FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

SISTEMA BASADO EN BIOMETRIA DE LA DINAMICA DE TECLEO, APLICANDO RUP, PARA LA AUTENTICACIÓN DE PERSONAL EN LA EMPRESA SEVEROX PERU S.A.C

PARA OBTENER EL TÍTULO DE

INGENIERO DE SISTEMAS

AUTOR

JORDAN ALEXANDER DIAZ DIAZ

ASESOR

DR. JAVIER GAMBOA CRUZADO

LÍNEA DE INVESTIGACIÓN

DESARROLLO DE SOFTWARE

LIMA, PERÚ, MARZO DE 2021

DEDICATORIA

Dedico esta tesis en primer lugar a mis padres por todo su apoyo.

AGRADECIMIENTOS

Agradezco a todos los profesionales que contribuyeron en el desarrollo de esta tesis.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

SISTEMA BASADO EN BIOMETRIA DE LA DINAMICA DE TECLEO, APLICANDO RUP, PARA LA AUTENTICACIÓN DE PERSONAL EN LA EMPRESA SEVEROX PERÚ S.A.C

JORDAN ALEXANDER DIAZ DIAZ

UNIVERSIDAD AUTÓNOMA DEL PERÚ

RESUMEN

En la actualidad, en las empresas de seguridad se usan sistemas de autenticación de un solo factor y también de doble factor de autenticación que no son muy seguros ya que sufren problemas de seguridad en su implementación. La presente tesis plantea la implementación de un sistema basado en biometría de la dinámica de tecleo, aplicando RUP, para la autenticación de personal en la empresa Severox Perú S.A.C. La finalidad al implementar un sistema de autenticación basado en biometría de dinámica de tecleo es contar con sistema que autenticación de doble factor basado en biométrica de dinámica del tecleo que mejorara la seguridad y exactitud en la autenticación del personal de la empresa Severox Perú S.A.C.

Palabras Clave: Doble factor de autenticación, biometría, metodología RUP, dinámica de tecleo.

SYSTEM BASED ON BIOMETRY OF THE TYPE OF DYNAMICS, APPLYING RUP, FOR THE AUTHENTICATION OF PERSONNEL IN THE COMPANY SEVEROX PERÚ S.A.C

JORDAN ALEXANDER DIAZ DIAZ

UNIVERSIDAD AUTÓNOMA DEL PERÚ

ABSTRACT

Currently, security companies use single-factor authentication systems and double-factor authentication systems that are not very secure since they suffer from security problems in their implementation. This project proposes the implementation of a system based on typing dynamics biometry, applying RUP, for the authentication of personnel in the Severox Peru S.A.C. The purpose of implementing an authentication system based on typing dynamics biometrics is to have a two-factor authentication system based on click dynamics biometrics that will improve the security and accuracy in the authentication of the personnel of the company Severox Peru S.A.C.

Keywords: Double factor authentication, biometrics, RUP methodology, typing dynamics.

INTRODUCCIÓN

Los sistemas de autenticación basados en un usuario y contraseña son los más usados para la protección de recursos en sistemas, pero han demostrado con el tiempo lo débiles que son a cierto tipo de ataques los cuales tiene como objetivo saltarse la protección brindada por estos sistemas de autenticación.

Por tal motivo es que se plantea esta tesis, para ayudar en la seguridad de los sistemas de autenticación basados en el ingreso de un usuario y contraseña aumentándole un nivel de autenticación más.

En el Capítulo I – Problema de la Investigación: se realiza todo el análisis de la realidad problemática, el planteamiento metodológico, la hipótesis de la investigación junto con el objetivo general y los específicos.

En el Capítulo II – Marco Teórico: se realiza el marco teórico investigando todas las tesis relacionadas con el tema, luego el marco conceptual, donde se colocan todas las definiciones y temas que serán utilizados en el desarrollo de la tesis.

En el Capítulo III – Marco Metodológico: se hace el estudio de factibilidad para luego hacer el análisis del sistema, creando los casos de uso, diagramas de clases, y de secuencia.

En el Capítulo IV – Desarrollo de Solución: se hace el desarrollo de la solución teniendo como puntos el estudio de factibilidad, modelamiento y metodología aplicada al desarrollo de la solución.

En el Capítulo V – Análisis e Interpretación de Resultados: se hace el análisis e interpretación de resultados y su contrastación de hipótesis.

En el Capítulo VI – Discusiones, Conclusiones y Recomendaciones: se hacen las conclusiones las conclusiones y recomendación de la presente investigación.

CAPÍTULO I
PROBLEMA DE LA INVESTIGACIÓN

1.1 Realidad problemática

a) Ámbito internacional

En la actualidad se puede ver que el mundo de la seguridad ha tomado una gran importancia en nuestras vidas, pero toda tecnología trae consigo problemas como la seguridad al autentificarse en una aplicación de escritorio el cual va a permite acceso a recursos del sistema por lo cual los sistemas de autenticación actuales usados por empresas y bancos donde se puede ver que sus sistemas de autenticación se basan en el ingreso de un usuario y su contraseña, el cual no brinda la adecuada seguridad ya que puede ser vulnerada de distintas formas como ataques de fuerza bruta, robos de sesión o robos de credenciales por lo cual es necesario un sistema de autenticación de doble factor el cual tenga el usuario, contraseña y la identificación de la dinámica de tecleo que se hace al usuario al ingresar su usuario y contraseña mejorando así la autenticación en la aplicaciones de escritorio.

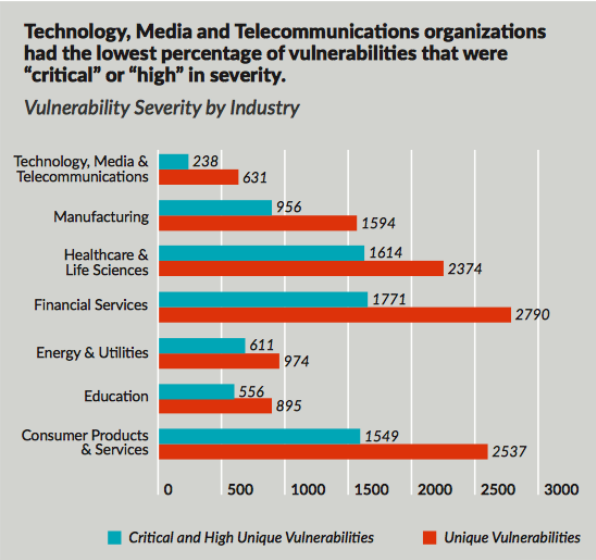

Figura 1. Vulnerabilidades por industria. Adaptado de *CTMfile.*

Figura 2. Las peores contraseñas de 2020. Adaptado de *NordPass*

b) Ámbito nacional

En el Perú, el uso de sistema biométricos y dobles factores de autenticación para la autenticación a sistema de escritorio es poco usada por las empresas ya que conllevan un costo extra o bien son difícil de implementar en los sistemas, mayormente los sistemas biométricos como doble factor de autenticación son usados por entidades gubernamentales.

Figura 3. La Seguridad informática en el Perú. Adaptado de *gestion.pe*

c) Ámbito Institucional

Actualmente la empresa Severox Perú S.A.C. tiene desarrollado software in-house. Esta es una pequeña empresa que se creó como un emprendimiento de un grupo de personas. Al trabajar con información sensible la empresa busca mejorar la seguridad de autenticación de sus sistemas desarrollados.

d) Definición del problema

Actualmente la empresa Severox Perú S.A.C. no tiene una correcta seguridad en la autenticación de sus sistemas in-house.

Todos los sistemas desarrollados por la empresa cuentan con un sistema de autenticación básico (usuario y contraseña) que no tienen ningún tipo de doble factor ni de seguridad biométrica por lo que pueden ser vulnerables por delincuentes informáticos o personas de la misma institución.

Frente a esto la empresa teme por la seguridad de su información ya que podría ocasionarles pérdidas económicas y de información privada.

El proceso de autenticación muestra los siguientes problemas:

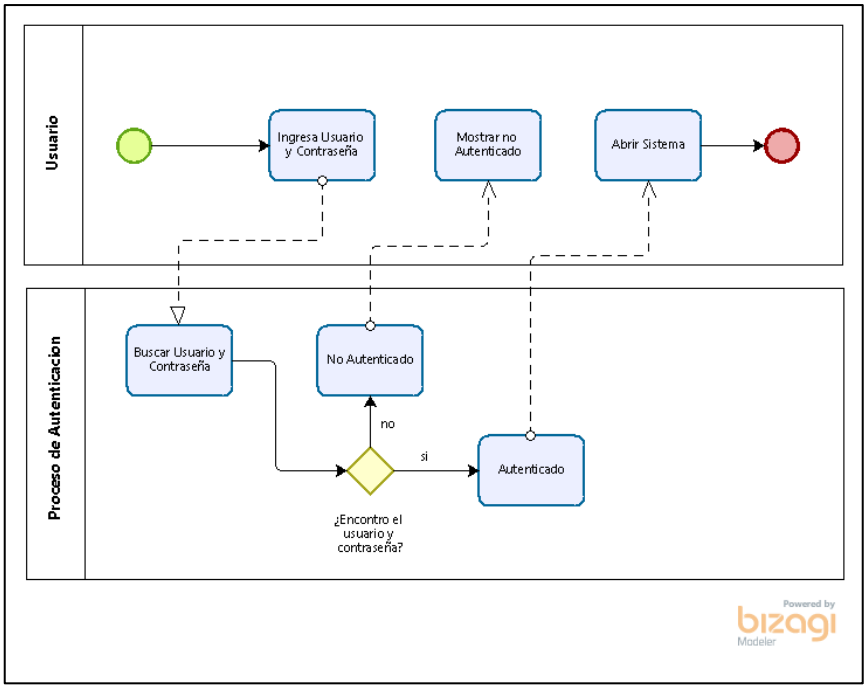

Figura 4. Proceso de Autenticación (as-is).

- Número de incidentes que se informaron
- Costos por incidente
- Nivel de Satisfacción
- Exactitud de la autenticación

Tabla 1

Datos actuales de los indicadores

Indicador	Datos de Pre-Prueba (Promedio)
	6 por mes
Costo por incidente	650 soles por mes
Nivel de Satisfacción en el uso del sistema	Mala
Exactitud de la autenticación	60%

Para solucionar estos problemas que existe en los sistemas desarrollados al autenticarse los usuarios la solución más factible es implementar una aplicación basada en biometría de la dinámica de tecleo, para satisfacer la necesidad de seguridad, mejorar la exactitud de autenticación y bajar el número de incidentes que se informan por mes.

