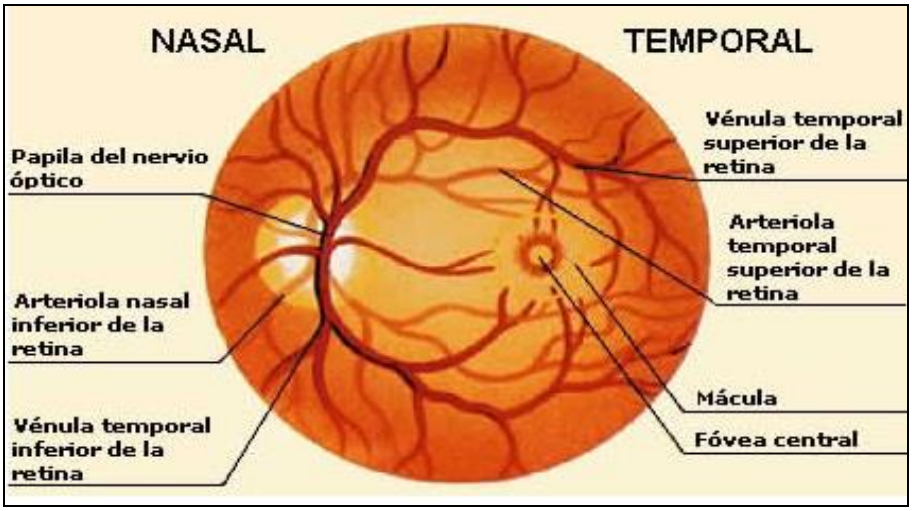


Figura 0.3 : Imagen vasculatura retinal.
Fuente [2]

La vascularización de la retina es rica en estructuras, características de cada individuo y ojo. Es la más segura, ya que no es fácil de cambiar o reproducir. La adquisición de la imagen requiere que una persona mire a través de un ocular, centrándose en un punto específico, de modo que una parte determinada de los vasos retinianos puedan ser reflejados, la adquisición de la imagen implica la cooperación del individuo y el contacto con un ocular. Dichos factores afectan negativamente a la aceptación pública de la retina como técnica de reconocimiento biométrico. Además, la vascularización de la retina puede revelar algunas condiciones médicas, como la hipertensión, siendo éste otro factor disuasorio para su aceptación.

3.3.1.1.4 IRIS

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

la lectura. La facilidad de uso y la integración con otros sistemas no han sido puntos fuertes de los lectores de iris. [5]

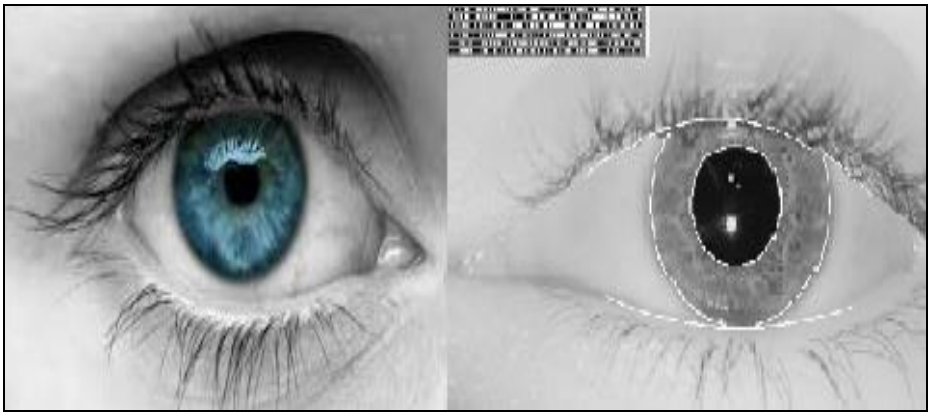


Figura 0.4 : Iris humano con la extracción de su iriscode.
Fuente [6]

La textura del iris se forma durante el desarrollo fetal y se estabiliza durante los dos primeros años de vida. La compleja textura del iris lleva una información muy útil como distintivo de reconocimiento personal, la precisión y la velocidad de los actuales sistemas de reconocimiento basados en el iris son prometedores y punto de partida para la viabilidad de sistemas de identificación a gran escala. Cada iris es distinto, al igual que las huellas dactilares; incluso en gemelos idénticos. Es muy difícil manipular quirúrgicamente el iris y relativamente fácil detectar uno artificial (p.ej. unas lentes de contacto), a pesar que los primeros sistemas basados en el reconocimiento del iris requerían una considerable participación de los usuarios y caros equipamientos, los actuales sistemas se han vuelto más fáciles de usar y económicos.

Ventajas

- Alta precisión y bajos niveles de error.
- Unicidad del rasgo biométrico.
- Poca variación del rasgo a lo largo de la vida.

Desventajas

- Coste de los dispositivos.
- Intrusividad.

- Necesidad de desarrollo de los algoritmos.
- **No apropiado para entornos web y remotos.**

3.3.1.1.5 RECONOCIMIENTO DE LA CARA

Reconocer a personas conocidas por nosotros 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 [8],

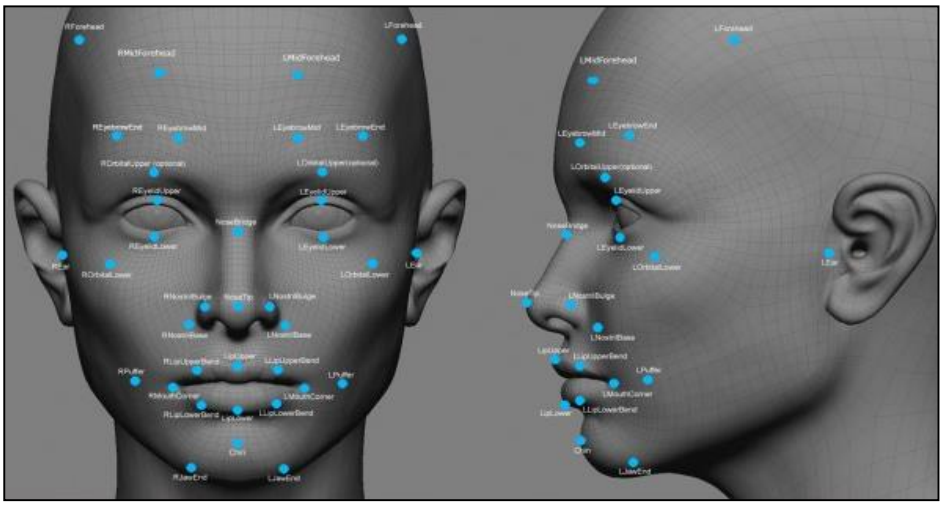


Figura 0.5 : Patrones faciales
Fuente [5]

Es un método no intrusivo y las imágenes faciales son, probablemente, la característica biométrica más comúnmente utilizada por los seres humanos para hacer un reconocimiento personal. Las aplicaciones van desde la aplicación estática y controlada de la toma de imagen, a la identificación dinámica de la cara, con un fondo desordenado y en movimiento (ej. un aeropuerto), los métodos más populares de reconocimiento facial se basan en: la ubicación y la forma de los atributos faciales, como los ojos, cejas, nariz, labios y barbilla y sus

relaciones espaciales, el rendimiento y eficacia de los sistemas de reconocimiento facial disponibles comercialmente es razonable, pero la naturaleza compleja y mutable de los rasgos faciales impone una serie de restricciones tanto en la forma y ángulo de obtención de la imagen, como en el fondo de iluminación, a pesar de su complejidad, todavía se discute si la propia cara, sin ningún tipo de información contextual, es suficientemente identificativa para el reconocimiento mediante computación y qué grado de confianza tiene.

Ventajas

- Elevada tasa de eficacia.
- Puede ser usado desde la distancia.
- Aceptado por muchos usuarios.
- No invasivo.
- No requiere acciones manuales.

Desventajas

- No tiene en cuenta todos los casos, los efectos de la edad.
- Sensible a las condiciones de iluminación.
- Uso casi exclusivo en sistemas de verificación.
- **No apropiado para entornos web y remotos.**

3.3.1.2 MECANISMOS DE AUTENTICACIÓN BIOMÉTRICOS DINÁMICOS

Estos mecanismos se basan en factores asociados al comportamiento de las personas, a cómo se mueven, a cómo articulan sonidos y a cómo interactúan con el sistema que lo está intentando reconocer. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz (o manera de hablar), firma manuscrita (o análisis de escritura), dinámica del tecleo [4].

3.3.1.2.1 RECONOCIMIENTO DE VOZ

Los biométricos de reconocimiento de voz están basados en la verificación del patrón de voz. Su implementación puede ser económica si es realizada en computadoras, ya que la mayoría trae el hardware necesario: micrófonos y bocinas. Sin embargo, factores ambientales,

como el ruido, pueden afectar la comunicación. Además, el patrón de reconocimiento de voz es el que más espacio ocupa de todas las tecnologías biométricas, pudiendo llegar hasta 1MB. Por estas razones, los biométricos de voz son percibidos por los usuarios como dispositivos poco amigables. [4].

La voz es una combinación de datos biométricos fisiológicos y de comportamiento. Las características de la voz de una persona se basan en la forma y el tamaño de los apéndices (p. ej. tractos vocales, boca, fosas nasales y labios) que se utilizan en la creación del sonido. Estas características fisiológicas del lenguaje humano son invariables. Sin embargo, la parte del comportamiento del discurso sí lo es, pudiendo variar con el tiempo debido a los cambios causados por la edad, condiciones médicas (como el resfriado común), estado emocional, etc. También puede verse afectada por factores externos, como el ruido de fondo. En consecuencia, el reconocimiento por la voz puede no ser apropiado para la identificación a gran escala, existen tres sistemas:

Sistemas de texto fijo: el usuario deberá repetir una determinada palabra o una frase concreta, que fue grabada anteriormente. La palabra o frase deberá ser secreta, como una contraseña. Si se graban estas contraseñas puede burlarse el sistema de forma sencilla y sería necesario repetir el reclutamiento para cambiar la palabra o frase utilizada.

Sistemas de texto dependiente: el sistema tendrá almacenado un conjunto muy limitado de frases y palabras que será capaz de reconocer. El usuario se limitará a pronunciar una de estas frases guardadas, esperará entonces a que el sistema le reconozca y le autentique.

Sistemas de texto independiente: este tipo de sistemas proporciona mayores niveles de seguridad en comparación con los dos anteriores. En este caso, el sistema va pidiendo al usuario la pronunciación de unas determinadas palabras extraídas de un conjunto bastante grande.

Ventajas

- Sistemas no invasivos y relativamente fáciles de usar por el consumidor.
- Presentan una gran acogida por parte de los usuarios.

Desventajas

- La voz está sujeta a variaciones.
- Cambios en el volumen, velocidad o calidad y tono de la voz (por ejemplo al estar resfriado).
- A medida que la tecnología sea desarrollada con mayor amplitud podrán reconocerse las voces provenientes de una grabación en lugar de un sujeto vivo, pero actualmente es posible engañar a estos sistemas mediante la utilización de voces grabadas.
- El coste de un micrófono de alta calidad es elevado.

3.3.1.2.2 LECTURA DE FIRMA

La técnica de verificación de firma analiza la manera que el usuario realiza su firma personal. Factores diversos, como la rapidez y presión, son cuantificados, así como la forma de firma. La verificación tiene uno de los niveles más bajos de exactitud entre los lectores biométricos. Sin embargo, su familiaridad con los actuales procesos de verificación manual la hace una de las técnicas más fáciles de introducir al usuario [4].

El modo en que una persona firma es característico de cada individuo. Aunque la firma requiere contacto con el instrumento de escritura y un esfuerzo por parte del usuario, está universalmente aceptada como método de autenticación en operaciones gubernamentales, legales y comerciales. También es cierto que la firma presenta cambios con el tiempo y puede sufrir variaciones debido a condiciones físicas y emocionales. Las firmas de algunas personas varían considerablemente, incluso las impresiones sucesivas de su firma pueden llegar a ser significativamente diferentes, dependiendo del modo de adquisición se pueden distinguir dos modalidades de firma: estática (digitalización de una firma manuscrita) y dinámica (capturada usando dispositivos

especiales con capacidad de registrar la evolución temporal de varias señales generadas por el lápiz al firmar). Además de las coordenadas posicionales, algunos de estos dispositivos proporcionan características adicionales, como, por ejemplo, la presión ejercida sobre el plano de escritura y los ángulos formados entre el lápiz y la superficie de escritura.

Ventajas

- Bastante aceptado por parte de los usuarios.
- Bueno para aplicaciones de autenticación de documentos firmados.
- Elevada cantidad de información derivada del proceso.
- Dificultad para copiar efectivamente el proceso completo de firma.
- No intrusiva y de sencillo uso.

Desventajas

- Elevada variación intra-usuario.
- Afectado por estado del usuario y por el tiempo.
- Los instrumentos empleados, como tablas y lápices electrónicos, resultan caros y complejos.
- Falsificaciones.
- El potencial de miniaturización es reducido.
- Bajo nivel de precisión.
- **No apropiado para entornos web y remotos.**

3.3.2 MECANISMOS DE AUTENTICACIÓN NO BIOMÉTRICOS

3.3.2.1 CONTRASEÑA

Es el sistema típico de identificación en una red de ordenadores. El usuario introduce su "nombre" (identificador de usuario) y su contraseña. Una variación de este método es la utilización de teclados en un sistema de acceso, donde el usuario debe teclear su Número de Identificación Personal (Personal Identificación Number - PIN). La gran ventaja de este método es la no necesidad de una inversión grande en infraestructura, de forma que se tenga que distribuir a los usuarios elementos de identificación. El inconveniente principal es la facilidad con el que las contraseñas pueden ser copiadas y,

sobre todo, la imposibilidad de plantear un control del conocimiento de las mismas, sin perjudicar a los usuarios del sistema.

3.3.2.2 ELEMENTOS DE IDENTIFICACIÓN

Desde el Pasaporte o el Documento Militar, tarjetas inteligentes hasta el uso de dispositivos Token, pasando por cualquier otro tipo de elemento, las soluciones basadas en este tipo de elementos han sido ampliamente utilizadas. El inconveniente de esta técnica es la necesidad de distribuir a cada usuario un elemento de identificación y renovárselo con el tiempo, limitando así este tipo de autenticación a entornos corporativos, donde se conoce con claridad a los usuarios, así como la posibilidad de robo y en algunos casos, la falsificación. La ventaja es que con la tecnología actual se puede plantear sistemas anti-fraude bastante robustos.

3.4 COMPARACIÓN ENTRE LOS DIFERENTES MECANISMOS

En la tabla 3.1 se reflejan los resultados de la comparación realizada. Como se puede comprobar, cada mecanismo cuenta con sus puntos fuertes y débiles, por lo que la elección de una de ellas se deberá basar en el análisis de estas características y las necesidades específicas de cada caso.

TECNOLOGÍA		C1	C2	C3	C4	C5	C6	C7	C8	C9
1.	**Huella dactilar**	M	A	M	A	A	A	M	B	B
2.	**Reconocimiento facial**	A	B	A	B	M	B	A	B	M
3.	**Reconocimiento de iris**	B	A	M	A	A	A	A	A	B
4.	**Geometría de la mano**	M	M	A	M	M	M	M	A	B
5.	**Reconocimiento de retina**	B	A	B	A	A	A	A	A	B
6.	**Geometría de venas**	M	A	M	M	M	M	M	A	B
7.	**Reconocimiento de voz**	A	B	M	B	B	B	M	M	M
8.	**Reconocimiento de firma**	A	B	A	B	B	B	B	A	B
9.	**Forma de andar**	A	M	A	B	B	B	M	M	B
10.	**ADN**	A	A	B	A	A	A	A	A	B
11.	**Contraseña**	A	M	A	A	M	M	A	B	A
12.	**Elementos de Identificación**	A	M	A	A	A	A	A	A	A
(C1)Aceptación (C2)Robustez (C3)Facilidad de Captura (C4)Rendimiento (C5)Estabilidad (C6)Unicidad (C7)Universalidad (C8)Coste (C9) Aplicable en Entornos Web y Remotos / A: Alto M: Medio B: Bajo										

Tabla 0.1 : Comparativa entre métodos de autenticación.
Fuente: elaboración propia.

3.5 COMPARATIVAS

De la tabla anterior podemos afirmar que los mecanismos que se ajustan de mejor modo a las necesidades de autenticación en aplicaciones web y remotas son los mecanismos de (11) contraseña y de (12) elementos de identificación. Cada uno de estos mecanismos tiene diversas variantes que les permite elevar sus respectivos niveles de seguridad, particularmente nos interesa el mecanismo de uso de Tokens, debido a que estos son aplicables en entornos web y remotos, el uso de Tokens es una variante de lo que son los elementos de identificación, ya que debido a su modo de operación permite altos niveles de seguridad y para lo que son los mecanismos de contraseña proponemos el mecanismo de autenticación por Patrones de digitación, a continuación se muestra un gráfico que ilustra la **ventaja económica** que tiene el mecanismo de autenticación por patrones de digitación comparado con el de Tokens.

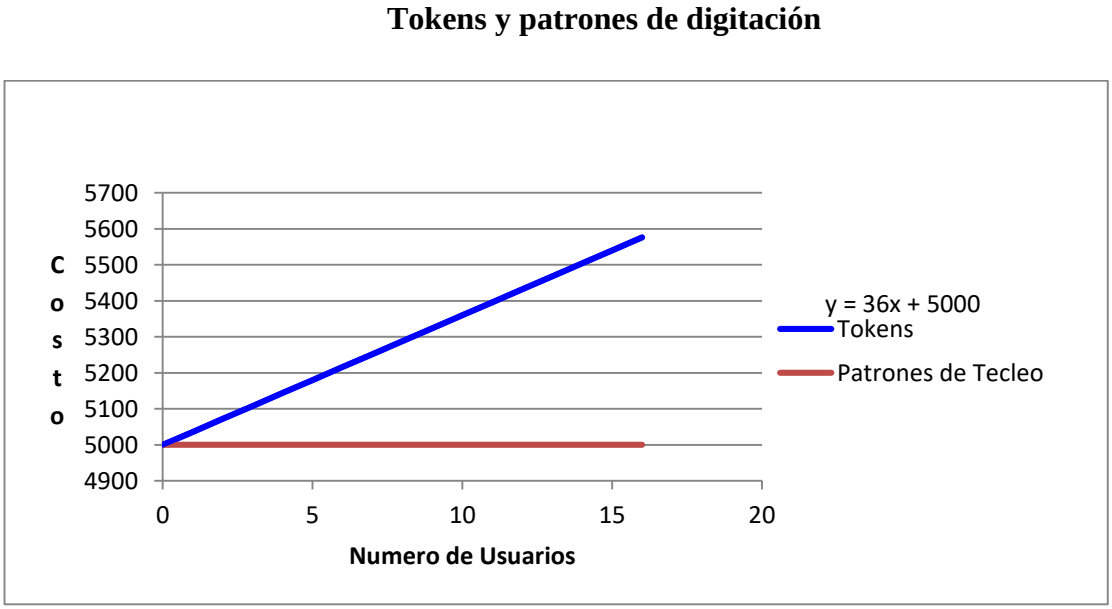


Figura 0.6 : Costo de mecanismos de autenticación.
Fuente: elaboración propia.

Del gráfico podemos deducir que el costo del mecanismo basado en Tokens varía en forma directamente proporcional al número de usuarios, puesto que se requiere un dispositivo Token por cada usuario, mientras que en el caso de los patrones de digitación se tiene un costo único de implementación, por lo tanto podemos

concluir que los patrones de digitación representan una alternativa económica para entornos de aplicación web y remotos.

CAPÍTULO 4.
PATRONES DE LA DINAMICA DE DIGITACIÓN.

4.1 INTRODUCCIÓN

La dinámica de digitación, o biometría de digitación, es la información de tiempo detallado que describe exactamente cuando cada tecla es presionada y soltada por una persona cuando escribe en un teclado de computadora. La dinámica de digitación es una rama de la biometría que se dedica al estudio del reconocimiento del patrón de digitación de un usuario. Es así que la dinámica de digitación utiliza la manera y el ritmo en la cual un individuo escribe con un teclado. Los ritmos de golpes de teclas de un usuario son medidos y registrados por un algoritmo para desarrollar una plantilla biométrica de patrones de escritura de usuarios para autenticaciones futuras.

Este tipo de biometría se centra en las técnicas necesarias para identificar en qué medida existe una cierta regularidad en el modo de digitar de un usuario de un sistema.

El proceso de tecleo es realmente complejo y trasciende el aspecto meramente físico en tanto que es una capacidad emergente que surge de la propia dinámica cerebral en su origen. Desde el cerebro generamos los estímulos necesarios que se transmiten por el sistema nervioso periférico hasta nuestros músculos que efectúan complejas contracciones y distensiones para presionar un centenar de teclas de un ordenador, plasmando la información verbal que el cerebro está procesando en un momento determinado. Además el hecho de no necesitar un hardware adicional para el muestreo de los tecleos hace que sea un sistema ideal para su aplicación sobre Internet, ya que todos los ordenadores comparten la capacidad de admitir el

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

El punto central para el cálculo de patrones en estos sistemas consiste en poder medir en el tiempo con la mayor precisión posible la ocurrencia de estos eventos. Una vez que se tienen registrados todos los eventos ocurridos en la entrada de texto por parte del usuario, el resto consiste en aplicar un algoritmo para la obtención de una medida que represente a la muestra. Existen varias aproximaciones para procesar los datos de tiempo: métodos estadísticos, lógica difusa, redes neuronales [9].

4.2 JUSTIFICACIÓN

4.2.1 JUSTIFICACIÓN SOCIAL

La tendencia actual del desarrollo de sistemas esta en poner estos ya sea en la web o como servicios remotos, no obstante los mecanismos de autenticaciones de los que podemos valernos para aportar algo de seguridad a dichos sistemas son bastante reducidos debido a limitaciones de los propios mecanismos por lo tanto los Patrones de Dinámica de Digitación son una buena alternativa para aportar seguridad a cualquier tipo de sistema.

4.2.2 JUSTIFICACIÓN TÉCNICA

La dinámica de patrones de digitación no tiene grandes requerimientos de hardware como otros mecanismos, basta con tener un teclado, mismo que poseen gran parte de los dispositivos ya sean computadoras o dispositivos como los cajeros automáticos y celulares, en cuanto a su implementación no es necesario

un cambio rotundo puesto que bastaría con agregar unos pocos campos sobre la base de datos de la aplicación.

4.2.3 JUSTIFICACIÓN ECONÓMICA

De lo muchos mecanismos de autenticación de los que se dispone, solo dos son aplicables en entornos web y remotos, esto más que todo limitado por la enorme inversión que representaría poner un sensor del tipo que requieren los diversos mecanismos de autenticación en cada locación en que se pretenda realizar la autenticación, que llevándolo a un entorno web, vendría a ser cada computadora del mundo.

La Primera de estas alternativas vendría ser los Token criptográficos que implican una inversión inicial por la implementación del sistema de autenticación y un coste adicional por cada usuario nuevo, que podemos expresar por la siguiente formula.

$$P = N*X + I$$

Donde:

- P: Precio
- N: Numero de usuarios.
- I: Inversión Inicial.
- X: Precio del Token

La segunda alternativa la constituye los patrones de dinámica de digitación que implica solo la inversión inicial ya que hace uso de los teclados de las computadoras o dispositivos.

Asumiendo una inversión inicial de S/5000 para la implementación de cada uno de los sistemas y un coste de S/15 por token (BCP) y estimando unos 10000 usuarios tendríamos

Precio del sistema de Token: S/155000

Precio del Sistema de Patrón de Dinámica de Digitación: S/5000

Como podemos ver el costo de implementación del sistema basado en Patrón de Dinámica de Digitación es bajo comparado con la alternativa del Token, por lo tanto representa una alternativa económica muy buena.

4.3 MODELOS DE OPERACIÓN

4.3.1 MODELO CLÁSICO

Este modelo se sostiene sobre la idea de que los patrones de digitación tienden a mantenerse constante con el tiempo, y por lo tanto basta con tomar una muestra inicial y los intentos de ingreso futuro serán comparados con la muestra inicial y comparando el porcentaje de similitud con el porcentaje de aceptación se decide la aceptación o rechazo de un usuario.

4.3.2 MODELO DINÁMICO

Este modelo se sostiene sobre la idea de que los patrones de digitación tienden a cambiar con el tiempo, se plantea una comparación entre las plantillas de manera cambiante o dinámica es decir que la primera plantilla obtenida en un proceso previo a un intento de autentificación (muestreo), se actualizara con los datos del perfil conductual de los patrones de la dinámica de digitación en cada acceso positivo al modulo por parte del usuario identificado plenamente, en este sentido se propone un modelo de autentificación e identificación mediante la dinámica de digitación con un valor de aceptación, pero basado en la actualización de la plantilla que contiene las primeras muestras del perfil conductual

MÓDULOS DEL MODELO DINÁMICO

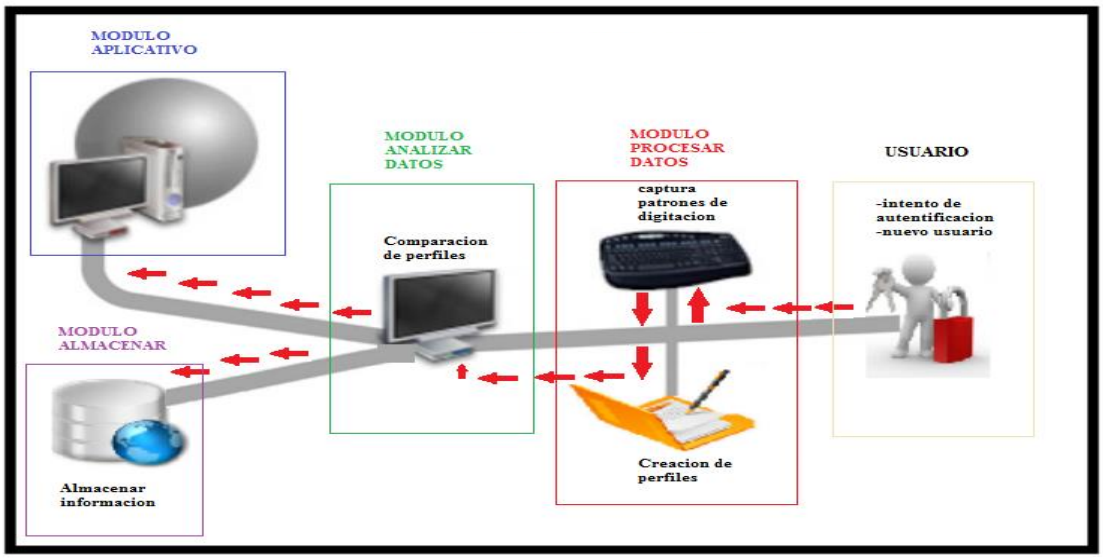


Figura 17: esquema partes del modelo dinámico.
Fuente: elaboración propia.

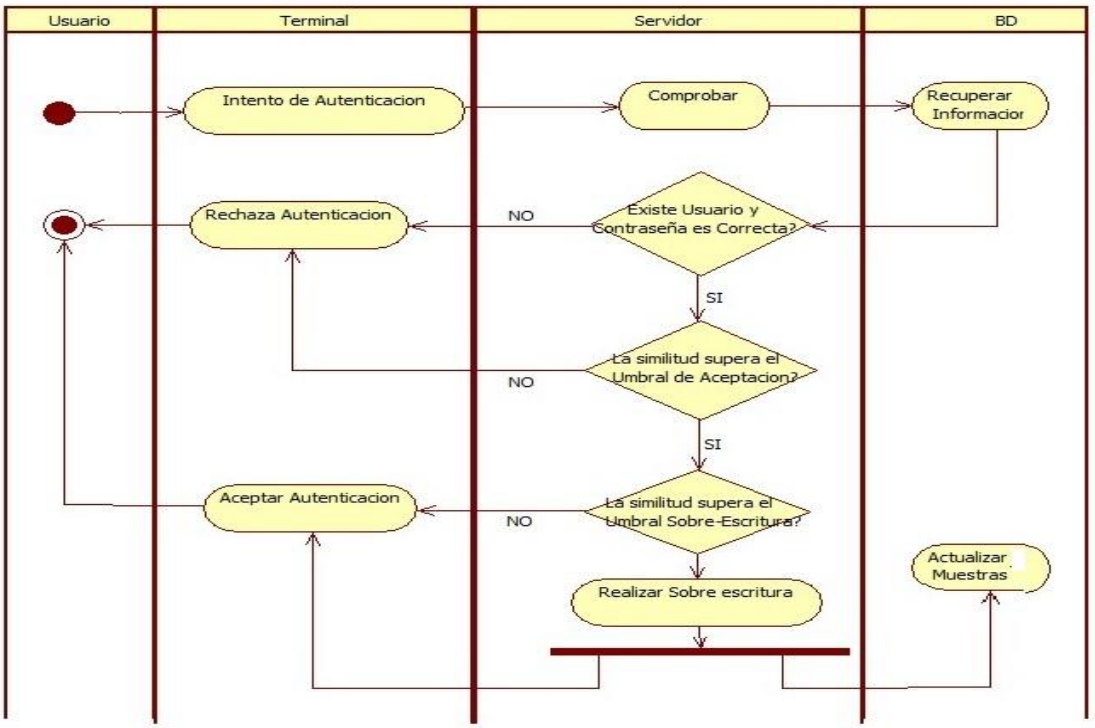


Figura 18: esquema procesos del modelo dinámico.
Fuente: elaboración propia.

4.3.2.1 MODULO PROCESAR DATOS

A. Captura patrón de digitación

En este proceso se captura los patrones de los tiempos de digitación de un determinado usuario, mediante la detección de los eventos del teclado en el lenguaje de programación de con la incorporación de rutinas que se encargan del manejo de los eventos de teclado como son: pulsar tecla, soltar tecla y pulsar tecla entre tecla.

Es así que para medir el comportamiento del usuario ante el teclado se mide las características siguientes:

- El tiempo que transcurre cuando el usuario presiona una tecla y suelta la misma tecla, a este evento llamaremos *pulsar – soltar*.
- El tiempo que transcurre cuando el usuario suelta una tecla y presiona la tecla siguiente, a este evento le llamaremos *soltar - pulsar*.
- El tiempo que transcurre cuando el usuario presiona tecla entre tecla, a este evento le llamaremos tiempo de cambio.