Cuadro comparativo entre la situación actual (AS IS) y la situación propuesta (TO BE).

Tabla 2

Comparación de as – is y to – be

Situation Actual (AS IS)	Situación Propuesta (TO BE)
Insatisfacción de los usuarios por la seguridad de los sistemas desarrollados	Satisfacción de los usuarios por mejora en la seguridad de sus sistemas
Cantidad de incidentes de seguridad registrados por mes	Disminución de la cantidad de incidentes registrados por mes
Baja seguridad en los sistemas por la autenticación	Mejora en la seguridad a la hora de autenticarse
Costos por problemas de seguridad	Reducción en los costos ocasionados por problemas de seguridad

1.1.1. Problema general

¿En qué medida el uso de un Sistema Basado en Biometría de la Dinámica de Tecleo, aplicando la metodología RUP, mejora la Autenticación de Personal en la empresa Severox Perú S.A.C.?

1.1.2. Problemas específicos

- ¿En qué medida el uso de un sistema basado en biometría de la dinámica de tecleo aplicando la metodología RUP, mejora la seguridad al autenticarse en la empresa Severox Perú S.A.C.?

- ¿En qué medida el uso de un sistema basado en biometría de la dinámica de tecleo aplicando la metodología RUP, disminuye el número de incidentes de seguridad reportados en la empresa Severox Perú S.A.C?

- ¿En qué medida el uso de un sistema basado en biometría de la dinámica de tecleo aplicando la metodología RUP, disminuye los costos por incidente de seguridad en la empresa Severox Perú S.A.C.?

- ¿En qué medida el uso de un sistema basado en biometría de la dinámica de tecleo aplicando la metodología RUP, incrementa el nivel de satisfacción del personal en la empresa Severox Perú S.A.C?

- ¿En qué medida el uso de un sistema basado en biometría de la dinámica de tecleo aplicando la metodología RUP, mejora la exactitud de autenticación en la empresa Severox Perú S.A.C?

1.2 Justificación e importancia de la investigación

a) Conveniencia

La presente investigación mejorara la seguridad en la autenticación del personal de la empresa.

b) Relevancia Social

La finalidad de esta investigación será desarrollar un aplicativo que nos permita mejorar la seguridad en la autenticación del personal de la empresa Severox Perú S.A.C.

c) Aplicación practica

En la actualidad la aplicación de biometrías para la autenticación de personas se está convirtiendo en una gran herramienta en procesos de seguridad. Me veo en la necesidad de trabajar con estas herramientas para poder mejorar el proceso de autenticación de personas.

d) Valor teórico

El presente investigación se podrá conocer la exactitud que nos da la autenticación por biometría de dinámica de tecleo y explorar la mejora en la seguridad y satisfacción del personal de la empresa Severox Perú S.A.C.

e) Utilidad metodología

La investigación servirá a la vez como un instrumente de medida de la fiabilidad de la autenticación por biometría de dinámica de tecleo lo que permitirá mejoras en los métodos de autenticación actuales.

1.2.1 Viabilidad

a) Viabilidad económica

Este proyecto es factible económicamente ya que se contamos con los recursos económicos necesarios para realización de la tesis.

b) Viabilidad técnica

La investigación es viable ya que los recursos necesarios para realizar la tesis son accesibles. Lo cual nos genera una gran ventaja al contar con las herramientas requeridas para la tesis

c) Viabilidad operativa

La tesis es viable operativamente ya que estamos realizando una profunda investigación en tesis, libros, artículos, entre otros.

1.3 Objetivos de la investigación: general y específicos

1.3.1 Objetivo general

Mejorar el proceso de autenticación de personal mediante un sistema Basado en biometría de la dinámica de tecleo, para la autenticación de personal en la empresa Severox S.A.C., aplicando RUP.

1.3.2 Objetivos específicos

- Disminuir el número de incidentes que se informaron.
- Disminuir el costo de los incidentes que se informaron.
- Mejorar el nivel de satisfacción en el uso del sistema.
- Mejorar la exactitud de la autenticación.

1.4 Limitaciones de la investigación

- El tiempo para completar la investigación es corto.
- Son pocas las investigaciones hechas sobre el tema.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de estudios

Hoy en día existen pocos sistemas que brindan autenticación de doble factor usando biometría de tecleo, generalmente el desarrollo de estos sistemas en el país y sobre todo en la ciudad de Arequipa es muy poco por no decir nulo, debido a problemas económicos y a la falta de una cultura de investigación de proyectos en el país, como podemos observar en la figura 4, mostrado a continuación. Estos sistemas de información son desarrollados normalmente fuera del país por lo que su costo es alto y no suele ofrecer soluciones personalizadas.

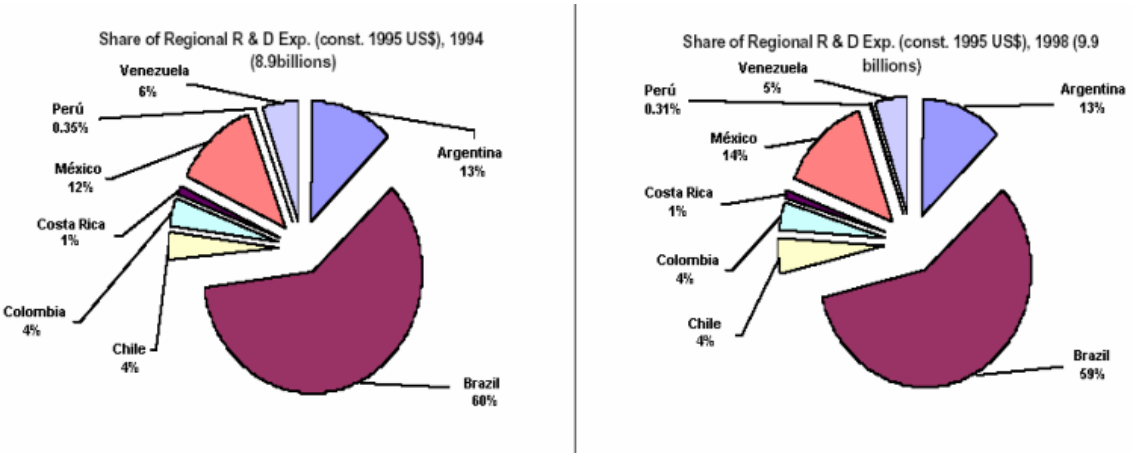

Figura 5. Investigación y desarrollo del Perú con respecto a otros países. Adaptado de *La participación pública y privada en la investigación y desarrollo e innovación.*

a) Sistema de protección de datos usando dinámica de tecleo

En este artículo, se presenta una metodología basada en la dinámica dactilar. Se llama dinámica dactilar, a los eventos de pulsar-soltar y soltar pulsar y al tiempo transcurrido entre estos dos eventos, es decir la velocidad del desplazamiento transcurrido entre tecla y tecla. Estos tiempos se definen por usuario, teniendo así una huella digital de acceso al sistema computacional de datos.

Para ello se desarrolló una herramienta capaz de medir los tiempos de tecleo de cada usuario. Los componentes que integran esta herramienta son: rutinas para la detección de eventos del teclado, un contador de tiempo, rutinas

para la selección de modelo estadístico dependiendo del comportamiento de los tiempos del usuario. Esta herramienta se implementó en equipos móviles (laptop). Para el proceso de autentificación se han definido dos modelos estadísticos. El primero originado por el comportamiento de los tiempos del usuario y el segundo basado en el comportamiento de la totalidad de los tiempos de todos los usuarios. A esto le denominamos autenticación conjunta. (Acosta y Torres, 2008).

b) Sistema de autenticación para dispositivos móviles basados en la Biometría de la dinámica de tecleo

La tesis pretende desarrollar un sistema capaz de reconocer dinámicas de tecleo y que pueda trabajar en conjunto, de forma transparente, con los tradicionales sistemas de autenticación basados en nombre de usuario y contraseña fortaleciendo la seguridad proporcionada por estos últimos, mediante el uso de biometría de dinámica del tecleo para el reconocimiento de los patrones de tecleo en dispositivos móviles usando latencias y probabilidades para las creación de la plantilla y funciones estadísticas de dispersión para la comparación de las plantillas la cual dará si un usuario es autenticado con éxito o no. (Iglesias, 2007).

c) Reconocimiento de escritor independiente de texto basado en características de la escritura

El presente proyecto se centrará en el estudio de una serie de características que permitan identificar a las personas en base a su escritura independientemente del contenido del texto escrito. Se asumirá que las muestras de escritura han sido tomadas de forma natural, es decir, sin alterar el estilo en el que el individuo suele escribir y manteniendo la curvatura y forma de las letras junto con su separación original. Para desarrollar el estudio se utilizarán una serie de características que operan en el nivel de análisis de textura. Las características del nivel de textura proporcionan información referente a la forma habitual de cada individuo de coger el bolígrafo y la inclinación preferente de los trazos a la hora de escribir, junto con la curvatura.

El objetivo final de este proyecto es estudiar, desarrollar, implementar y documentar un sistema automático de identificación y verificación de escritor independiente de texto. Empleando un método independiente de texto presenta varias ventajas dado que no es necesario conocer el contenido semántico del mismo y requiere una mínima intervención humana. (Pecharromán, 2007).

d) Captura de datos para análisis de la dinámica del tecleo de números para sistema operativo Android

En este artículo, se desarrolló una aplicación para sistema operativo Android, que permite capturar los tiempos de presión y de cambio en este tipo de teclado. Se realizaron pruebas con 14 usuarios reales, a quienes se solicitó capturar un mismo nombre de usuario y contraseña un total de 10 veces. Los datos generados para cada intento exitoso se han puesto disponibles públicamente en la Internet, para ser utilizados en futuros experimentos. (Nieto, Gómez, López y Rojas, 2015).

e) Autenticación web de estudiantes mediante reconocimiento biométrico

En este trabajo se hace un análisis de reconocimiento biométrico basado en dinámica de tecleo para la autenticación de estudiantes en entornos web. A diferencia de la autenticación basada en algo que tenemos o algo que sabemos, el reconocimiento biométrico hace uso de características propias de los individuos para verificar sus identidades. En este trabajo se estudian las características de estos sistemas, así como su idoneidad para la aplicación en entornos docentes. Los resultados muestran una tasa de reconocimiento superior al 90% lo cual anima a seguir investigando esta línea para su implementación en entornos reales. (Morales, Fierrez, Vera y Ortega, 2015).

f) Autenticación y verificación de usuarios mediante dinámica del tecleo

La dinámica de tecleo ofrece una gran cantidad de posibilidades y técnicas a la hora de evaluar a un usuario. Por tanto, en este apartado explicaremos todo lo necesario para comprender el funcionamiento básico de un sistema de dinámica de pulsación y los datos que utiliza.