B. Creación de perfiles

En este proceso los eventos del teclado son procesados con modelos estadísticos, los cuales representan los patrones de digitación del usuario en el último intento de autentificación.

4.3.2.2 MODULO ANALIZAR DATOS

Comparación de perfiles

En este modulo se recibirá como parámetros de entrada una lista de tiempos, dicha lista son los tiempos procesados de los eventos *del teclado*, de la misma manera se recibirá la plantilla correspondiente con la que se compararán los nuevos tiempos, los parámetro de salida que enviará el modulo es tres porcentajes el primero se denomina porcentaje de similitud, este indicará en qué medida son parecidos los nuevos tiempos a los tiempos que se encuentran en la plantilla, y de la misma manera se calculará un porcentaje al que llamaremos porcentaje de aceptación (PA) que nos indicará el porcentaje mínimo que debe alcanzar el usuario para poder acceder a una aplicación.

El tercer porcentaje se denominara porcentaje de sobre escritura será determinante para la actualización de la plantilla más antigua del usuario.

4.3.2.3 MODULO ALMACENAR DATOS

Almacenar información

Si el porcentaje de similitud supera el umbral de sobre escritura se almacenara el ultimo patrón de la digitación del usuario, los porcentajes de sobre escritura son valores que muestran que la dinámica de digitación del usuario no permanece constante en el tiempo, ya que es una característica conductual de las personas, en el presente capitulo se detallara este punto.

4.3.2.4 MODULO APLICATIVO

Este modulo es el prototipo basado en los eventos del teclado para capturar los patrones de la dinámica de digitación del usuario, utilizado para la recolección de datos y la autentificación e identificación de usuarios.

4.4 INVESTIGACIÓN

4.4.1 INFORMACIÓN GENERAL

Para la investigación se tomo una muestra de 31 usuarios a los cuales se les pidió que intentasen ingresar al sistema entre 1 a 3 veces al día durante un periodo de 3 meses, mismo que comenzó el 14 de julio del 2015 y termino el 14 de septiembre del 2015, llegando a capturarse un total de 138 intentos de Ingreso por usuario, que dieron lugar a 276 Datos por usuario, que en total hacen 8556 datos de los 31 usuarios.

4.4.2 RECOLECCIÓN DE DATOS

Para la recolección de datos se hizo uso de un aplicativo que permite obtener el porcentaje de similitud alcanzado por un determinado usuario previamente registrado, con respecto al patrón guardado; el porcentaje de similitud se obtiene procesando por los dos modelos de operación, haciendo uso de la función de scoring y estos porcentajes son guardados en la Base de Datos.

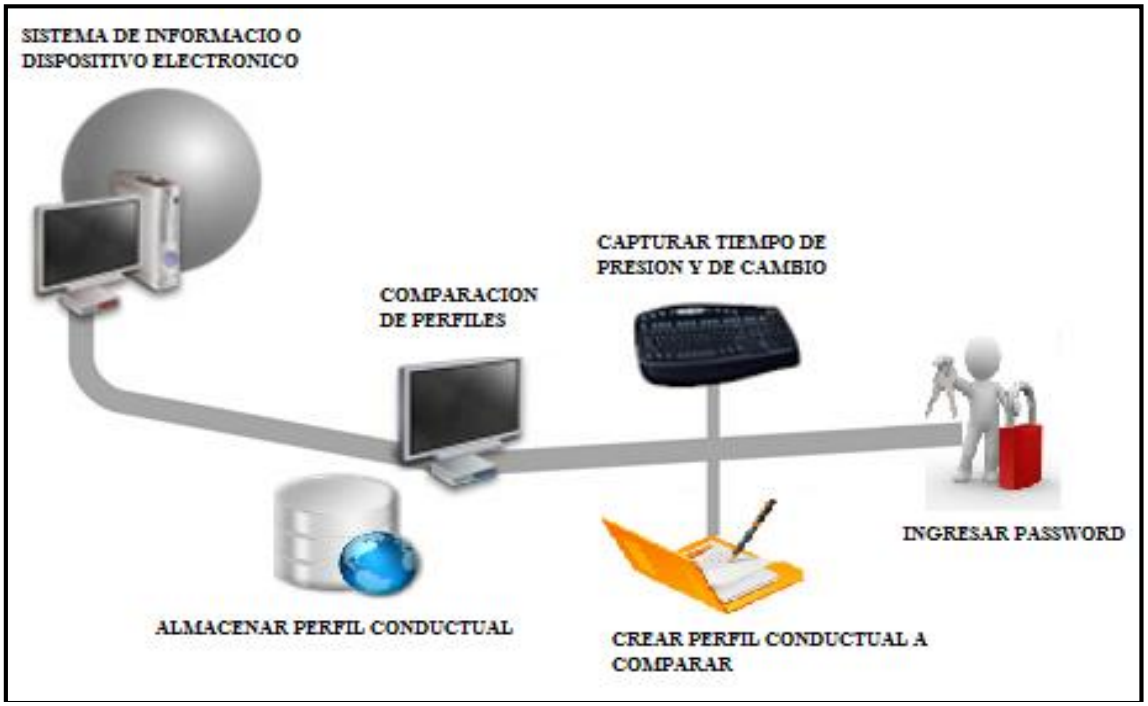


Figura 0.1 : Esquema básico de recolección de datos.
Fuente: elaboración propia.

4.4.3 PROCESAMIENTO DE DATOS

Una vez finalizado la fase de recolección de datos será necesario utilizar un método para procesar la data obtenida y obtener los valores planteados en el objetivo específico, entre los cuales podemos mencionar: modelo markov y modelo gaussiano de la teoría estadística de aprendizaje utilizado en el trabajo hecho por cheng huang jiang, shiuping shieh y jen chien liu [15], para el presente trabajo se utilizara los clasificadores basados en modelos estadísticos.

En este sentido detallamos los pasos a seguir para obtener los valores de similitud para cada usuario, los cuales serán base para determinar el valor de aceptación y de sobre escritura, bajo el modelo dinámico.

Los pasos a seguir para estimar el valor de similitud son:

- Promediar los tiempos de presión y de cambio del muestreo de datos (perfil conductual) para cada usuario.
- Estimar la desviación estándar para cada usuario.

- Promediar los tiempos de presión y de cambio para cada intento de autenticación del usuario.
- Estimar el valor de similitud (scoring), para cada usuario.
- Determinar el porcentaje del valor de similitud.
- Promediar los porcentajes de similitud.

Es así que el vector"M" representa la media o los promedios de los tiempos de digitación de muestreo de un determinado usuario.

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

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

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

Donde:

- M es el vector de tiempo promedio de las muestras conformado por los tiempos medios de presión y de cambio.
- m_i es el i - esimo tiempo medio.
- TP es el tiempo promedio de presión.
- tp_i es el i – esimo tiempo de presión de una tecla.
- TC es el tiempo promedio de cambio.
- tc_i es el i – esimo tiempo de cambio entre dos teclas.
- n es el tamaño de de la contraseña del usuario n=8.

Luego se debe de calcular la variabilidad que existe entre los diferentes tiempos de las muestras, para esto se debe de calcular la desviación estándar para cada dato obtenido en la recolección de datos, el cual estará almacenada en un vector de la siguiente forma.

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

Donde:

$$s_i = \sqrt{\frac{(x-\overline{x})^2}{n-1}}$$

- x Es cada uno de los tiempos de la muestra para un evento.
- $\overline{x}$ Es el promedio de los tiempos de presión y de cambio.

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

Las matrices “M” y ”S” serán utilizada para realizar la comparación entre el promedio de los tiempos de pulsación y de cambio, obtenidos en un intento de autenticación por un determinado usuario, para esto se utilizara la función de scoring.

Los valores de similitud para cada usuario estarán almacenados en la siguiente matriz.

$$S_{(n)} = \{s_{(1)}, s_{(2)}, s_{(3)}, \ldots\ldots, s_{(n)}\}$$

Donde:

$$s_{(i)} = \exp((-1/2\ s_i)(x_i - P_i))$$

- si Es la desviación estándar para cada usuario.
- xi Es el tiempo de presión y de cambio en un intento de autenticación
- Pi Promedio de los tiempos del perfil conductual de un usuario.

Para estos valores le determinamos su porcentaje, aplicándoles la covarianza a cada una de los valores de scoring, obteniendo las siguientes tablas.

Muestras	U-1	U-2	U-3	U-4	U-5	U-6	U-7	U-8	U-9	U-10
1	48.96	56.21	55.29	48.74	56.40	47.90	47.76	46.59	54.41	58.27
2	34.97	45.77	39.07	31.56	58.46	43.91	56.28	40.10	42.72	59.64
3	32.24	50.04	52.48	43.19	61.29	36.97	46.25	35.93	50.86	68.80
4	40.89	57.46	54.35	37.92	54.67	44.60	45.18	35.26	46.89	48.63
5	39.59	56.23	46.59	51.41	55.19	37.07	47.65	45.21	50.48	55.13
6	48.67	55.41	52.35	38.38	59.06	44.25	55.50	44.65	41.17	58.78
7	61.17	58.11	49.72	34.14	56.61	50.20	49.65	46.12	57.33	58.52
8	39.51	53.42	53.21	29.88	55.40	45.74	54.58	39.21	45.00	45.38
9	47.53	60.16	48.97	44.34	53.66	41.18	57.21	43.14	45.72	62.41
10	50.67	54.23	45.87	41.04	56.69	40.80	56.45	43.70	50.45	56.36
11	46.31	58.54	48.31	34.90	58.87	45.45	47.36	53.69	46.82	58.92
12	33.16	53.69	51.92	39.66	60.00	49.68	52.47	49.59	46.14	52.02
13	59.74	52.76	47.47	35.04	48.45	43.75	41.99	33.65	53.37	58.28
14	53.55	43.95	46.05	39.54	51.77	41.57	56.48	36.12	50.72	48.53

Tabla 0.1: Similitud bajo el modelo clásico.
Fuente: elaboración propia
Tabla completa: Anexo C

Muestras	U-1	U-2	U-3	U-4	U-5	U-6	U-7	U-8	U-9	U-10
1	48.96	56.21	55.29	48.74	56.40	47.90	47.76	46.59	54.41	58.27
2	37.31	48.22	43.01	38.00	61.60	48.86	58.09	47.20	47.78	59.09
3	36.75	59.12	52.40	58.67	60.37	44.18	47.14	44.26	53.06	69.08
4	38.34	56.62	56.13	56.14	60.90	53.11	44.23	40.48	47.96	48.47
5	44.22	52.83	53.32	60.77	58.35	52.72	46.38	59.12	57.68	56.68
6	52.41	54.36	62.96	57.78	62.93	47.81	51.23	55.34	51.43	57.77
7	51.50	58.53	62.14	52.48	62.34	60.60	50.18	54.22	55.13	62.56
8	46.82	50.53	61.07	49.55	53.94	59.60	55.42	57.41	54.64	61.92
9	54.60	57.39	63.39	58.99	61.71	61.83	54.91	60.37	63.17	65.71
10	57.79	50.79	59.32	55.23	64.22	61.06	49.24	52.55	62.08	71.04
11	57.29	56.60	63.00	58.24	66.60	54.20	50.42	59.23	67.97	72.12
12	55.90	64.30	65.51	64.82	66.59	51.33	56.30	46.00	62.86	69.32
13	56.68	65.12	63.36	57.28	53.67	49.20	50.88	55.15	58.81	62.16
14	55.31	59.12	60.87	65.05	63.61	45.13	53.71	51.75	57.71	68.63

Tabla 0.2: Similitud bajo el modelo dinámico.
Fuente: elaboración propia.
Tabla completa: Anexo D

Luego se promedian los valores de similitud para cada muestra los promedios con sus respectivos errores estadísticos en la siguiente tabla, de la cual nos valdremos para realizar el estudio diferenciado por los dos modelos de operación.

	Modelo Clásico	
Muestra	**Porcentaje**	**Error**
1	53.73	1.62
2	51.50	1.87
3	51.33	1.74
4	51.81	1.76
5	52.34	1.52
6	51.38	1.42
7	52.41	1.68
8	49.78	1.62
9	52.01	1.50
10	52.07	1.53
11	53.05	1.64
12	51.64	1.80
13	50.69	1.55
14	50.92	1.42

Tabla 0.3: Porcentajes de similitud para el modelo clásico.

Fuente: elaboración propia.
Tabla completa: Anexo C

	Modelo Dinámico	
Muestra	**Porcentaje $S_{(n)}$**	**Error (e_m)**
1	53.73	1.62
2	53.83	1.67
3	54.56	1.36
4	54.91	1.61
5	56.43	1.37
6	57.33	1.26
7	57.54	1.03
8	57.11	1.12
9	60.04	0.82
10	58.90	1.26
11	60.48	1.39
12	59.78	1.24
13	58.52	1.27
14	59.73	1.11

Tabla 0.4: Porcentajes de similitud para el modelo dinámico.
Fuente: elaboración propia.
Tabla completa: Anexo D

Finalmente se promedian los porcentajes de similitud y sus respectivos errores estadísticos (e_m), siendo esta media o promedio un **valor tentativo como umbral de sobre escritura** planteado para los dos modelos respectivamente.

	Modelo Clásico		Modelo Dinámico	
	Porcentaje de similitud promedio	**Error**	**Porcentaje de similitud promedio**	**Error**
Promedio	**49.12**	**1.75**	**58.00**	**1.31**

Tabla 0.5: Porcentajes promedios de similitud para el modelo dinámico y clásico.
Fuente: elaboración propia.

Es así que el valor de aceptación tentativo para los dos modelos estará dado por el mínimo valor del rango de variación de los valores de similitud, es decir:

$$VA=VE- e_m \text{ .....(*)}$$

Donde:

$$e_m = \frac{\sum(xi - X)}{n}$$

- e_m: error media aritmética o la media aritmética de los errores.
- VE: valor de sobre escritura.
- VA: valor de aceptación tentativo.
- x_i : Tiempo de presión y de cambio en un intento de autenticación de un determinado usuario.
- X: media aritmética o promedio de los tiempos de cambio y de presión.
- n : es el número de muestras tomadas para el perfil.