Este tipo de sistema sigue la siguiente estructura:

- Extracción de características: obtenemos los datos más relevantes de cada usuario para poder utilizarlos más tarde.
- Clasificación de usuarios: aplicamos diferentes cálculos en los datos obtenidos para decidir si un usuario es auténtico o es un impostor.
- Evaluación del rendimiento: realizamos una clasificación de usuarios masiva para obtener métricas sobre la eficiencia del sistema. (Rivilla, 2017).

g) Patrones de digitación para evitar la suplantación de identidad en el sistema transaccional de una Universidad Privada

En la presente tesis se muestra la aplicación de un método biométrico de autentificación para el acceso y uso del sistema académico de la Universidad Privada, el método biométrico está basado en el reconocimiento del patrón de tecleo del usuario; en inglés KeyStrokes Dynamics, o dinámica de tecleado. El método indicado, emplea cuatro características de tecleo: el código de la tecla presionada, dos tipos de tiempos entre pulsaciones de teclas consecutivas y el tiempo que cada tecla permanece presionada, las que en el sistema desarrollado se reconocen como: Código de la tecla, tiempo pulsar-pulsar, tiempo soltar-pulsar, tiempo pulsar soltar. Se llevaron a cabo pruebas de autenticación con 95 usuarios de la Universidad en mención, se consideraron pruebas durante 2 semanas. El software desarrollado contempla la ejecución del

proceso compuesto por dos fases. La primera fase considera la captura del patrón de digitación del usuario, mientras que, en la segunda fase, se aplicaron 4 ajustes de valores de Umbral, cada una con el objetivo de determinar el mejor valor de Umbral de aceptación, aplicando ajustes por aproximación. Los resultados finales de los experimentos arrojaron tasas de falsas aceptaciones con un valor de 1.89% y la tasa de falso rechazo obtenida al concluir el cuarto ajuste fue de 1.58%. (Marquez, 2018).

h) Método de autenticación basado en la dinámica de tecleo

En esta investigación se ha creado un método, el cual está compuesto por etapas, las cuales describen como realizar el reconocimiento de patrones biométricos, basados en la dinámica de tecleo de los usuarios, que se autentifiquen en una aplicación la cual fue implementada para demostrar el uso del método propuesto. Es importante destacar que la finalidad del método es generar información única a partir del comportamiento del usuario. Esta información es lo suficientemente diferente para cada uno, de tal manera que lo distinga de los demás usuarios. (Ugarte, 2018).

2.2. Bases teórico-científicas

a) Dinámica de tecleo

Es un tipo de rasgo biométrico conductual empleado en la verifica identidad de un individuo mediante su cadencia de escritura. Esta tecnología se sostiene sobre la premisa de que cada individuo exhibe un patrón y una cadencia distintivos. La mayoría de los sistemas se emplea la latencia entre pulsaciones como característica, sin embargo en otros se utiliza también el tiempo que permanece la tecla presionada. Esta tecnología no requiere de hardware o dispositivos adicionales ya que se soporta sobre software de captura de la dinámica de tecleo. (Arribas y Puente, 2009)

Al escribir en el computador cada persona lo hace de diferentes formas, algunas personas teclean rápidamente y otras lentamente, algunas usan todos

los dedos y otras usan solo dos o tres, para algunos las teclas inferiores representan cierta dificultad y para otros las superiores. Son muchas la característica que permiten diferenciar a una persona de otra según la forma con la que teclean (Obaidat y Sadoun, 1997). Un sistema recibe estas características como métricas que intentan describir el ritmo con el que la persona teclea. Entre las características más comunes se encuentran:

1. Tiempo de vuelo: Es el tiempo entre el cual una tecla se está dejando de presionar y de manera consecutiva se presiona la siguiente, como se muestra en la Figura 6. Este tiempo generalmente oscila entre 50 a 800ms. (Adams, 2017).

2. Tiempo de retención: Tiempo en el cual se mantiene presionada una tecla (ver Figura 6), esta medida suele oscilar entre 60 y 140 ms. (Adams, 2017).

3. Tecla: Es la tecla que se presionó, esta característica da información del lado del teclado que está siendo usado. Esta característica se usa para llevar a contexto los tiempos de vuelo y retención. (Adams, 2017).

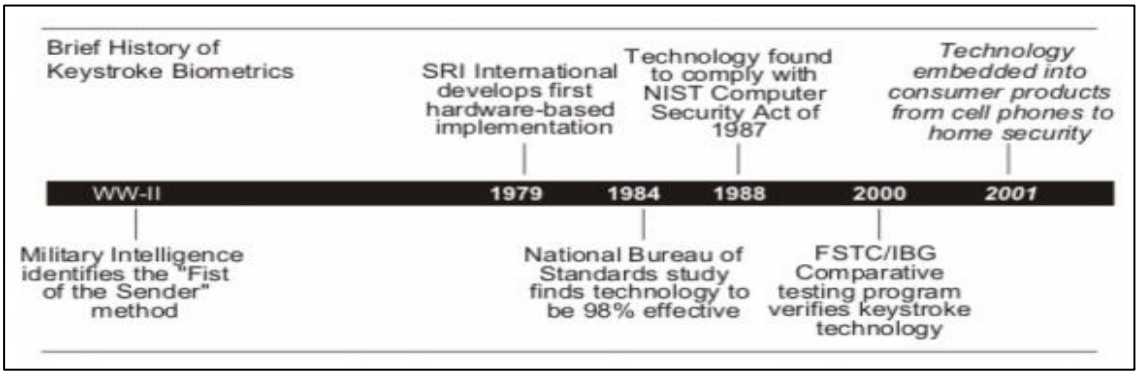

*Figura 6***.** Índice cronológico del desarrollo de la tecnología biométrica de escritura en teclado o dinámica de tecleo. Adaptado de *Sistema de Reconocimiento de Personas Mediante su Patrón de Iris Basado en la Transformada Wavelet.*

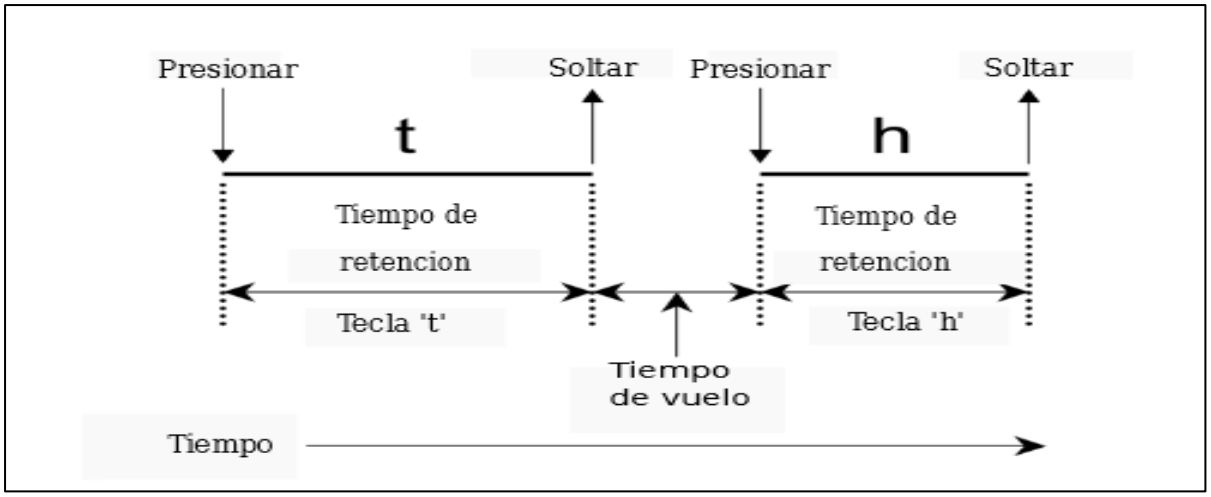

Figura 7. Relación entre el tiempo de retención y la latencia. Adaptado de *H. Crawford, "Keystroke dynamics: Characteristics and opportunities", en 2010 Eighth International Conference on Privacy, Security and Trust*,IEEE*, 2010, págs. 205-212 (Figura Adaptada)*

2.3. Definición de la terminología empleada

a) Biometría

Es decir, el reconocer a una persona por alguna característica biofísica o de comportamiento, está tomando cada vez más importancia en la actualidad. Su importancia radica en las limitaciones de los sistemas actuales de identificación personal, los cuales en su mayoría, están restringidos al uso de dispositivos externos como tarjetas inteligentes y claves personales. La biometría está basada en el principio de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris de los ojos, etc.) o de comportamientos (la voz, la manera de firmar, etc.), los cuales pueden ser utilizados para identificarla o validar restricciones de acceso. (Ruíz, Rodríguez, y Olivares, 2009).

b) Biometría estática

Se sabe pues que la biometría estática pertenece a esos atributos fisiológicas que son ideales por ser humano y que son firmes en el tiempo.

- Patrón de Voz.
- Firma manuscrita.
- Dinámica de tecleo.
- Cadencia del paso.
- Análisis gestual. (Iglesias, 2007).

c) Biometría dinámica

Los psicólogos han demostrado que los seres humanos somos predecibles en nuestro desempeño de tareas repetitivas y rutinarias. Aprovechando estas predicciones es que se ha desarrollado la biometría dinámica o de comportamiento, que analiza rasgos de la persona tales como la voz, la forma describir, la manera de teclear e incluso el ritmo al caminar. (Iglesias, 2007).

d) Autenticación

Acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto puede significar 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 de autenticación. Los métodos de autenticación suelen dividirse en tres grandes grupos:

- Algo que el usuario sabe.
- Algo que éste posee.
- Una característica física del usuario o un acto involuntario de este. (García y García, 2007).

e) Autenticación biométrica

Es en el tercero de los métodos de autenticación en el que se encuadra la autenticación biométrica. La autenticación biométrica consiste en

la verificación de la identidad de un sujeto, basándose en ciertos elementos morfológicos que le son inherentes y que solo se dan en ese sujeto. Es decir, mediante la autenticación biométrica nos proponemos recopilar información acerca de un rasgo distintivo de una persona (su voz, su huella dactilar, entre otros) para más tarde ser capaces de comparar esa muestra con otra, tomada normalmente en ese mismo instante, y poder averiguar sisones iguales o no. (García y García, 2007)

f) Dinámica del tecleo

Es posible pensar que cada persona escribe con un teclado de manera diferente, mostrando diferencias en el tiempo transcurrido entre cada pulsación o el tiempo que se tiene pulsada cada tecla. No es un rasgo de muy alta capacidad discriminativa y puede ser variable al tratarse de una característica de comportamiento. Por el contrario, puede obtenerse de un modo no intrusivo (simplemente monitorizando al usuario) y al poder observarse durante un periodo de tiempo más o menos largo, permite verificar la identidad del usuario a lo largo de todo ese tiempo. Por ejemplo, si en un momento dado se observan cambios importantes en la dinámica de tecleo, puede considerarse que el usuario no es el mismo y a continuación, bloquear el sistema. (Ortega, Fernández y Coomonte, 2008)

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación

a) Aplicada**:** ya que se solucionará el problema del proceso de autenticación mediante sistema basado en biometría de la dinámica de Tecleo, aplicando RUP, para la autenticación de personal en la empresa Severox Perú S.A.C.

3.1.2 Nivel de investigación

a) Descriptivo: Describe la realidad problemática de cómo se encuentra la autenticación en la empresa Severox Perú S.A.C.

b) Predictivo**:** Se realizará la investigación de cómo influirá el uso de autenticación basada en biometría de dinámica de tecleo mejorará la autenticación del personal de la empresa Severox Perú S.A.C

3.1.3 Diseño de la investigación

El diseño de la investigación es experimental puro:

RGe X O1

RGc -- O2

Donde:

R= Elección aleatoria de los elementos de los grupos.

Ge = Grupo experimental: Grupo de estudio al que se le aplicara el estímulo (Sistema basado en Biometría de la Dinámica de Tecleo).

Gc = Grupo control: Grupo de control al que no se le aplicara el estímulo (Sistema basado en Biometría de la Dinámica de Tecleo).

O1 = Datos de la PostPrueba para los indicadores de la VD: Mediciones postprueba del grupo experimental.

O2 = Datos de la PostPrueba para los indicadores de la VD: Mediciones postprueba del grupo de control.

X = Sistema de Autenticación de personal: Estimulo o condición experimental.

-- = Falta de estímulo o condición experimental.

Descripción

Se trata de la conformación de un grupo experimental (Ge) conformado por el numero de representativo de actividades de Proceso de Autenticación, al cual a sus indicadores de Postprueba(O1), se le administra un estímulo o tratamiento experimental, Sistema basado en Biometría de la Dinámica de Tecleo como estímulo (X) para solucionar el problema de dicho proceso, luego se espera que se obtenga (O2).

3.2 Población y muestra

Tabla 3

Universo y muestra de investigación

Unidad Muestral	Universo	Muestra	Tipo de muestreo
Procesos de autenticación de personal Limitaciones: Empresas del sector de seguridad informática	Todos los procesos de autenticación de personal en empresas del sector de seguridad informática, tenemos: N= Indeterminado	Procesos de autenticación de personal en la empresa Severox Perú S.A.C. N=30	Aleatorio

3.3 Hipótesis

3.1.1 Hipótesis general

Si se usa un sistema basado en biometría de la dinámica del tecleo, aplicando RUP, entonces mejora el proceso de autenticación de personal en la empresa Severox Perú S.A.C.

3.1.2 Hipótesis especificas

- Si se usa un sistema basado en biometría de la dinámica del tecleo aplicando RUP, entonces disminuye los incidentes que se informan en la empresa Severox Perú S.A.C.
- Si se usa un sistema basado en biometría de la dinámica del tecleo aplicando RUP, entonces disminuye los incidentes que se informan en la empresa Severox Perú S.A.C.
- Si se usa un sistema basado en biometría de la dinámica del tecleo aplicando RUP, entonces mejora la satisfacción del personal de la empresa Severox Perú S.A.C.
- Si se usa un sistema basado en biometría de la dinámica del tecleo aplicando RUP, entonces incrementa la exactitud de la autenticación del personal de la empresa Severox Perú S.A.C.

3.4 Variables – operacionalización

3.4.1 Variables

Variable independiente: Sistema basado en biometría de la dinámica del tecleo.

Variable dependiente: Autenticación de personal en la empresa Severox Perú S.A.C.

Variable interviniente: Metodología rup

3.4.2 Indicadores

A) Conceptualización

i) Variable independiente: Sistema basado en biometría de la dinámica de tecleo

Tabla 4

Conceptualización de la variable independiente

Indicador: Presencia – Ausencia
Descripción: En este momento tiene el valor NO, es porque aún no existe el Sistema de Autenticación Basado en Biometría de la Dinámica del tecleo en la Empresa Severox Perú S.A.C. y aún estamos en la situación actual del problema. Cuando tome el valor SI, es porque ya se implementó el Sistema de Autenticación Basado en Biometría de la Dinámica del tecleo y se espera obtener mejores resultados.

ii) Variable dependiente: Autenticación de personal en la empresa Severox Perú S.A.C.

Tabla 5

Conceptualización de la variable dependiente

Indicador	**Descripción**
Número de incidentes que se informaron	Es el número de incidentes en el sistema transcurridos por mes
Costo por incidente	Es el costo por incidente que la empresa sufre por mes
Nivel de Satisfacción en el uso del sistema	Es el nivel de satisfacción del personal que hace uso del sistema de la empresa Severox Perú S.A.C.
Exactitud de la autenticación	Es el porcentaje de exactitud al autenticarse correctamente al sistema

B) Operacionalización

i) Variable independiente: Sistema basado en biometría de la dinámica de tecleo.

Tabla 6

Operacionalización de la variable independiente

Indicador	Índice
Presencia – Ausencia	No, Si

ii) Variable Dependiente: Autenticación de personal en la empresa Severox Perú S.A.C

Tabla 7

Operacionalización de la variable dependiente

Dimensión	Indicador	Índice	Unidad de Medida	Formula	Unidad de Observación
Incidente	Número de incidentes que se informaron	[4-6]	Número de incidentes	--- ---------	Revisión Manual/Virtual
	Costo por incidente	[500-650]	Cantidad de dinero	--- ---------	Revisión Manual/Virtual
	Nivel de Satisfacción en el uso del sistema	[mala-regular-buena]	Escala	--- ---------	Revisión Manual/Virtual
Calidad	Exactitud de la autenticación	[20-60]	(%)	Total de Autenticaciones correctas /Total de autenticaciones * 100	Revisión Manual/Virtual

3.5 Métodos ytécnicas de investigación

a) Técnicas de instrumentos de la investigación de campo

Tabla 8

Técnicas e instrumentos de la investigación de campo

Tecnicas	Instrumentos
1. Observación Directa • Individual 2. Realización de Entrevista • Estructurado • Dirigida 3. Aplicación de Cuestionario • Cerrado	• Ficha de observación • Formato de entrevista • Diario de Campo

b) Técnicas e instrumentos de la investigación experimental

Tabla 9

Técnicas e instrumentos de la investigación experimental

Técnicas	Instrumentos
• Seguimiento de la mejora del proceso de autenticación	• Diario de campo

c) Técnicas e instrumentos de la investigación documental

Tabla 10

Técnicas e instrumentos de la investigación documental

Técnicas	Instrumentos
Revisión de: • Tesis • Libros • Artículos científicos • Páginas web • Internet • Revistas	• Impresiones • Computadoras • Libreta de apuntes

3.6 Técnicas de procesamiento y análisis de datos

Una vez aplicado el instrumento “Cuestionario” al personal de la empresa Severox Perú S.A.C. que fueron elegidas teniendo en cuenta el muestreo estratificado por afijación proporcional, y posteriormente probabilístico aleatorio simple que determinó la representatividad de la muestra, se recogen los datos y se procede a la tabulación estadística, agrupados en función de las dimensiones de las variables de estudio, organizando la información en gráficos estadísticos.

Los datos recopilados se analizaron sobre una hoja de cálculo, el presenta tendencia y con el análisis se estimo la influencia de las variables sobre los observables.

Para el análisis de resultados y comprobación de hipótesis de la investigación, se utilizo el coeficiente de correlación lineal de Pearson; pensando para variables cuantitativas, es un índice que calcula el grafo de covariación entre diferentes variables relacionadas linealmente. Sus valores absolutos oscilan entre 0 y1.

Esto es, si tenemos dos variables X e Y, y definimos el coeficiente de correlación de Pearson entre estas dos vaiables como rxy entonces:

$$0 \leq r_{xy} \leq 1$$

Hemos especificado los términos “valores absoutos” ya que en realidad si se contempla el signo el coeficiente de correlación de Pearson oscila entre –1 y +1 (Restrepo, 2007). El análisis de la dispersión de los datos nos permite establecer si existe una relación entre los datos bajo estudio. Para el nivel de significancia se consideró un α=5%, equivalente a 0,05 en términos de probabilidad, para aceptar la hipótesis estadística alterna, con un nivel de confianza de 95%.

CAPÍTULO IV
DESARROLLO DE LA SOLUCIÓN

4.1 Estudio de factibilidad

4.1.1 Factibilidad técnica

El Equipo con el que se desarrollara la tesis tiene las siguientes características:

- Procesador Ryzen 5.
- Memoria 12000MB RAM.
- Capacidad libre en disco 60 GB.

Por otro lado, Software con el que se cuenta:

- Windows 10.
- Office 365.
- Visual Studio 2019.
- Rational Rose.

4.1.2 Factibilidad operativa

Para el desarrollo del presente proyecto, se cuenta con los conocimientos necesarios en materia de biometría de pulsaciones de teclado, así como en las maneras de medir los tiempos de los micro movimientos que involucra la medición de las pulsaciones.

4.1.3 Factibilidad económica.

La tesis será subvencionada en su totalidad por el investigador, los importes en los que se incurrirá en el presente trabajo están detallados a continuación:

A) Determinación del costo del sistema

1. Costos de personal:

Los costos de apoyo serán calculados teniendo en cuenta dos tipos de involucrados en la tesis los cuales son en primera instancia personal encargado del desarrollo en si del proyecto de investigación (jefe de proyecto, analista, programador, testeador, entre otros) y personal de apoyo (Asesoría de terceros y apoyo logístico si se da el caso).

a) Personal de desarrollo

Participa en todas las etapas del proyecto dado que estos involucrados serán representados por el investigador, el cual desarrollara todas las funciones las cuales son:

- Encargado del Proyecto
- Analista
- Programador
- Persona encargada de Pruebas

Todos los roles citados con anterioridad al ser desarrollados por el propio investigador tendrán coste cero y probablemente en una versión posterior se considerará el coste correspondiente de los roles citados.

b) Personal de apoyo

Una parte integral de la tesis está en la evaluación de asesorías adicionales las cuales tendrían un costo de S/.480.