Sustituyendo en ecuación (*):

Modelo Clásico	**Modelos Dinámico**
VA = 49.12 % – 1.75 %	VA = 58.00 % – 1.31 %
VA = 47.37 %	**VA = 56.69 %**

4.4.3.1 PROCESAMIENTO DE DATOS DEL MODELO CLÁSICO

De la distribución de los datos de la tabla 10 obtenemos la siguiente grafica:

Modelo clásico

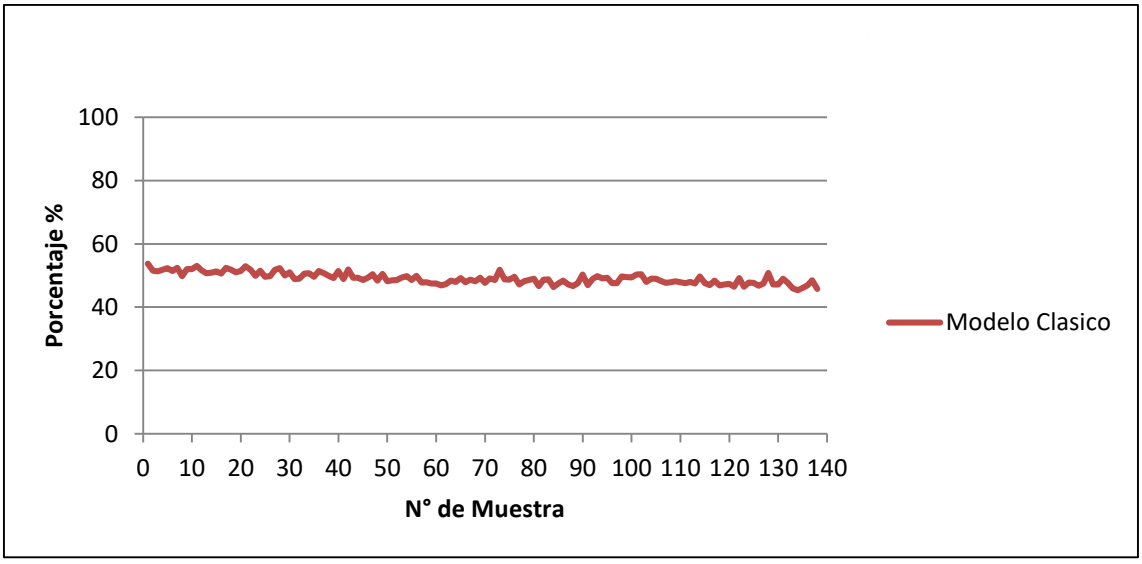


Figura 0.2 : Porcentaje de similitud vs numero de muestras bajo modelo clásico.

Fuente: elaboración propia.

Aplicando regresión lineal a esta grafica se obtiene:

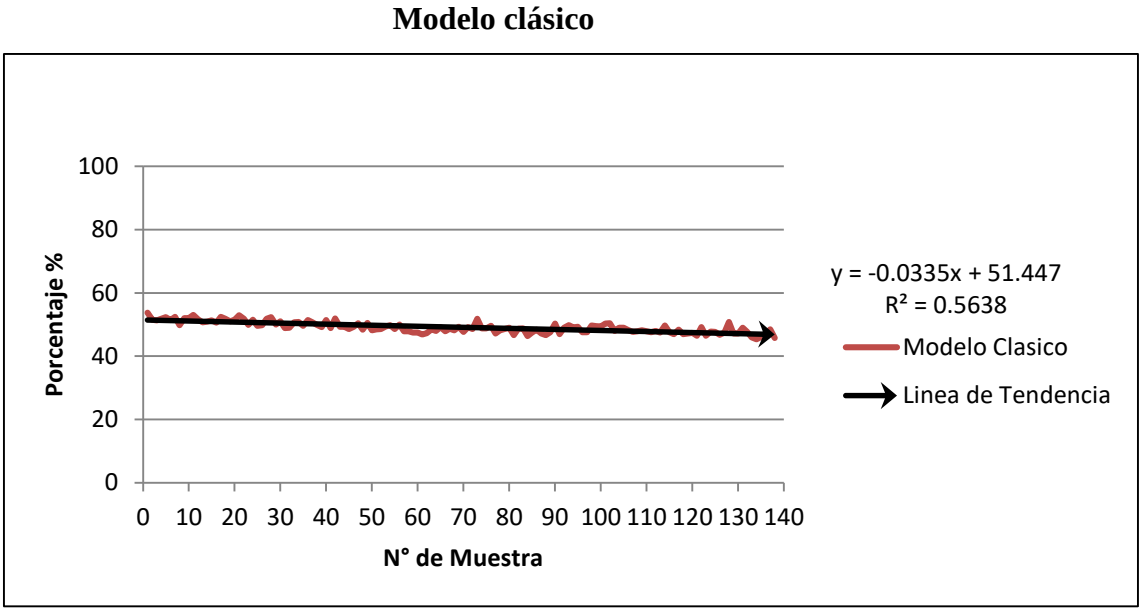


Figura 0.3 : Regresión lineal de la curva del modelo clásico.
Fuente: elaboración propia.

4.4.3.1.1 ANÁLISIS DEL MODELO CLÁSICO

De la ecuación; y = -0.0335x + 51.447, podemos deducir que:

El valor de "R^2=0.5638", para la recta del grafico es significativo (cercano a uno), por lo tanto existe una gran dependencia entre el porcentaje de similitud y el numero de muestra de digitación de una determinada contraseña.

La pendiente" m = -0.0335"; tiene un valor significativo y es negativa, lo que indica que los patrones de digitación cada vez se parece menos al perfil conductual inicial, con lo cual podemos concluir que los patrones de digitación varían en el tiempo y el porcentaje de similitud alcanzado varia de forma inversamente proporcional al número de muestra.

4.4.3.2 PROCESAMIENTO DE DATOS DEL MODELOS DINÁMICO

De la distribución de los datos de la tabla 10 obtenemos la siguiente grafica:

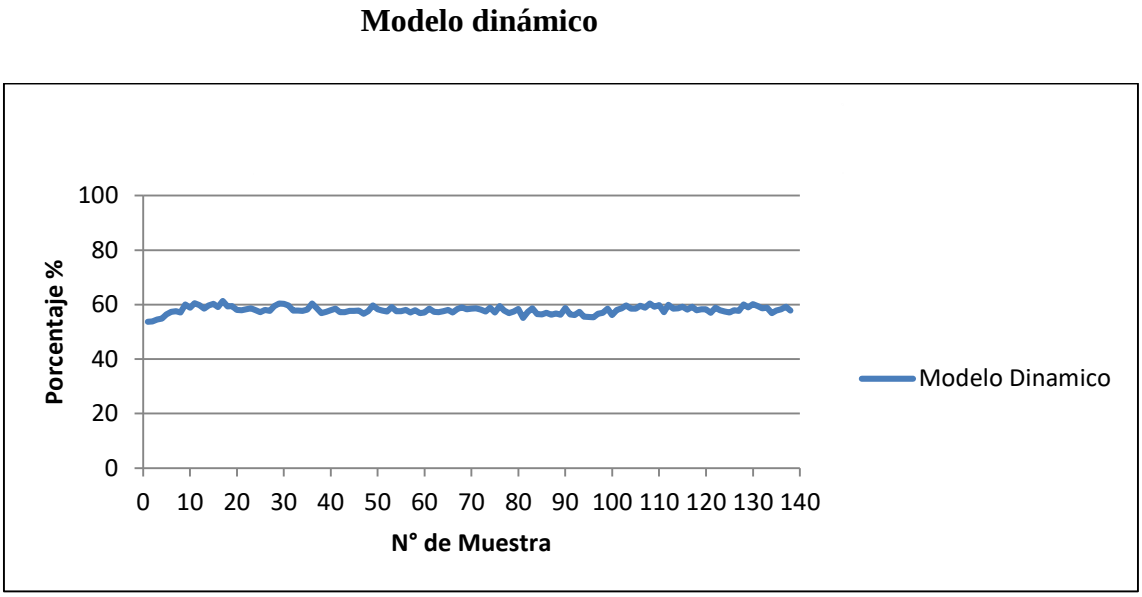


Figura 0.4 : Porcentaje de similitud vs numero de muestras bajo modelo dinámico. Fuente: elaboración propia.

Aplicando regresión lineal a esta grafica se obtiene:

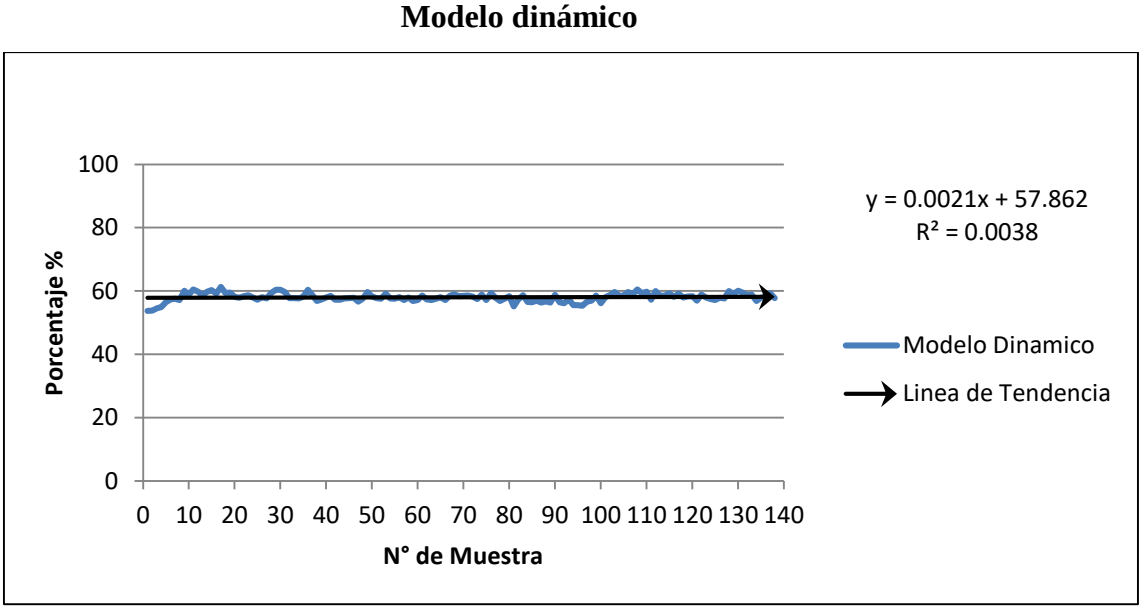


Figura 0.5 : Regresión lineal de la curva del modelo dinámico.

Fuente: elaboración propia.

4.4.3.2.1 ANÁLISIS DEL MODELO DINÁMICO.

De la ecuación; y = 0.0021x + 57.862, podemos deducir que:

El valor de "R^2= 0.0038", para la recta del grafico no es significativo (cercano a 1), por lo tanto no existe una gran dependencia entre el porcentaje de similitud y el numero de muestras de digitación de una determinada contraseña.

La pendiente" m = 0.0021"; tiene un valor próximo a cero por lo que podemos retirarla de la ecuación obteniendo así una función constante de valor: "y =57.862", por lo que este valor es también un **umbral tentativo de Sobre escritura**; el valor de "m", a pesar de ser muy pequeño, es positivo, lo que nos da la idea de que los porcentaje de similitud tienen a subir con el tiempo.

4.4.3.3 COMPARATIVA DEL MODELO DINÁMICO CON EL MODELO CLÁSICO.

Del promedio de los porcentajes de similitud se tiene la siguiente grafica:

Modelo dinámico vs modelo clásico

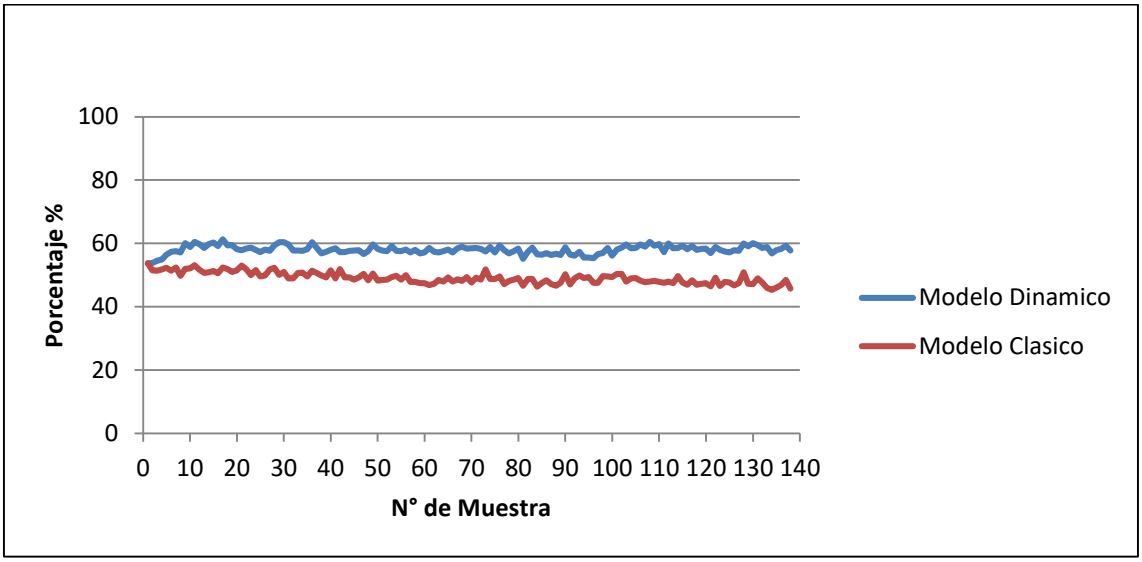


Figura 0.6 : Patrones de la dinámica digitación para modelo dinámico y clásico.
Fuente: elaboración propia.

Aplicando regresión lineal para los dos modelos, obtenemos la siguiente figura:

Modelo dinámico vs modelo clásico

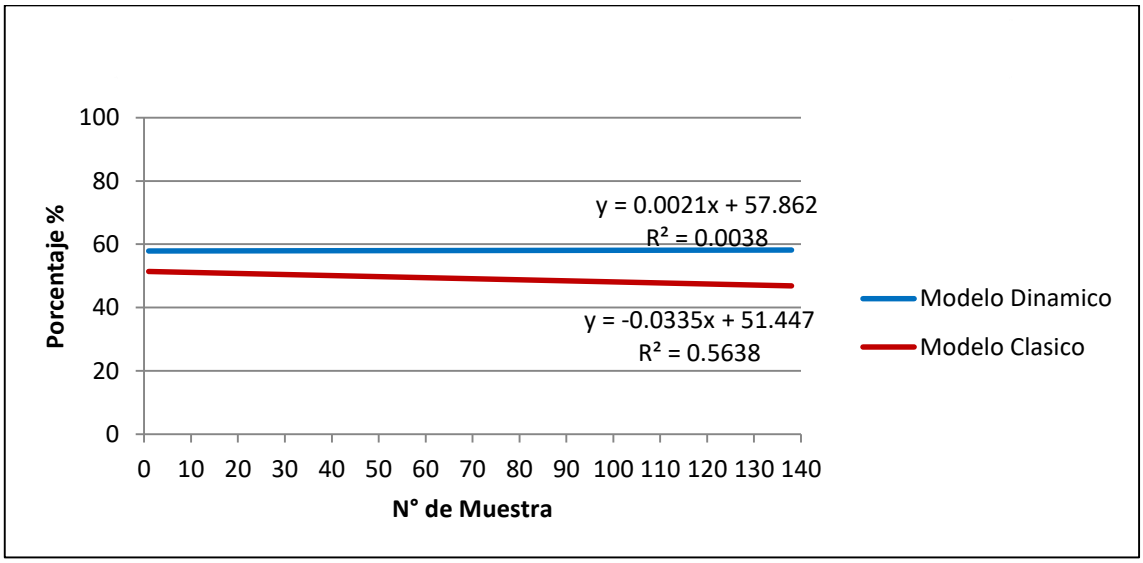


Figura 0.7 : Ecuaciones lineales para modelo dinámico y clásico.
Fuente: elaboración propia.