Tabla 11

Personal Encargado del Desarrollo

Personal	Números de Meses	Tarifa Mensual	Total(S./)
Desarrollo en Si	3	950	2850.00
Apoyo	3	230	690.00
		Total	3540.00

2. Costos de equipo:

En cuanto a costos de equipos podemos mencionar dos clases de costos, uno relacionado con el desarrollo del aplicativo y otro relacionado con el equipamiento básico para el funcionamiento operativo del sistema.

a) Equipo para desarrollo

Si hablamos del equipo necesario para el desarrollo del proyecto, este es cubierto por el investigador por consiguiente no existe costo alguno y podemos especificar algunas características de este:

- Procesador Ryzen 5.
- Memoria 12000MB RAM.
- Capacidad libre en disco 60 GB.

b) Equipo para funcionamiento operativo

Al hablar del equipo operativo es hablar de lo mínimo que se considera para un adecuado funcionamiento del sistema el cual será:

- Procesador Intel Pentium I3.
- Memoria 4000MB RAM.
- Capacidad libre en disco 40 GB.

Tabla 12

Costos de equipos

Equipo	Cantidad	Costo unitario (S./)	Total(S./)
Computador	1	1686.00	1686.00
Monitor	1	500.00	500.00
Impresora	1	657,50	657.50
Kits Dispositivos Periféricos	1	189.00	189.00
		Total	3032.50

3. Costos de software:

En cuanto al valor del software, es tan igual como el valor del hardware, el cual es, para la despliegue del sistema y costo de software.

a) Costo de software para la implementación

Tabla 13

Costos de software de implementación

Software	Cantidad	Costo de licencia(S./)	Total(S./)
Windows 10	1	635.77	635.77
Office 365 Personal	1	219.99	219.99
Visual Studio 2019	1	(gratuito)	----------
SQL Server 2019 express	1	(gratuito)	--------
		Total	855.76

b) Costo de software para el funcionamiento

Tabla 14

Costos de software funcionamiento

Software	Cantidad	Costo de licencia(S./)	Total(S./)
Windows 10	1	635.77	635.77
		Total	635.77

4. Costos de suministros:

En suministros esenciales se consideran los siguientes: hojas bond, útiles de oficina, discos, tinta, memoria de USB.

Tabla 15

Costos de suministros

Suministro	Cantidad	Costo por Unidad (S./)	Total(S./)
Hojas Bond	½ millar	10.50	10.50
Útiles de Escritorio	1 kit	10.00	10.00
Tinta	1 recargar	6.50	6.50
Memoria USB	1	25.00	25.00
		Total	56.00

5. Costos de servicios:

En la siguiente parte se toman en cuenta los gastos de servicios como el agua, la luz y internet.

Tabla 16

Costos de servicios

Servicio	Cantidad/Mes	Costo Estimando al mes (S./)	Total(S./)
Luz %20	3	19.60	58.80
Agua %20	3	5.00	15.00
Internet %40	3	82.00	246.00
		Total	319.8

6. Resumen de costos:

En la siguiente parte se hace un resumen de todos los costos que serán utilizados en el desarrollo.

- Valor de desecho (VD): (3032.50*0.1)=303.25
  Denominador= (3+ (3*3))/2=6
  Suma a depreciar=3032.50-606.5= 2426

- Luz e Internet: (19.60*12) + (12*12)=379.20 y para cada año se tomará un incremento de 10% sobre el valor de dicho año.

Tabla 17

Resumen de costos

Criterio	Costo Inicial	Año 1	Año 2	Año 3
Personal	3540.00	------	------	------
Suministros	56.00	------	------	------
Software	635.77	------	------	------
Equipo de	(2426)	(5/15)	(4/15)	(3/15)
usuario	3032.50	1010.83	808.66	606.5
Servicios	319.8	379.20	417.12	458.83
Total	7584.07	1390.03	1225.78	1065.33

4.2 Modelamiento

4.2.1 Análisis de requisitos funcionales

Tabla 18

Requisitos Funcionales

Código	Requerimientos
R01	Autenticar Usuario Clásicamente
R02	Autenticar Biométricamente
R03	Registrar Usuario Clásicamente
R04	Registrar Usuario Biométricamente

R01: Autenticar usuario clásicamente.- el componente deberá verificar el usuario y contraseña de acceso del usuario.

R02: Autenticar biométricamente.- el componente deberá verificar la contraseña del usuario usando biometría de la dinámica de tecleo.

R03: **Registrar usuario clásicamente.-**el componente deberá permitir registrar nuevos usuarios.

R04: **Registrar usuario biométricamente.-**el componente deberá almacenar los patrones de tecleo del usuario ingresados en la contraseña al registrarse.

4.2.2 Análisis de requisitos funcionales

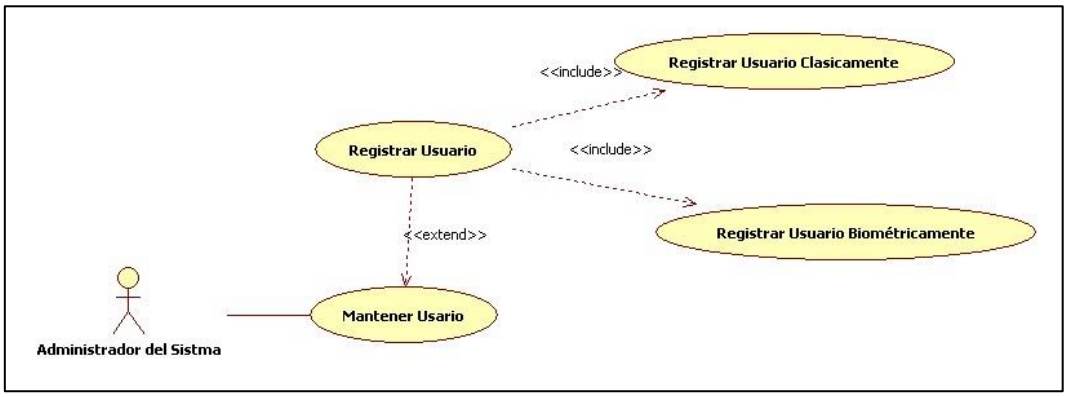

Figura 8. Diagrama de casos de uso – Registro de usuario.

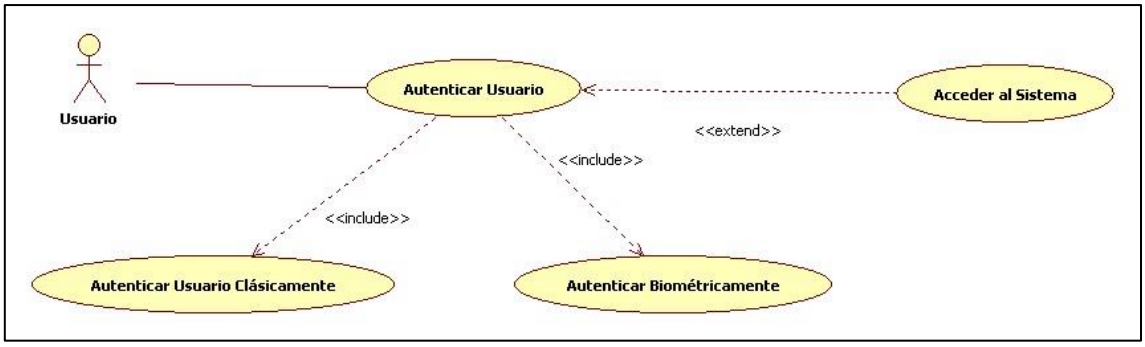

Figura 9. Diagrama de casos de uso – Autenticación de usuario.

Tabla 19

Especificaciones del caso de uso: Autenticar usuario

ID	ECU_01
Nombre	Autenticar usuario
Descripción	El Sistema deberá verificar el usuario y contraseña de acceso del usuario.
Autor	Jordan Diaz.
Actores	Usuario.
Prioridad	Alta.

Tabla 20

Especificaciones del caso de uso: Autenticar biométricamente

Especificación del caso de Uso: Autenticar biométricamente	
ID	ECU_02
Nombre	Autenticar biométricamente
Descripción	El componente deberá verificar la contraseña del usuario usando biometría de la dinámica de tecleo.
Autor	Jordan Diaz.
Actores	Usuario
Prioridad	Alta

Tabla 21

Especificaciones del caso de uso: Registrar usuario

Especificación del caso de Uso: Registrar usuario	
ID	ECU_03
Nombre	Registrar Usuario
Descripción	El componente deberá permitir registrar nuevos usuarios.
Autor	Jordan Diaz.
Actores	Usuario
Prioridad	Moderada.

Tabla 22

Especificaciones del caso de uso: Registrar usuario biométricamente

ID	ECU_04
Nombre	Registrar usuario biométricamente
Descripción	El componente deberá permitir registrar nuevos usuarios.
Autor	Jordan Diaz.
Actores	Usuario
Prioridad	Alta.

4.2.3 Lista de cotejos requisitos funcionales -Casos de uso

Tabla 23

Matriz de Cotejos

	C01	C02	C03	C04
R01			X	
R02		X	X	X
R03	X			
R04				X

4.2.4 Diagrama de secuencia

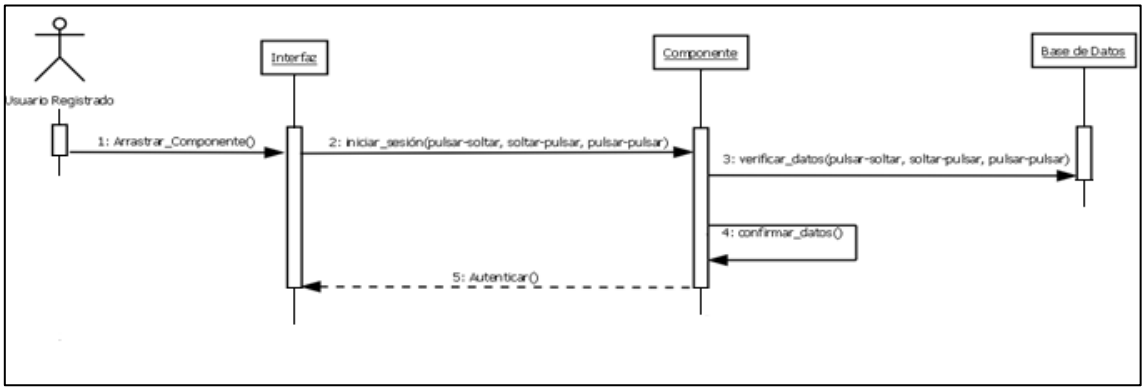

Figura 10. Autenticación de usuario

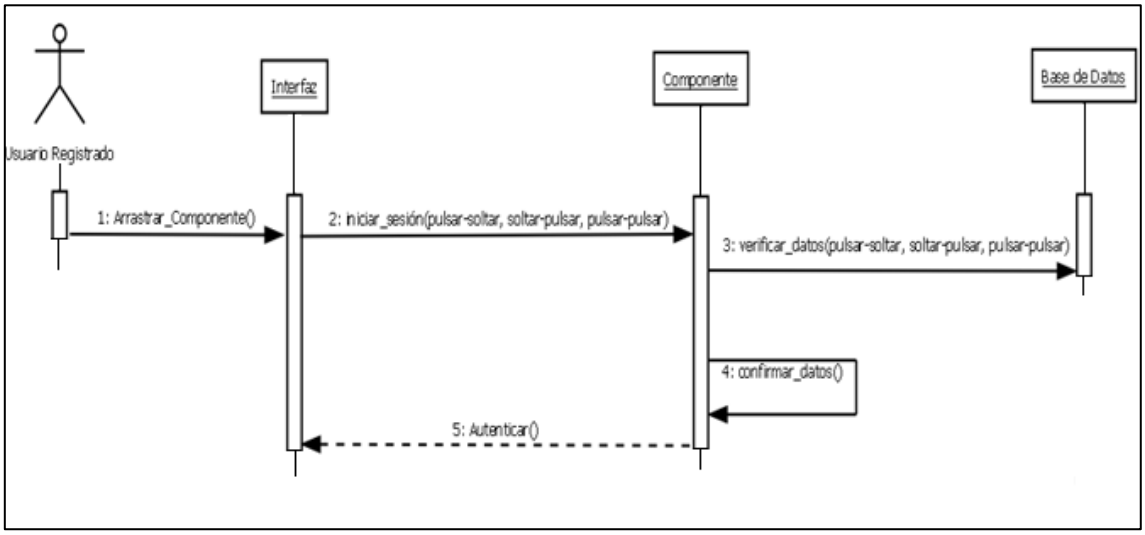

Figura 11. Autenticación de usuario

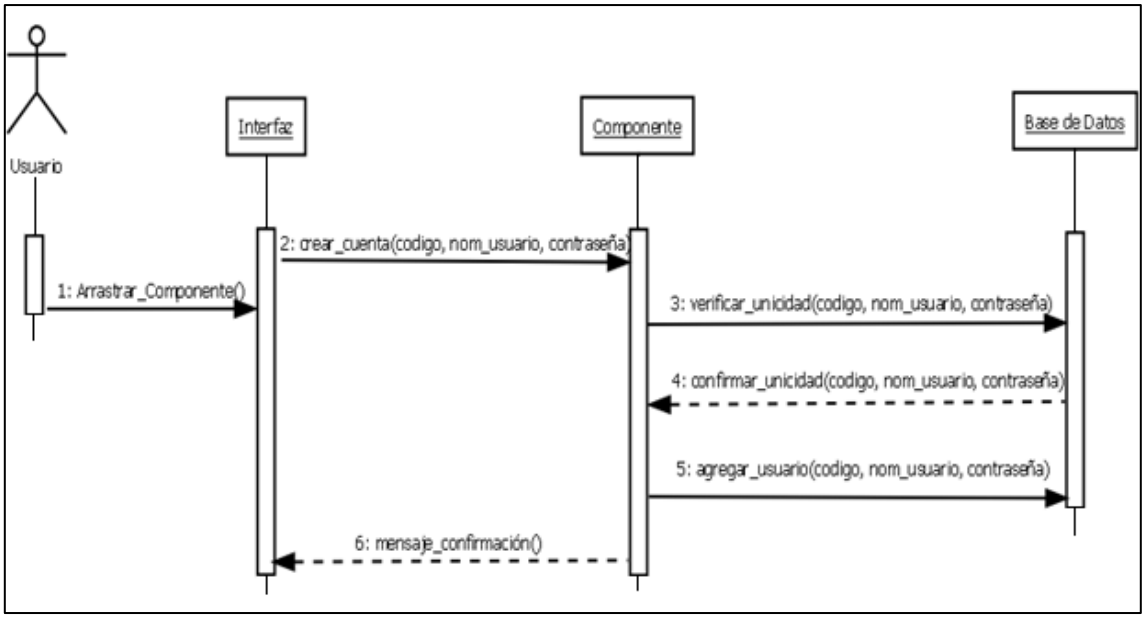

Figura 12. Registrar usuario

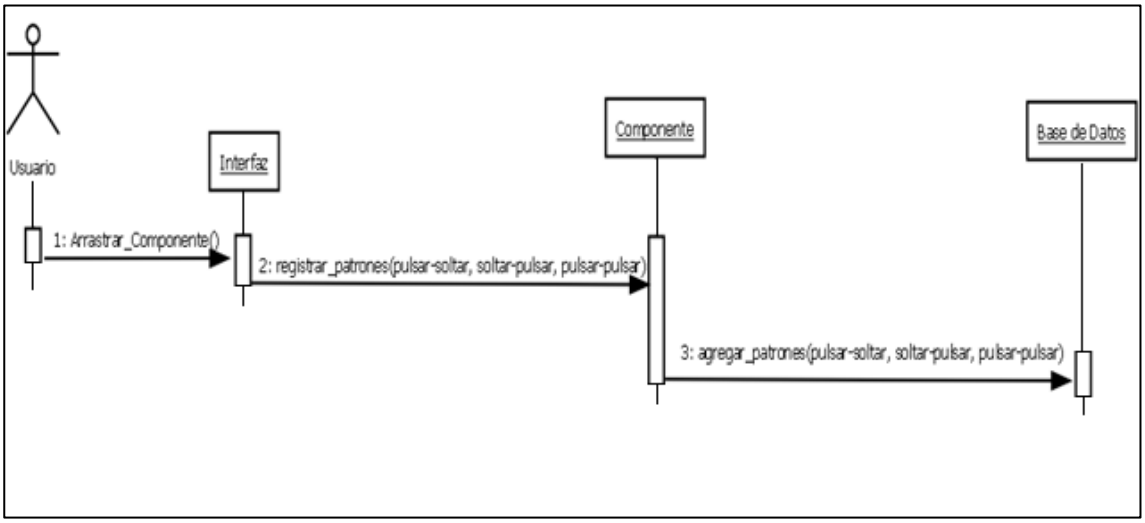

Figura 13. Registrar usuario biométricamente

4.2.5 Diagrama de Clases

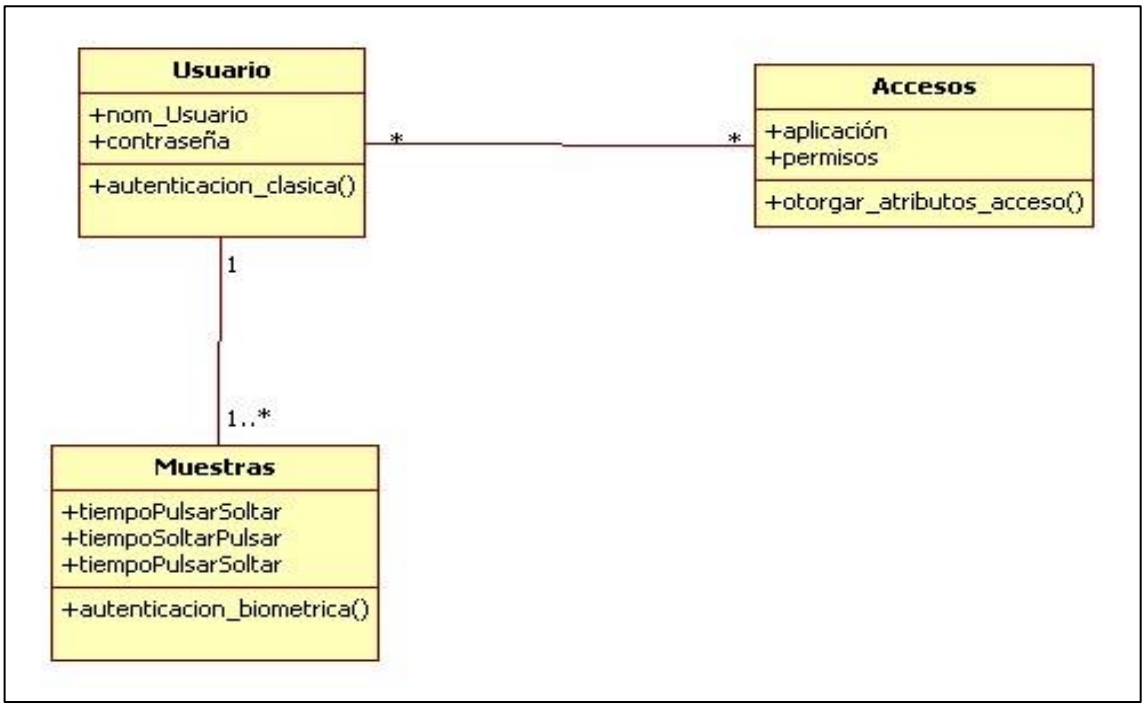

Figura 14. Diagrama de clases

4.3 Metodología aplicada al desarrollo de la solución

4.3.1 Diagrama de casos de uso

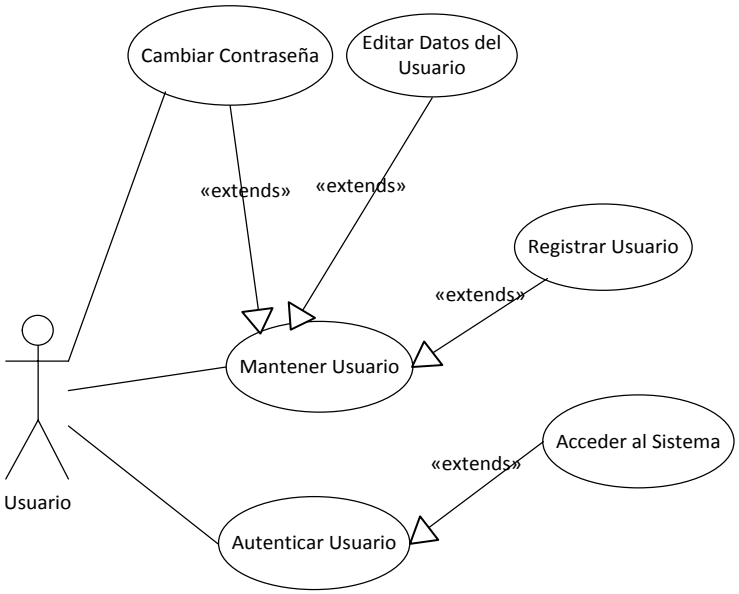

Figura 15. Modulo tecleo

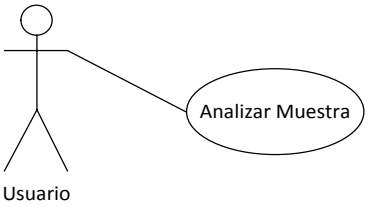

Figura 16. Modulo biometría.