Análisis

De la regresión lineal para los dos modelos se tiene los porcentajes de similitud máximo en la siguiente tabla:

	% Máximo	R2	Error estadístico

Modelo clásico	51.41	0.563	1.75
Modelo Dinámico	57.86	0.003	1.31

Tabla 0.6: Porcentajes máximos alcanzados por modelo dinámico y clásico. Fuente: elaboración propia.

En donde porcentaje Máximo Dinámico (57.41) es mayor que él porcentaje Máximo clásico (51.41), por lo tanto los patrones de la dinámica de digitación bajo el modelo dinámico es óptimo frente al modelo clásico.

4.4.3.4 VALIDACIÓN DE DATOS

En la realización de la validación datos del modelo propuesto participaron un total de quince (15) usuarios. Estos realizaron dos tipos de autentificaciones:

- **Autenticación de usuario legítimo**: usuarios previamente registrados hicieron parte de este proceso. En el cual los 15 usuarios digitaron entre 24 y 56 veces su clave o contraseña durante un mes. Al conjunto de tentativas de acceso a través de la clave original denominamos sesión. Un total de 568 muestras fueron adquiridas en aproximadamente ciento cincuenta (150) sesiones.
- **Autenticación de usuario impostor**: los usuarios realizaron esta autenticación la cual consiste en hacerse pasar por otro usuario sabiendo de antemano la secuencia de caracteres de la clave de ese usuario. Un total de seis cientos cincuenta y cuatro (654) muestras fueron adquiridas en aproximadamente ciento cincuenta (150) sesiones.

La validación del modelo dinámico propuesto en la presente tesis se realizo mediante ataques de autenticación de usuarios impostores y legítimos al prototipo de seguridad, **con 56.69 %, 58.00 % de valor de aceptación y de sobre escritura** respectivamente obteniéndose los siguientes resultados, graficados en la siguiente tabla:

Usuarios	FN	Total FN	FA	Total FA
usuario 1	5	51	7	49
usuario 2	5	50	3	53
usuario 3	7	46	1	38
usuario 4	7	49	5	47
usuario 5	9	52	5	43
usuario 6	8	41	3	45

usuario 7	6	52	5	39
usuario 8	2	38	3	45
usuario 9	6	46	3	49
usuario 10	6	40	5	51
usuario 11	4	48	2	49
usuario 12	3	44	0	38
usuario 13	6	43	5	50
usuario 14	6	49	4	45
usuario 15	6	45	4	50
Total	**86**	**694**	**54**	**691**
Tazas		**12.39 %**		**7.81 %**

Tabla 0.7: Número de autentificaciones correctas e incorrectas.
Fuente: elaboración propia.

- Para la autenticación de usuario legítimo se obtuvo 86 Falsas Negaciones (FN) de un total de 694 intentos, obteniéndose una Tasa de Falso Rechazo (TFR) de **12.3919308 %**.
- Para la autenticación de usuario impostor se obtuvo 54 Falsas Aceptaciones (FA) de un total de 691 intentos, obteniéndose una Tasa de Falsa Aceptacion (TFA) de **7.81476122 %,** como se muestra en la siguiente tabla.

TFA	**7.81 %**
TFR	**12.39 %**
TOTAL MUESTRAS	**1385**

Tabla 0.8 : Resumen de tasas.
Fuente: elaboración propia.

En general se obtuvo una tasa de falsa aceptación de **7.81476122 %**, lo que constituye la fortaleza de este método, al no aceptar a un usuario que no sea el autentico, ya que al rechazar al correcto tiene como consecuencia únicamente que el usuario tenga que intentar autentificarse nuevamente.

CAPÍTULO 5.

MARCO APLICATIVO.

5.1 METODOLOGÍA PARA EL DESARROLLO DEL MODULO.

Dado que una de las metas de la presente tesis es Implementar un aplicativo de autenticación e identificación a aplicaciones web, mediante los patrones de la dinámica de digitación. Nos mantendremos independientes de la tecnología a emplear y de los aspectos técnicos en general.

El contexto en donde se llevara el ejemplo aplicativo será el modo de funcionamiento en el acceso a un cajero automático teniendo como usuarios a clientes de un banco que en algún momento desearán acceder a su cuenta bancaria a través de este dispositivo para lo que deberá ingresar al sistema mediante nombre de usuario y contraseña. El sistema verificara si el que ha digitado es el propietario de la contraseña y del nombre usuario y si no es propietario, el sistema enviara dos notificaciones de advertencia al celular del propietario de la cuenta y a una determinada entidad de seguridad.

5.2 CICLO DE VIDA DEL PROTOTIPO.

5.2.1 FASE DE ANÁLISIS:

Actores.- Entidades que interactúan con el sistema.

1) Usuario.- cliente de la entidad bancaria que desea acceder a su cuenta mediante un cajero automático.
2) Institución bancaria.- Provee información de los usuarios al sistema para la autenticación e identificación de los mismos.
3) Institución de seguridad.- recibe la notificación de advertencia, mediante un mensaje de texto.

Casos de uso.- Acciones que se hacen en torno a este sistema.

1) Loguearse como usuario.
2) registrar usuario.
3) Modificar usuario.
4) Bloquear cuenta de usuario.

5) Enviar notificaciones de advertencia.

5.2.1.1 DIAGRAMA DE LOS CASOS DE USO

5.2.1.1.1 LOGUEARSE COMO USUARIO.

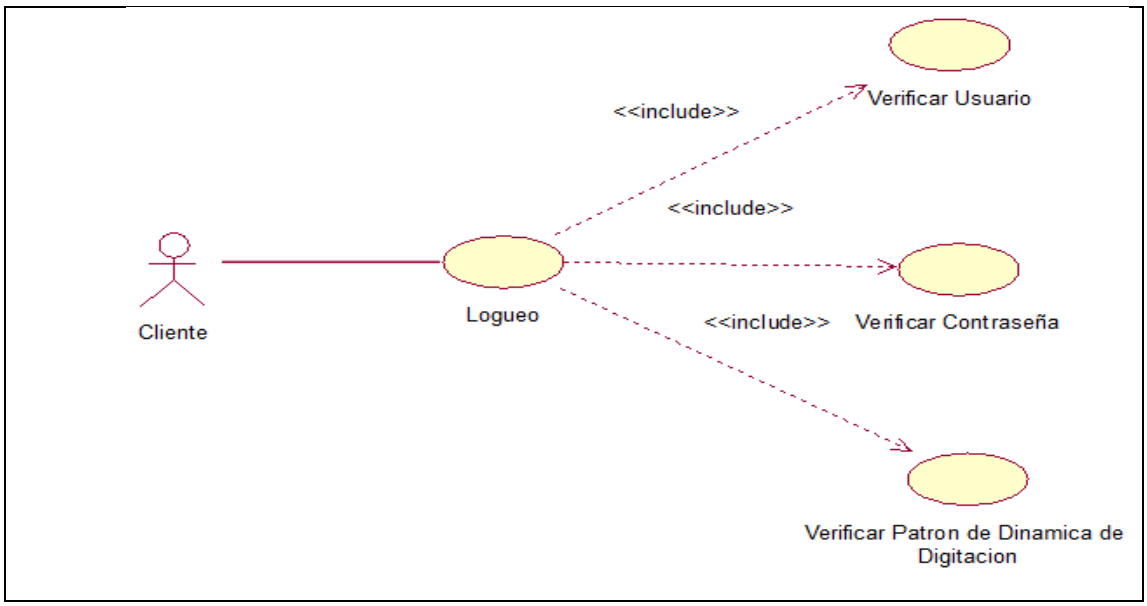


Figura 0.1 : Diagrama de caso de uso. Loguearse como usuario.
Fuente: elaboración propia

5.2.1.1.2 MODIFICAR USUARIO

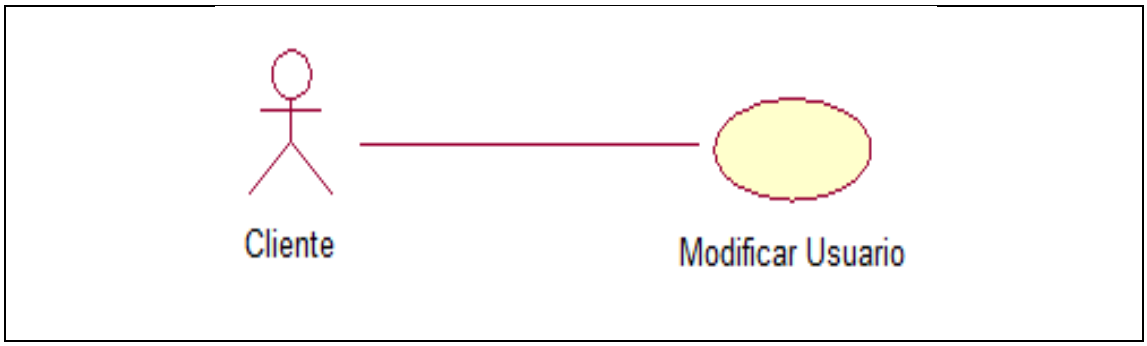


Figura 0.2 : Diagrama de caso de uso. Modificar usuario.
Fuente: elaboración propia

5.2.1.1.3 REGISTRAR USUARIO

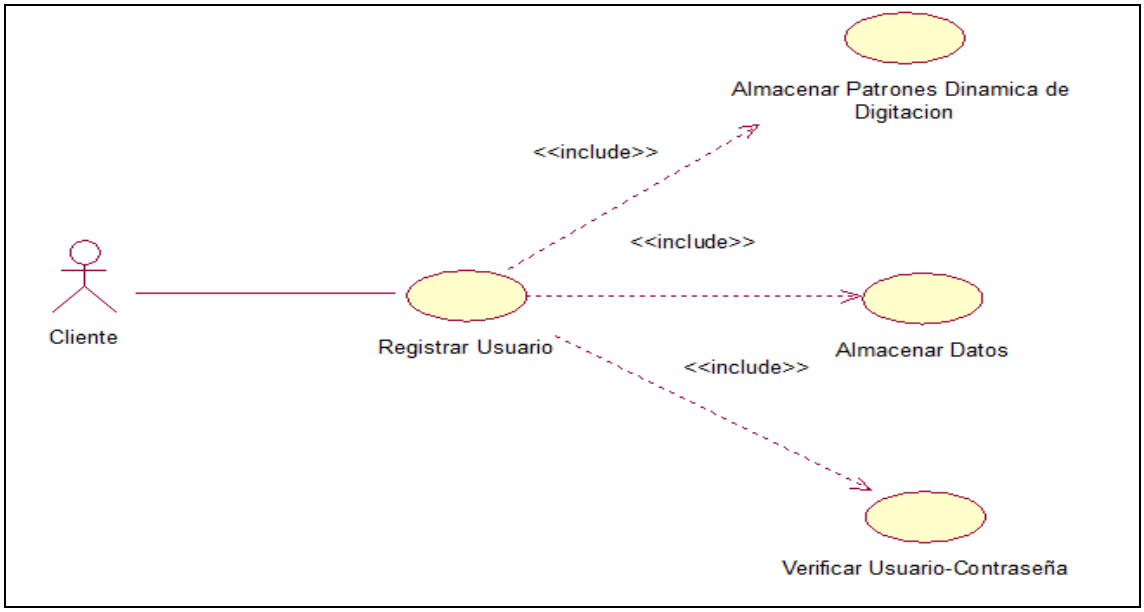


Figura 0.3 : Diagrama de caso de uso. Registrar usuario.
Fuente: elaboración propia

5.2.1.1.4 BLOQUEAR CUENTA DE USUARIO

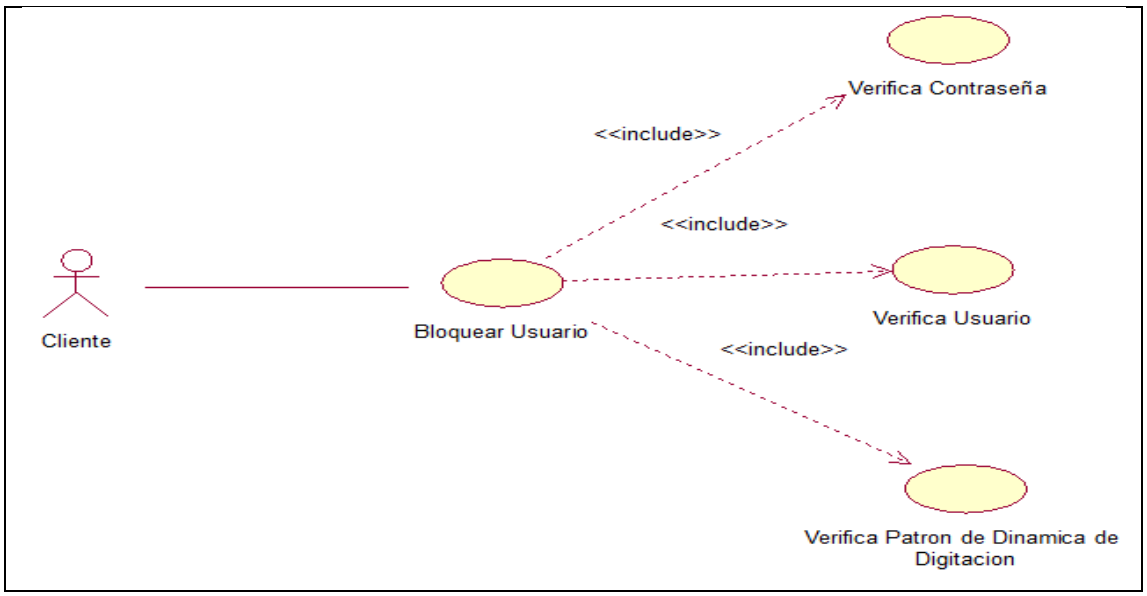


Figura 0.4 : Diagrama de caso de uso. Bloquear Cuenta de Usuario.
Fuente: elaboración propia

5.2.1.1.5 ENVIAR NOTIFICACIONES DE ADVERTENCIA

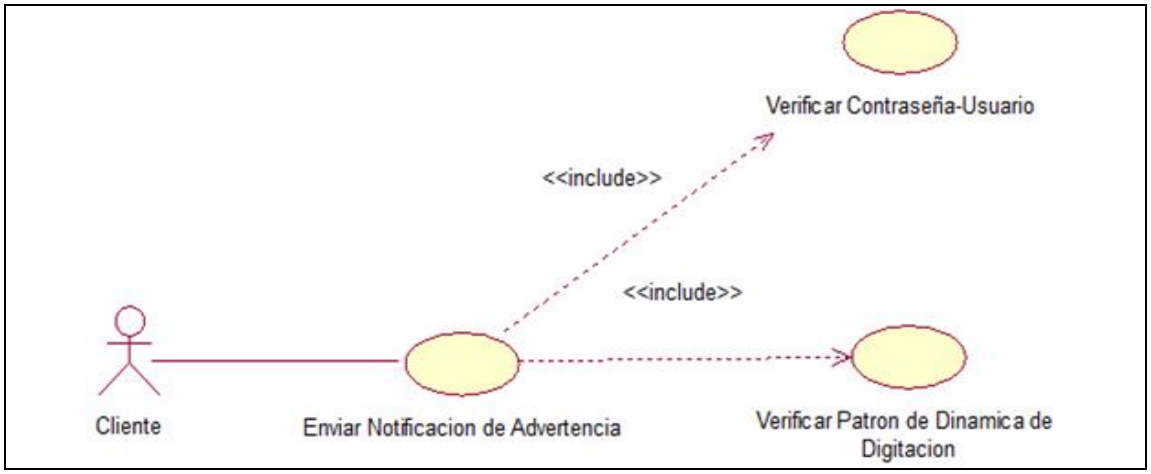


Figura 0.5 : Diagrama de caso de uso. Enviar Notificaciones de Advertencia.
Fuente: elaboración propia

5.2.1.2 ESPECIFICACIÓN DE CASOS DE USO

5.2.1.2.1 LOGUEARSE COMO USUARIO

Nombre: Loguearse como usuario.