4.3.2 Diagrama de componentes

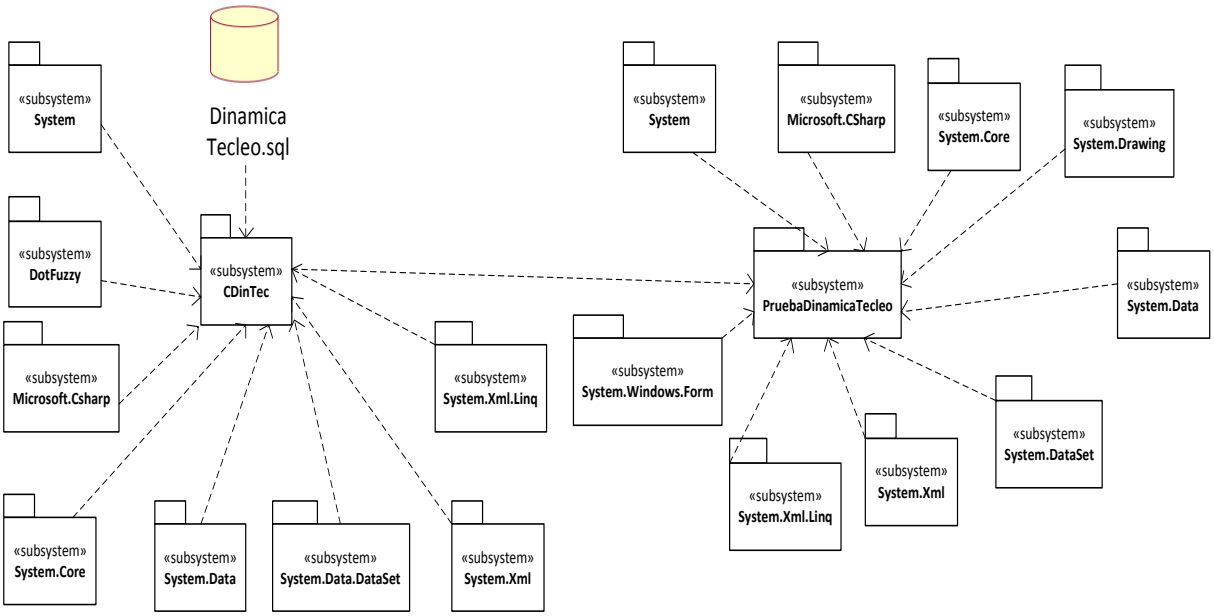

Figura 17. Diagrama de componentes.

4.3.3 Diagrama de Clases

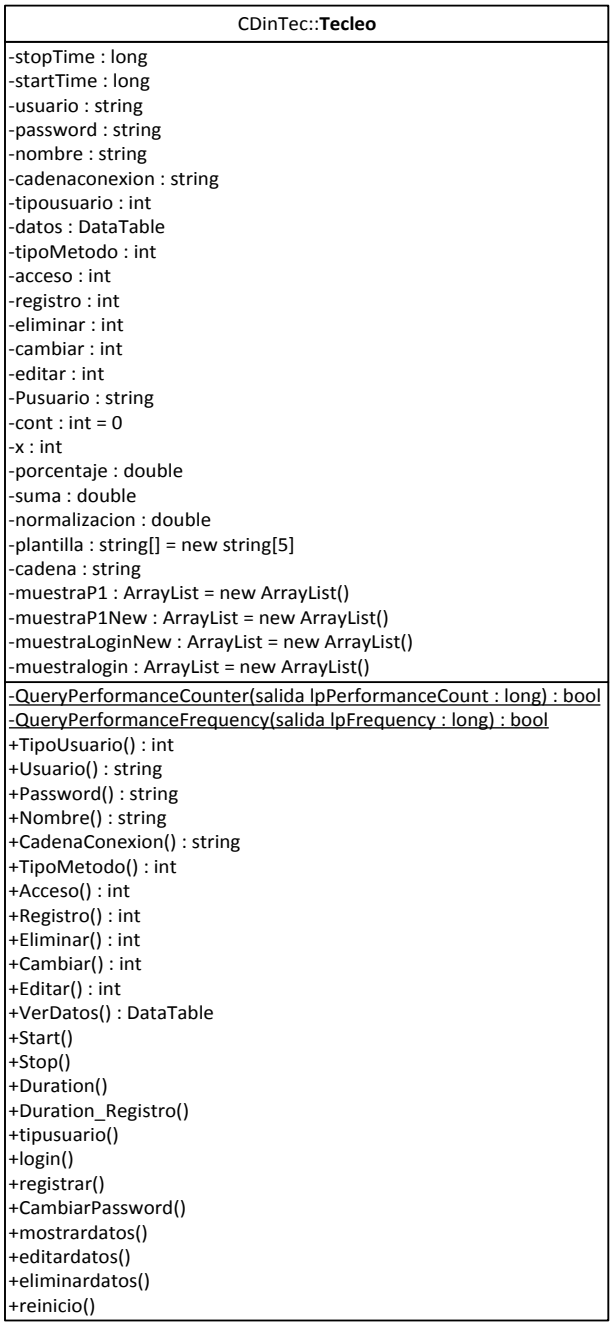

Figura 18. Clase tecleo.

CDinTec::**Biometria**
-muestra : double[,] = new double[5, 11] -Columna : double[,] = new double[5,11] -muestraloginB : ArrayList = new ArrayList() -mediaM : ArrayList = new ArrayList() -dstandarM : ArrayList = new ArrayList() -varinzaM : ArrayList = new ArrayList() -NmediaM : ArrayList = new ArrayList() -NdstandarM : ArrayList = new ArrayList() -NNdstandarM : ArrayList = new ArrayList() -NvarinzaM : ArrayList = new ArrayList() -scoring : ArrayList = new ArrayList() -muestralogin : ArrayList = new ArrayList() -usuario : string -password : string -cadenaconexion : string -delimit : char[] = new char[] { '/' } -sum : double -contador : int -avg : double -suma : double -normalizacion : double -promedio : double -obj : Tecleo = new Tecleo()
+MuestraLogin() : ArrayList +Usuario() : string +Password() : string +CadenaConexion() : string +reinicio() +SelecionMuestrasUsuario() +ordenardatos() +media() +desviacionstandar() +coeficientevariacion() +comparador() : double +nuevamedia() +nuevadesviacionstandar() +nuevavariacion() +verificar() : double

Figura 19. Clase biometría.

Figura 20. Diagrama de Clases.

4.3.4 Diagrama de colaboración

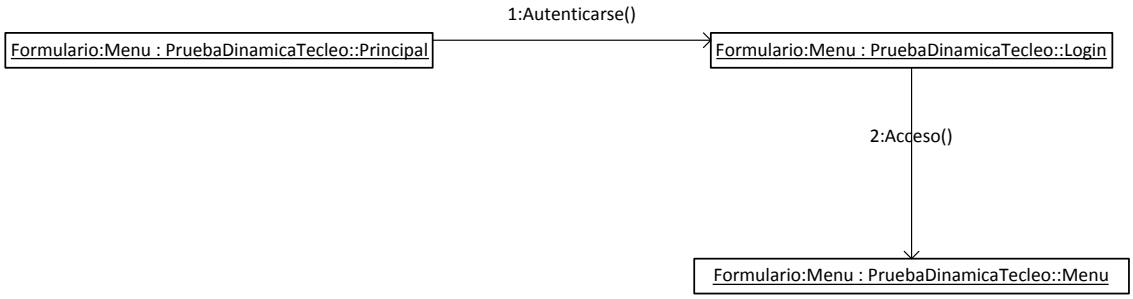

Figura 21. Diagrama de Colaboración – Autenticación.

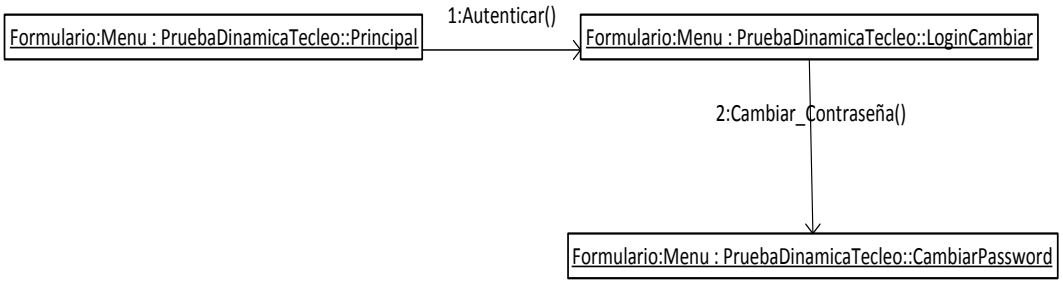

Figura 22. Diagrama de Colaboración – Cambiar contraseña.

4.3.5 Diagrama de secuencia

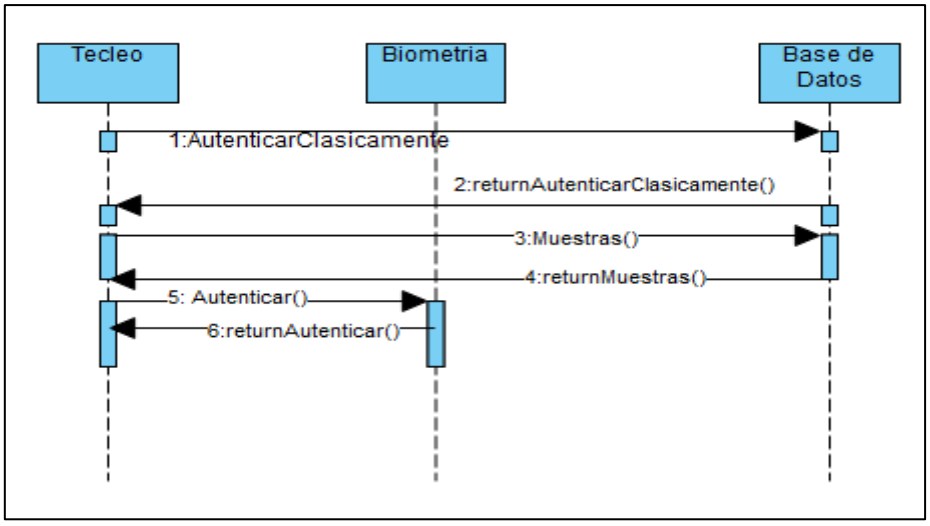

Figura 23. Diagrama de secuencia – autenticación.