Descripción: Procedimiento que se lleva a cabo para permitir el ingreso de un usuario, tenerlo autentificado e identificado y darle acceso a elementos apropiados del sistema.

Actores: Usuario cliente.

Pre condiciones: El usuario está registrado en el sistema.

Pos condiciones: El usuario está dentro del sistema con su sesión de cuenta y el sistema lo tiene identificado.

Flujo normal de eventos

1) El sistema solicita el nombre del usuario (clave pública) y una contraseña (la clave privada).
2) El actor ingresa los dos datos apropiados.
3) El sistema corrobora ambas claves en su base de datos.
4) El sistema corrobora los patrones de la dinámica de digitación.
5) El sistema permite el ingreso del usuario al sistema con los accesos apropiados.

Flujos alternos

1) **El actor ingresa información errónea:** El sistema notifica tal error al usuario.
2) **El actor digita contraseña con los patrones de dinámica de digitación diferente con plantilla de muestreo:** el sistema notifica error de información, en el tercer intento el sistema se bloquea enviando dos mensajes de texto, uno al propietario de la cuenta y el otro a una determinada institución de seguridad

Excepciones

1) **El sistema no tiene conexión con su base de datos**: El sistema notifica al usuario la imposibilidad de acceder al sistema por razones técnicas y que vuelva a intentarlo pasado algún periodo en tiempo.

5.2.1.2.2 REGISTRAR USUARIO

Nombre: Usuario cliente y administrador.

Descripción: Procedimiento que se lleva a cabo para que un usuario pueda registrarse en el sistema para poder hacer uso del mismo.

Actores: Usuario cliente.

Pre condiciones: Ninguna.

Pos condiciones: Ninguna.

Flujo normal de eventos

1) El sistema solicita información al usuario. Ésta incluye nombre de usuario, password o contraseña, apellido, número de celular.
2) El usuario ingresa los datos requeridos.
3) El sistema pide que actor digite 10 veces la contraseña.
4) El sistema almacena la información.

Flujos alternos

1) El usuario a registrar ya existe: El sistema notifica de error.

Excepciones

1) **El sistema no tiene conexión con su base de datos**: El sistema notifica que no puede corroborar los datos ingresados y que vuelva a intentarlo al rato, terminando el caso de uso.

5.2.1.2.3 MODIFICAR USUARIO

Nombre: Modificar usuario.

Descripción: Procedimiento que se lleva a cabo para cambiar datos de un usuario.

Actores: Usuario cliente.

Pre condiciones: El usuario está registrado en el sistema.

Pos condiciones: El usuario está dentro del sistema con su sesión de cuenta y el sistema lo tiene identificado y autentificado.

Flujo normal de eventos

1) El actor modifica datos personales.
2) El sistema almacena las modificaciones.

Flujos alternos

1) **El actor ingresa datos no valida:** El sistema notifica tal error al usuario.

Excepciones

1) **El sistema no tiene conexión con su base de datos**: El sistema notifica al usuario la imposibilidad de acceder al sistema por razones técnicas y que vuelva a intentarlo pasado algún periodo en tiempo.

5.2.1.2.4 BLOQUEAR CUENTA DE USUARIO

Nombre: bloquear cuenta de usuario.

Descripción: Procedimiento que se lleva a cabo para permitir el bloqueo de acceso al sistema (cajero automático).

Actores: Usuario cliente.

Pre condiciones: El usuario está registrado en el sistema.

Pos condiciones: El usuario está dentro del sistema con su sesión de cuenta y el sistema lo tiene identificado.

Flujo normal de eventos

1) El sistema solicita su contraseña.
2) El actor ingresa datos requeridos.
3) El sistema verifica la discrepancia de los patrones de su dinámica de digitación actual con su base de datos.
4) El sistema notifica error al usuario (error 1).

5) El sistema solicita el nombre del usuario y su contraseña.
6) El actor ingresa datos requeridos.
7) El sistema verifica la discrepancia de los patrones de su dinámica de digitación actual con su base de datos.
8) El sistema notifica error al usuario (error 2).
9) El sistema solicita el nombre del usuario y su contraseña.
10) El actor ingresa datos requeridos.
11) El sistema verifica la discrepancia de los patrones de su dinámica de digitación actual con su base de datos.
12) El sistema notifica error al usuario (error 3).
13) El sistema bloquea el acceso al cajero automático.

Flujos alternos

1) **El actor ingresa información errónea:** El sistema notifica tal error al usuario.
2) **El actor digita contraseña con los patrones de dinámica de digitación diferente con plantilla de muestreo:** el sistema notifica error de información (error 1), en el tercer intento el sistema se bloquea enviando dos mensajes de texto, uno al propietario de la cuenta y el otro a una determinada institución de seguridad.

   Excepciones

   1) **El sistema no tiene conexión con su base de datos**: El sistema notifica al usuario la imposibilidad de acceder al sistema por razones técnicas y que vuelva a intentarlo pasado algún periodo en tiempo.

5.2.1.2.5 ENVIAR NOTIFICACIÓN DE ADVERTENCIA

Nombre: enviar notificación de advertencia.

Descripción: Procedimiento que se lleva a cabo para el envió de mensajes de texto al teléfono celular del propietario de la cuenta y a una institución de seguridad con notificación de acceso no autorizado a dicha cuenta.

Actores: Institución de seguridad y Usuario cliente.

Pre condiciones: El usuario está registrado en el sistema.

Pos condiciones: El usuario está dentro del sistema con su sesión de cuenta y el sistema lo tiene identificado.

Flujo normal de eventos

1) El sistema solicita contraseña.
2) El actor ingresa dato.
3) El sistema verifica tres veces la discrepancia de los patrones de su dinámica de digitación actual con su base de datos.
4) El sistema envía notificación de advertencia mediante mensajes de texto al teléfono móvil del propietario de la cuenta y a una determinada institución de seguridad.

Flujos alternos

1) **El actor ingresa información errónea:** El sistema notifica tal error al usuario.
2) **El sistema pide información de usuario:** pide que digite usuario y contraseña.
3) **El actor ingresa contraseña.**
4) **El sistema verifica contraseña con los patrones de dinámica de digitación con un porcentaje de aceptación aceptable con plantilla de muestreo:** el sistema da acceso al usuario que digita contraseña.

Excepciones

1) **El sistema no tiene conexión con su base de datos**: El sistema notifica al usuario la imposibilidad de acceder al sistema por razones técnicas y que vuelva a intentarlo pasado algún periodo en tiempo.

5.2.1.3 DIAGRAMA DE SECUENCIA

5.2.1.3.1 LOGUEARSE COMO USUARIO

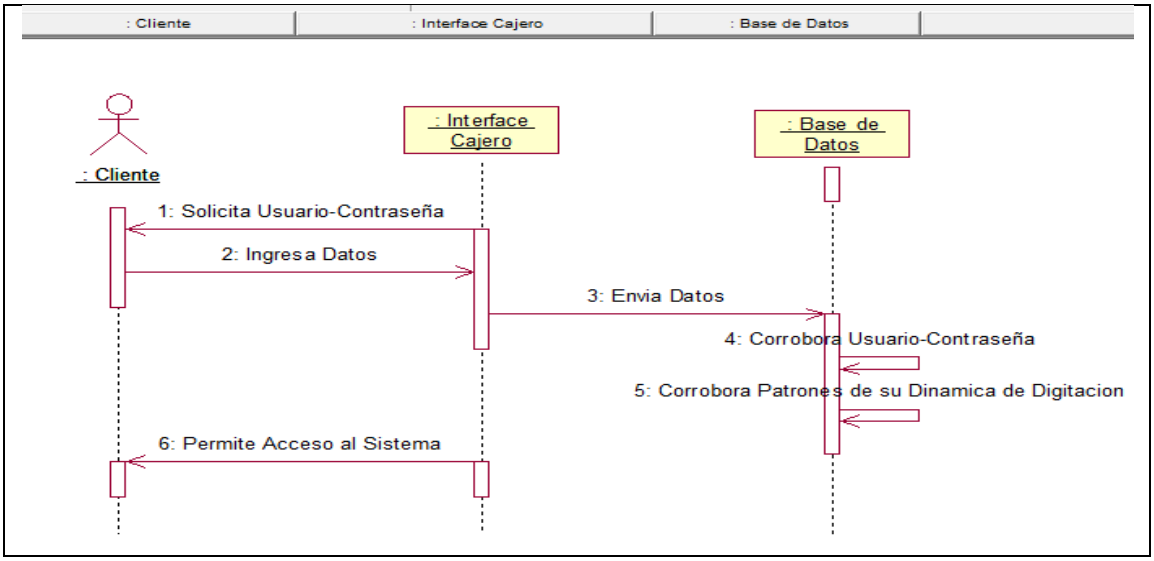


Figura 0.6 : Diagrama de secuencia. Loguearse como usuario.
Fuente: elaboración propia.

5.2.1.3.2 REGISTRAR USUARIO

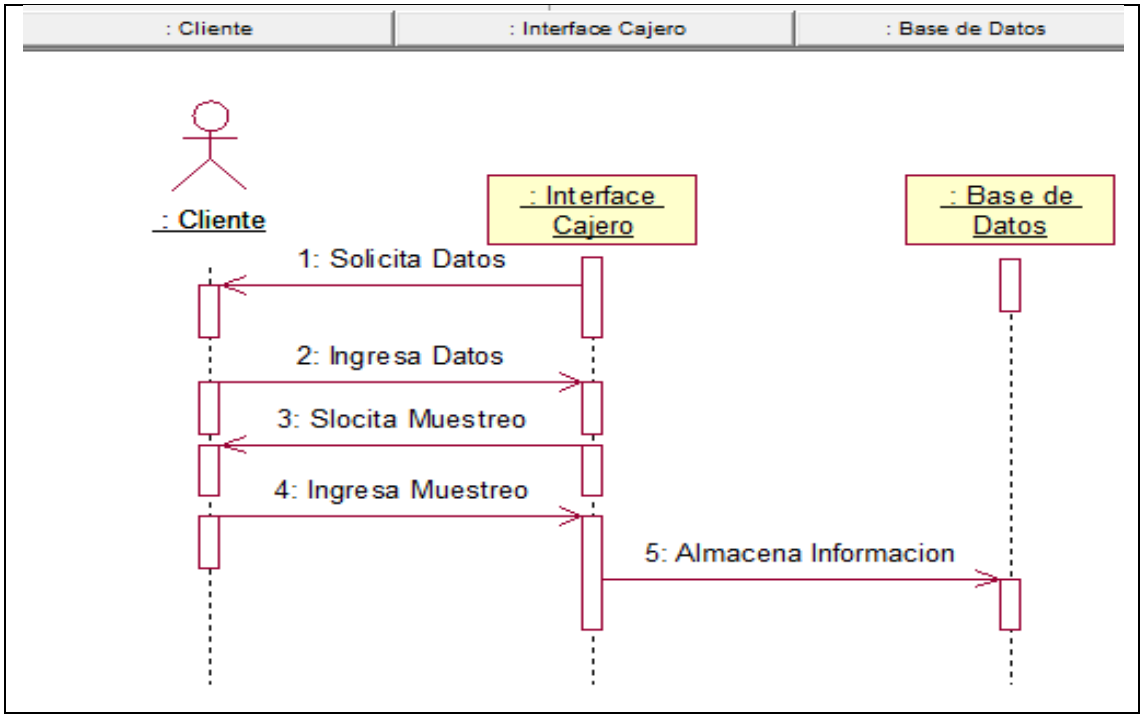


Figura 0.7 : Diagrama de secuencia. Registrar usuario.
Fuente: elaboración propia

5.2.1.3.3 MODIFICAR USUARIO

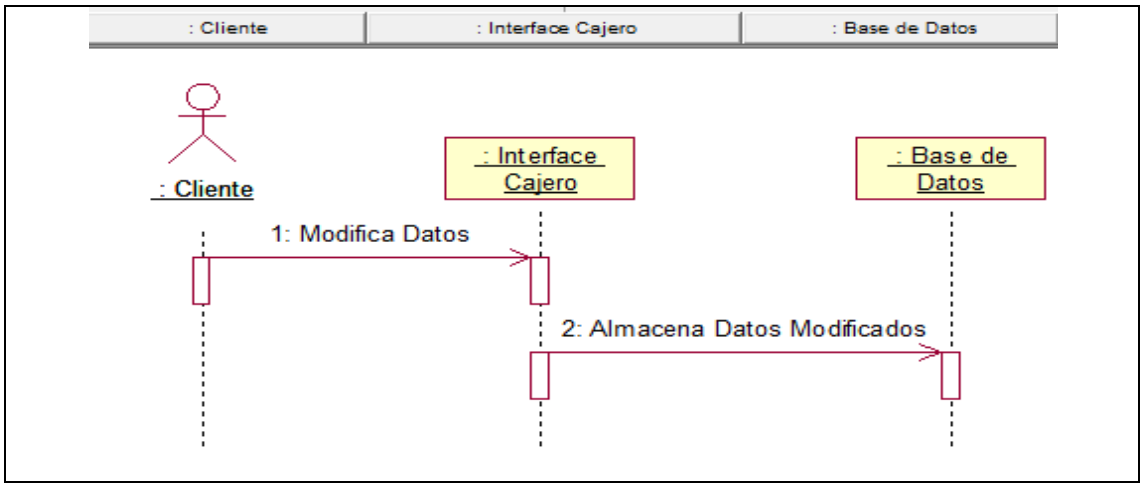


Figura 0.8 : Diagrama de secuencia. Modificar usuario.
Fuente: elaboración propia

5.2.1.3.4 BLOQUEAR CUENTA DE USUARIO

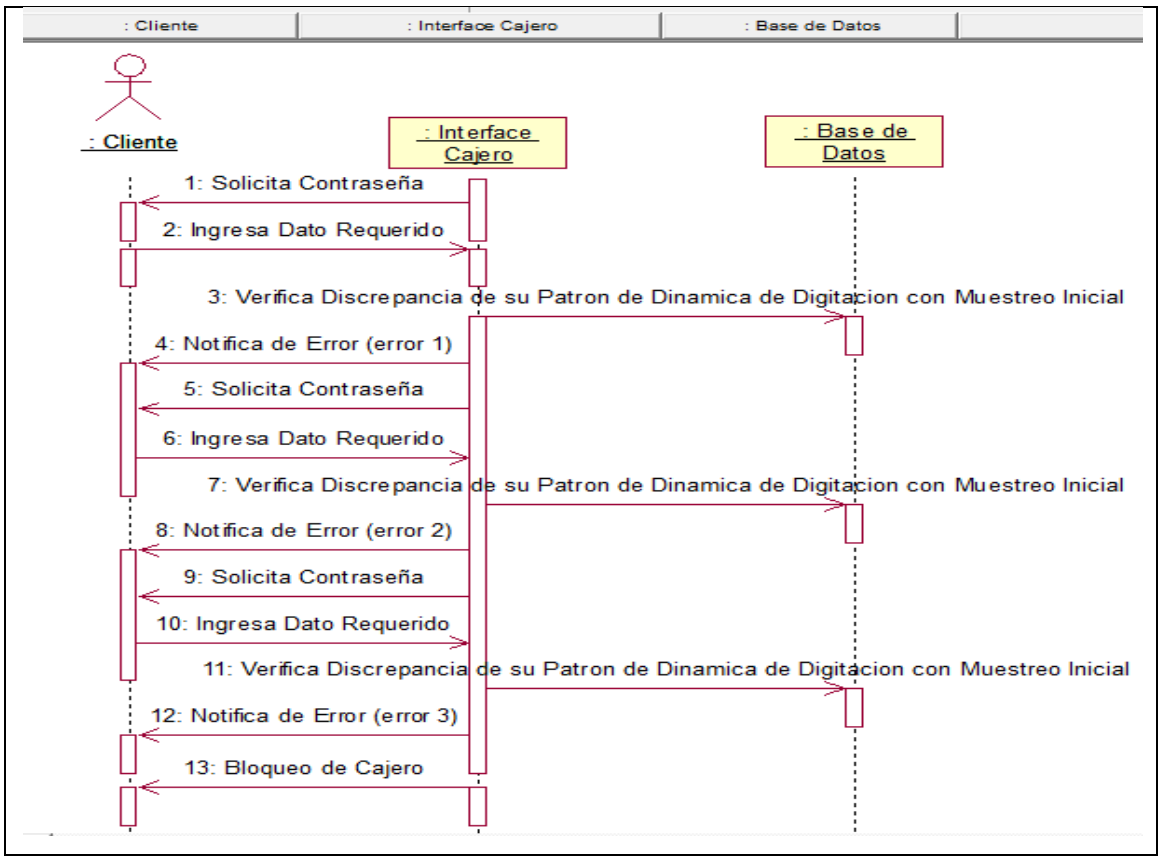


Figura 0.9 : Diagrama de secuencia. Bloquear cuenta de usuario.
Fuente: elaboración propia

5.2.1.3.5 ENVIAR NOTIFICACIONES DE ADVERTENCIA

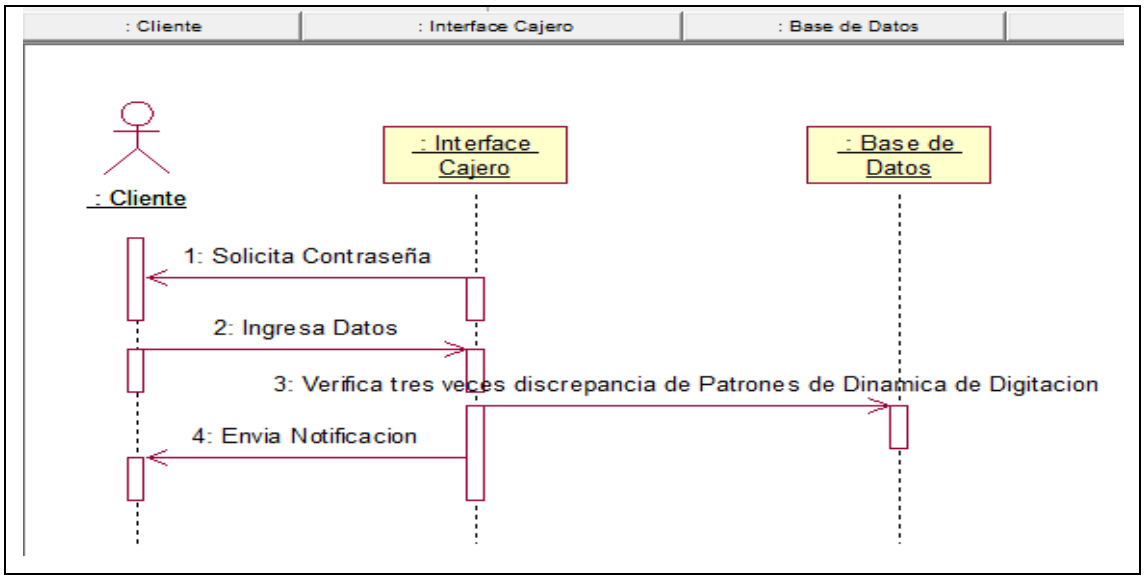


Figura 0.10 : Diagrama de secuencia. Enviar notificaciones de advertencia.
Fuente: elaboración propia

5.2.1.4 INTERFACES

5.2.1.4.1 REGISTRAR USUARIO.

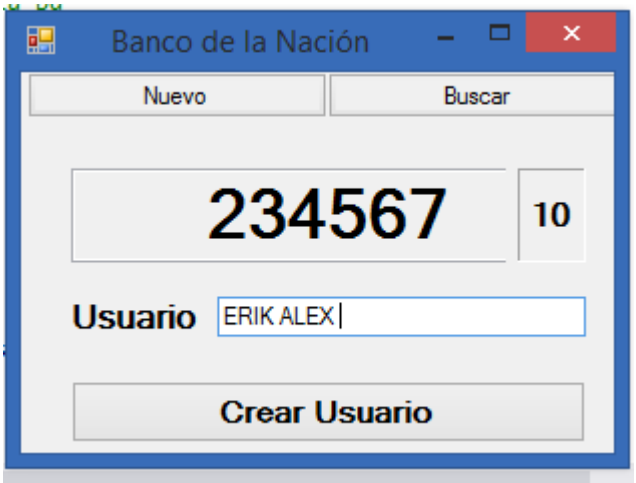


Figura 0.11 : Diagrama de secuencia. Registrar usuario.
Fuente: elaboración propia.

5.2.1.4.2 BUSCAR USUARIO.

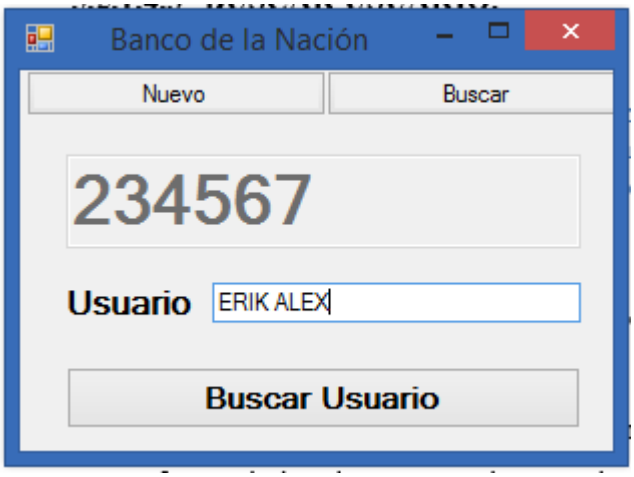


Figura 0.12 : Diagrama de secuencia buscar usuario.
Pantalla de la Búsqueda de contraseña y de Información.
Fuente: elaboración propia.

5.2.2 FASE DE IMPLEMENTACIÓN:

(Diagrama de componentes y diagrama de despliegue)**.**

El prototipo para la autenticación de usuarios tomando como parámetro la dinámica de digitación se basa en la comparación de plantillas, cada plantilla se conforma de los tiempos en el que cada usuario lleva a cabo los eventos pulsar – soltar tecla y soltar – pulsar tecla, dichos tiempos se manejan con una precisión de ocho cifras, para la comparación de similitud de las plantillas se utilizaron funciones estadísticas de dispersión, obteniendo un porcentaje de aceptación (PA) comparado con un porcentaje de similitud (PS) se decide la aceptación o rechazo de un usuario.

En este sentido los elementos necesarios para el desarrollo del prototipo son: rutinas para la detección de eventos del teclado, un contador de tiempo con una precisión de cuatro cifras para la diferenciación de los tiempos en cada usuario y comparación de estos tiempos, para realizar una autenticación.

DETECCIÓN DE LOS EVENTOS DEL TECLADO

La detección de los eventos del teclado en los lenguajes de programación de alto nivel no es una tarea difícil ya que éstos incorporan rutinas que se encargan del manejo de los eventos de teclado como son: pulsar tecla o soltar tecla.

Deseamos medir el comportamiento del usuario ante el teclado para esto mediremos las características siguientes:

El tiempo que transcurre cuando el usuario presiona una tecla y suelta la misma tecla, a este evento llamaremos pulsar – soltar.

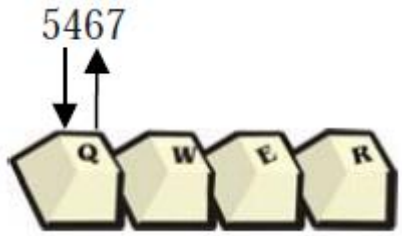


Figura 0.13 : Número de muestras de tiempo para el evento pulsar – soltar.
fuente elaboración propia

El tiempo que transcurre cuando el usuario suelta una tecla y presiona la tecla siguiente, a este evento le llamaremos soltar - pulsar.

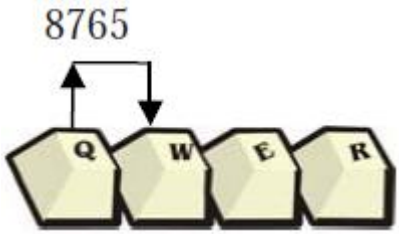


Figura 0.14 : Número de muestras de tiempo para el evento soltar – pulsar.
fuente elaboración propia

Entonces tendríamos lo siguiente:

Tiempos eventos pulsa – soltar = n

Tiempos eventos soltar – pulsar = n -1

Donde n es el número de caracteres de la contraseña o password.

CONTADOR PARA LA MEDICIÓN DE TIEMPOS DE TECLEO

El siguiente paso para el modelo es la implementación de un contador que indicará el tiempo que transcurre en cada unos de los eventos del teclado, este contador es deseable que se incremente con suficiente rapidez de tal manera que por ejemplo para el evento pulsar – soltar el tiempo que transcurren entre pulsar la tecla y soltar la tecla tenga cuatro cifras como mínimo. Entre más rápido se incremente el contador, existirá mayor diferenciación en la dinámica de tecleo de un usuario a otro, ya que los intervalos de tiempo estarán más separados. Así

entonces, la velocidad de tecleo puede ser una característica importante para la diferenciación de los usuarios.

El manejo e implementación de estos contadores depende en gran medida del sistema operativo, para ésta aplicación trabajaremos sobre plataforma Windows, dentro de las opciones con las cuales se puede implementar un contador bajo esta plataforma encontramos:

1) Componentes Timer, que vienen en lenguajes de alto nivel como Delphi, Visual Basic, Java, etc. estos componentes se manejan en milisegundos.
2) En Windows existe una función del API llamada GetTickcount, en el momento que hablamos a esta función nos regresa el tiempo en milisegundos que ha estado activo Windows.
3) En Java podemos encontrar una función llamada System.currentTimeMillis(), la cual nos proporciona un tiempo en milisegundo que es tomado del sistema.
4) QueryPerformanceCounter función del API de Windows que devuelve los ciclos de procesador que han transcurrido desde que se activó Windows con una precisión de once cifras.

COMPARACIÓN DE LA DINÁMICA DE TECLEO

Este modelo recibirá como parámetros de entrada una lista de tiempos, dicha lista puede ser los tiempos de los eventos pulsar – soltar o soltar – pulsar, de la misma manera se recibirá la plantilla correspondiente con la que se compararán los nuevos tiempos, el parámetro de salida que enviará el modelo es un porcentaje del 1 al 100 al que le llamaremos porcentaje de similitud (PS), este indicará en que porcentaje son parecidos los nuevos tiempos a los tiempos que se encuentran en la plantilla, y de la misma manera se calculará un porcentaje al que llamaremos porcentaje de aceptación (PA) que nos indicará el porcentaje mínimo que debe alcanzar el usuario para poder ser aceptado por la aplicación. Las plantillas de los eventos pulsar – soltar y soltar – pulsar se encuentran estructuradas por columnas que contienen los tiempos en el que se ejecuto el evento correspondiente y líneas que son el número de muestras tomadas al usuario.

La desviación estándar nos dice cuánto tienden a alejarse los puntos del promedio. De hecho específicamente la desviación estándar es el promedio de lejanía de los puntajes respecto del promedio, es así que si sacamos la desviación estándar de los patrones de tiempo de la dinámica de digitación de un determinado usuario, tendríamos un número que nos indicaría cuanto fue el grado de desviación del usuario al momento de capturar las muestras para la plantilla en dicha tecla o intervalo de tecla específico. Una vez teniendo la desviación estándar de cada columna de la plantilla, como segundo paso necesitaríamos saber cuánto se desvió la nueva muestra, para esto tomaremos como referencia la media de cada columna de la plantilla ya que la media es la que toma la desviación estándar en el proceso anterior. Entonces en este paso sacaremos una nueva desviación estándar a la que llamaremos S' en base a la media de cada columna de la plantilla y el nuevo tiempo de la columna correspondiente. Si se tratase de un usuario autentico entonces suponemos que la mayoría de las columnas S sería mayor a S'.

Otra de las funciones estadísticas que utilizamos para el modelo es el coeficiente de variación este nos indica cual es la desviación de los puntos pero en términos de porcentajes como mencionamos anteriormente lo que nos interesa es un porcentaje que nos indique el grado de similitud entre la muestras nuevas de tiempo y las muestras de tiempo almacenadas en la platilla.

Hasta aquí se ha calculado de manera porcentual que tanto están agrupados o desagrupados los puntos de la plantilla cuando el usuario teclea, de la misma manera el porcentaje que se desvió al autenticarse nuevamente en relación con la media de la plantilla. Entre más grande es el porcentaje, entonces mayor es la posibilidad de variación.

5.2.2.1 DIAGRAMA DE PAQUETES Y COMPONENTES

Partiendo del diagrama de clases, podemos crear seis componentes divididos en tres paquetes:

1) Paquete de interfaces: Representan las pantallas que interactúan con el usuario. Estos son las de logueo, modificación, y la de registro de usuarios.

2) Paquete de controladores: Representan los componentes de negocio que tienen que ver con las operaciones principales del sistema. Estas son la de control de usuarios (registro, autenticaciones e identificación).
3) Paquetes externos: Representan las que interactúan con sistemas externos (institución de seguridad, institución bancaria y usuario cliente).

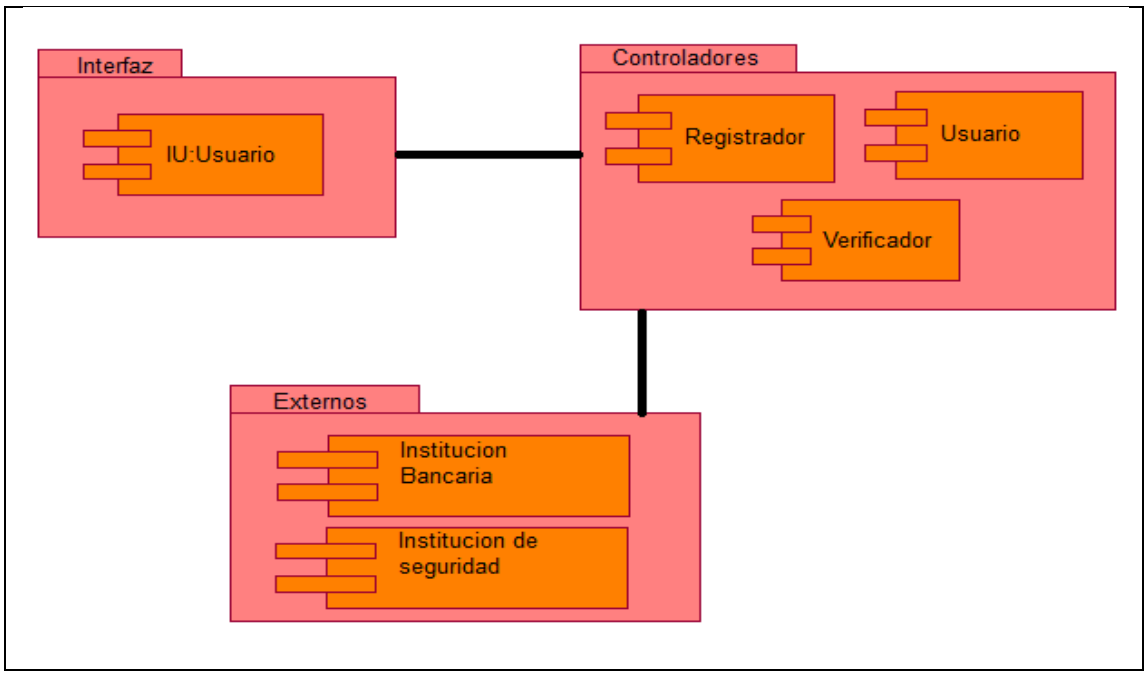


Figura 0.15 : Diagrama de paquetes de solución propuesta.
fuente elaboración propia.

5.2.2.2 DIAGRAMA DE DESPLIEGUE

En éste diagrama se puede ver una perspectiva un poco más enfocada a los elementos que se han de crear y en qué punto físico del sistema se van a insertar. Se distinguen 4 nodos (1 de ellos no es nodo, sino más bien una agrupación de ellas de una misma categoría).

1) El nodo del cliente (izquierda). Donde básicamente estará el navegador Web desde donde accederá a al prototipo para la autenticación e identificación.
2) Nodo de servidor (centro superior). Donde estará alojado prácticamente el prototipo por sí mismo. Se instalarán los componentes lógicos que abarcan los controladores del negocio, las interfaces de usuario, conectores con los servicios Web y las interfaces con Base de datos.

3) El nodo de base de datos (centro inferior). En este nodo es donde prácticamente estará la base de datos.

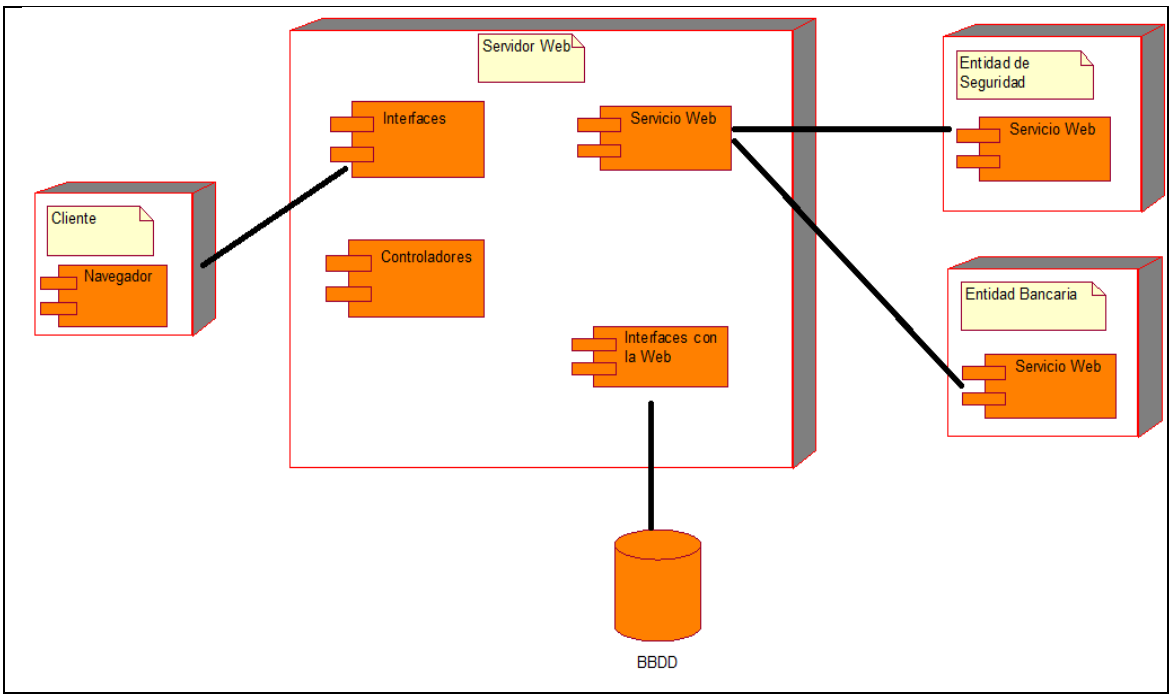


Figura 0.16 : Diagrama de despliegue de solución propuesta.
fuente elaboración propia

5.2.2.3 REQUISITOS MÍNIMOS DE PROTOTIPO

Considerando la arquitectura de la aplicación actual. No hay necesidad de complementos de hardware y software esencialmente sofisticados ni exclusivos de vendedores determinados. De hecho, eso es una ventaja, dado que abarata costos y exige menos de los usuarios.

A NIVEL CLIENTE:

A NIVEL DE HARDWARE:

- PC con teclado y Mouse.
- Disco duro.
- Conexión a Internet.

A nivel de software:

- Sistema operativo (edición doméstica).
- Navegador Web.

A NIVEL SERVIDOR DE LÓGICA DE NEGOCIO:

A nivel de hardware:

− Equipo servidor de mainframe.

− Conexión a Internet.

A nivel de software:

− Sistema operativo de servidor (edición empresarial).

− Hosting de aplicación Web.

− Servidor de servicios Web.

A NIVEL SERVIDOR DE DATOS:

A nivel de hardware:

− Equipo servidor de mainframe.

− Discos duros para almacenamiento redundante.

A nivel de software

− Sistema gestor de base de datos relacional.

PARA DESARROLLO:

A nivel de hardware:

- 1 Computador personal para trabajos de desarrollo.
- 1 Servidor exclusivo para aplicaciones.
- 1 Servidor para base de datos.

(Todos estos elementos podrían estar dentro de un equipo informático)

A nivel de software (para computador de desarrollo):

- Plataforma de desarrollo que incluya compilador, depurador y ensamblador.
- Entorno de desarrollo para aplicaciones Web. Debe permitir creación de librerías y servicios Web.

5.2.3 FASE DE PRUEBA

El prototipo para la autenticación de usuarios basado en los patrones de la dinámica de digitación ha funcionado correctamente ya que con este se ha tomado las muestras de los tiempos de digitación en el capítulo IV "Patrones de la dinámica de digitación" en el numeral 4.4.2. "recolección de datos", para el análisis y estudio de estos parámetros basados en el modelo dinámico, a demás de esto se ha utilizado para la validación de los valores de operación (valor de

aceptación y valor de sobre escritura), descritos en el capítulo IV “Patrones de la dinámica de digitación”, en el numeral 4.4.5 “validación de datos”, funcionando en estos procesos de manera idónea, ya que sin este prototipo no hubiera sido posible realizar la presente tesis.

CONCLUSIONES

1. Del estudio de los patrones de la dinámica de digitación y de los mecanismos de autenticación e identificación en entornos web, el primero es una alternativa económica y adecuada en comparación con los otros mecanismos de autenticación ya que estos requieren hardware adicional para su operatividad o funcionamiento.

2. Los patrones de digitación cambian con el tiempo, lo que da lugar a que el modelo clásico no sea una alternativa para la autenticación de usuarios con el esquema usuario-contraseña, mientras que el modelo propuesto en la presente tesis (**modelo dinámico**), el cual asume este hecho es una alternativa óptima, permitiendo obtener niveles de seguridad superiores al modelo clásico.

3. Los valores de los umbrales de aceptación y sobre escritura son de 56.69% y 58.00% respectivamente, para el modelo de autenticación propuesto en la presente tesis (modelo dinámico).

4. Se obtuvo una tasa de falsa aceptación de 7.81476122% y una tasa de falsa negación de 12.3919308%, alcanzando valores ideales cuando se incremente los umbrales de aceptación y de sobre escritura.

5. Se ha desarrollado un aplicativo de autenticación basado en los patrones de la dinámica de digitación usando el modelo dinámico, el cual tiene la capacidad de autenticar al propietario de una contraseña al momento de digitar la misma.

RECOMENDACIONES

1. Del estudio de los patrones de la dinámica de digitación y de los mecanismos de autenticación e identificación, se recomienda aplicar estos en dispositivos como celulares y laptop con pantalla táctil.

2. Se recomienda la construcción de un dispositivo electrónico para la autenticación de clientes en los cajeros automáticos, basado en los patrones de la dinámica de digitación, bajo el modelo dinámico propuesto en la presente tesis.

3. Se recomienda estudiar los patrones de la dinámica de digitación con valores de aceptación y sobre escritura mayores a los obtenidos en la presente tesis, para obtener mecanismos informáticos con niveles altos de seguridad en la autenticación a sistemas web.

4. Se recomienda construir un aplicativo de autenticación, basado en los patrones de la dinámica de digitación en el cual se capture los patrones de digitación para el muestreo sin que el usuario se percate de este proceso.

5. Los patrones de la dinámica de digitación se puede utilizar para detectar el estado anímico de las personas, ya que estos patrones son conductuales, ósea la manera de digitar de un usuario refleja en muchos casos el estado de ánimo de la misma.

BIBLIOGRAFÍA

[1]: AGUILAR, K, lógica difusa, 2009, Brasil.

[2]: AGUILERA. R, Tratamiento internacional, en Contribuciones a las Ciencias Sociales, 2009, cuba

[3]: ALLMYSOFT. A, biometría estática, 2007, puerto rico.

[4]: ANIL K. J, autentificación dinámica, 2004, Uruguay.

[5]: GRANGER .S, tendencias biométricas, 2001, chile.

[6]: HERNANDEZ. Z, "metodologias en la investigacion cientifica",2011, Colombia

[7]: JEREZ. L, técnicas de seguridad biométrica, 2006, Brasil.

[8]: MATTHEW , A, biometría facial, 1991, USA.

[9]: MUÑOZ, V, Tecnologías biométricas, 2007, chile.

[10]: RAMÍREZ. B, Los delitos informáticos, 2009, Perú.

[11]: ROMO. M, Las tecnologías biométricas, 2003, Ecuador.

[12]: RUUD. B, guide to biometrics, 2003, Brasil.

[13]: SEBESTAR, R, "concept of programing languajes",2011, U.S.A

[14]: YAUWEI. Y, The “123” of biometric technology, 2002, Brasil.

[15]: YABU-UTI. L, LING CHENG HUANG JIANG, SHIUPING SHIEH Y JEN CHIEN LIU, “Lógica Difusa”, 2004, U.S.A.

REFERENCIAS

[1]: http://csimg.choozen.es/srv/ES/2901507915132/T/300x300/C/FFFFFF/url/teclado-standard-ps-2-espaaol.jpg, **CHOOSEN, 1 Mar 2000, 12 Ago 2013.**

[2]: http://t0.gstatic.com/images?q=tbn:ANd9GcRbkT75M9UFbO0xunvhihOs9j-N9BFlWTTi6iwoSCOGFvO6_jNFCg, **CLINICAOFTA, 25 Dic 2000, 12 Ago 2013.**

[3]: http://t0.gstatic.com/images?q=tbn:ANd9GcTcVpvhAHt9sWBCtkvLyakDoKmYEnChrtax3_4L-CEf64Q-mZ7Tzg, **COMMUNITY, 1 Dic 2007**, **12 Ago 2013**.

[4]: http://t0.gstatic.com/images?q=tbn:ANd9GcSbCkIdp3dz8FdERfJK7jhg5wIRVgNaMa9Aq5eTx9_BfFhHil-ThQ, **COMUNICANTROPO, 2 Oct 2000, 12 Ago 2013.**

[5]: http://t1.gstatic.com/images?q=tbn:ANd9GcQ2VuxlMAQ3eGr3Fiz3mOzc2p1FaMgYx_4TJn8_z3zH0Fpx0rTL, **ENPOSITIVO, 19 Sep 2000, 12 Ago 2013.**

[6]: http://t3.gstatic.com/images?q=tbn:ANd9GcT7DbyYlWf_uC2sjhvBQZbH9dvoOxlBv4EsPBRoPx3lvQnk4yhl, **GEOFISICA, 4 Oct 2003, 12 Ago 2013.**

[7]: http://t1.gstatic.com/images?q=tbn:ANd9GcThVFiXkLT6tAw4g0z96YWTvgg7FIyjYk4GApSrkme8XvERNHMF, **IBIBLIO, 3 Jun 2000, 12 Ago 2013.**

[8]: http://www.islabit.com/wp-content/imagenes/ThinkPad-Keyboard-lenovo.jpg, **ISLABIT, 2 Nov 2001**, **12 Ago 2013**.

[9]: http://www.lohmanntapes.es/files_db/1316606457_79_28.png, **LOHMANN, 27 Jul 2002**, **12 Ago 2013**.

[10]: http://coding.smashingmagazine.com/2010/02/10/some-things-you-should know-about ajax/, **MAGAZINE, 28 Oct 2006**, **12 Ago 2013**.

[11]: http://t1.gstatic.com/images?q=tbn:ANd9GcT3peZzp-meezgWd2nRq0MLV1gnDksq72bygU7PQh-jBXgzoSV6OQ, **MICROSOFT, 2 Sep 2000, 12 Ago 2013.**

[12]: http://www.informaticamoderna.com/Teclado.htm, **MICROSOFT, 5 Mar 2000, 12 Ago 2013.**

[13]: http://res2.windows.microsoft.com/resbox/es/windows%20vista/main/d814bdd5-a33e-42f7-8417-7058a7df0440_0.png, **MICROSOFT, 18 Dic 2003, 12 Ago 2013.**

[14]: http://coding.smashingmagazine.com/2010/02/10/some-things-you-should know-about ajax/, **TRASNPORT, 2 Mar 2000, 12 Ago 2013.**

ANEXO A: GLOSARIO DE DE ACRÓNIMOS

API	Application Programming Interface
RIA	Rich Internet Applications
SDK	Software Developers Kit
SMTP	Simple Mail Transfer Protocol
EFF	Electronic Frontier Foundation
OTP	One Time Password
FA	Falsa aceptación
FN	Falsa negación
TFA	Tasa de falsa aceptación
TFN	Tasa de falsa negación