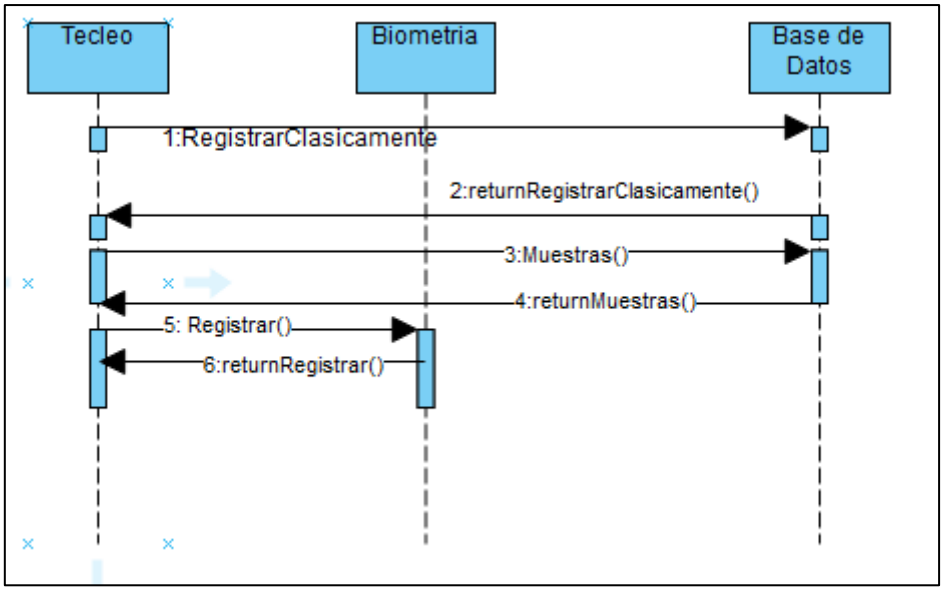

Figura 24. Diagrama de secuencia –registrar.

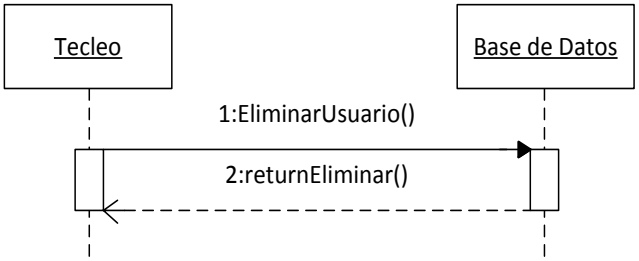

Figura 25. Diagrama de secuencia – eliminar.

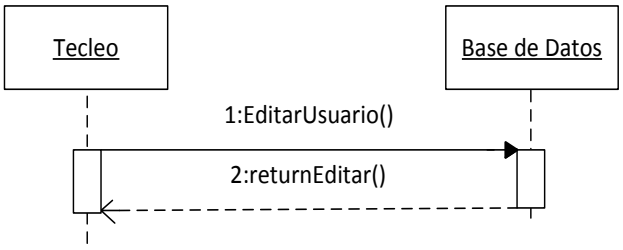

Figura 26. Diagrama de secuencia – editar.

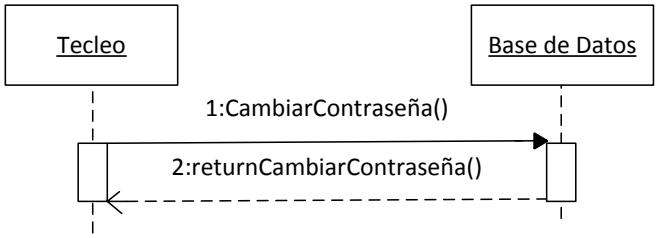

Figura 27. Diagrama de secuencia – Cambiar contraseña.

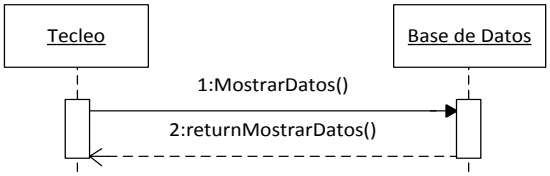

Figura 28. Diagrama de secuencia – Mostrar datos.

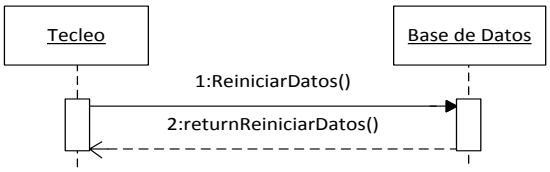

Figura 29. Diagrama de secuencia – Reiniciar datos.

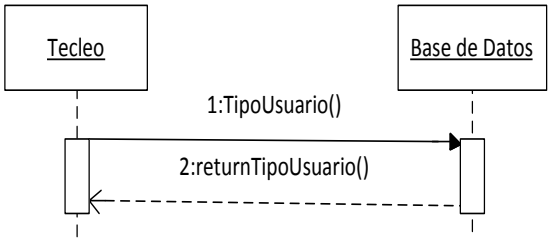

Figura 30. Diagrama de secuencia – Tipo de usuario.

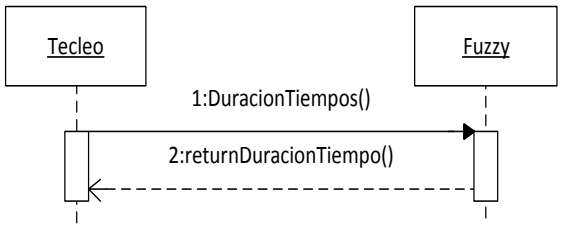

Figura 31. Diagrama de secuencia – Tiempo de duración.

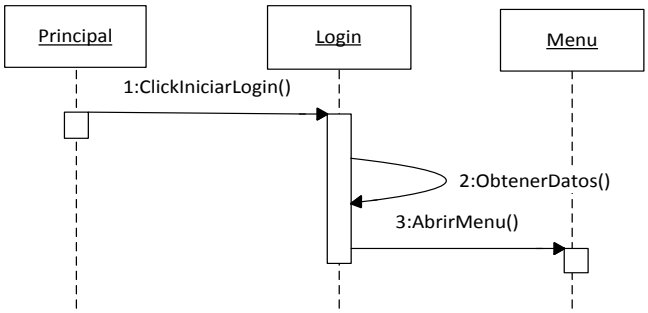

Figura 32. Diagrama de secuencia – Formulario login.

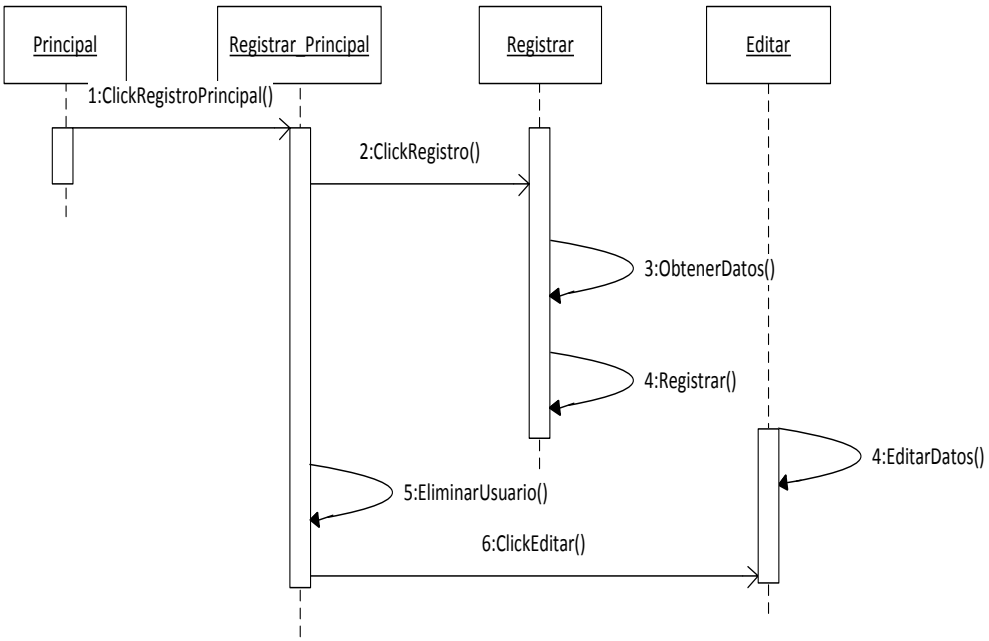

Figura 33. Diagrama de secuencia – Formulario registrar.

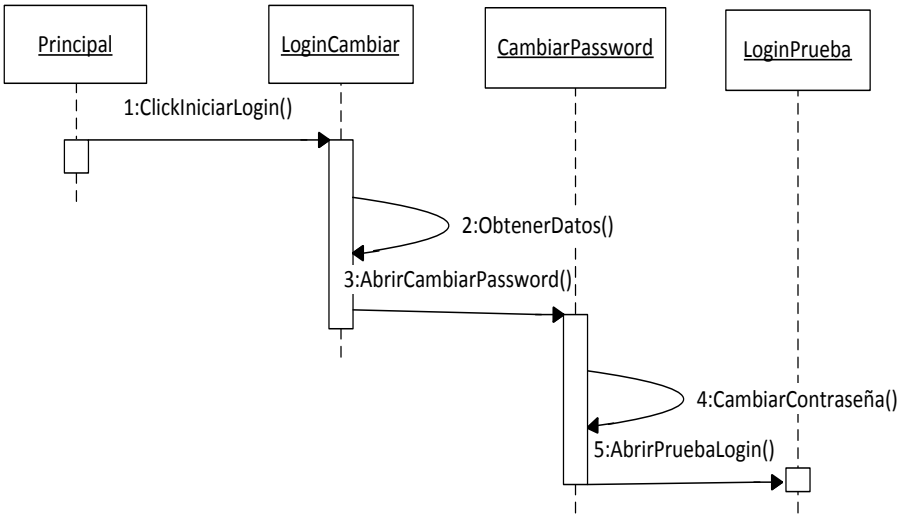

Figura 34. Diagrama de secuencia – Formulario cambiar contraseña.

3.6 Diseño de pantallas

A. Login

Para probar el login hacemos en el botón “Probar Login” del menú principal y luego en el formulario ingresamos nuestro usuario y contraseña.

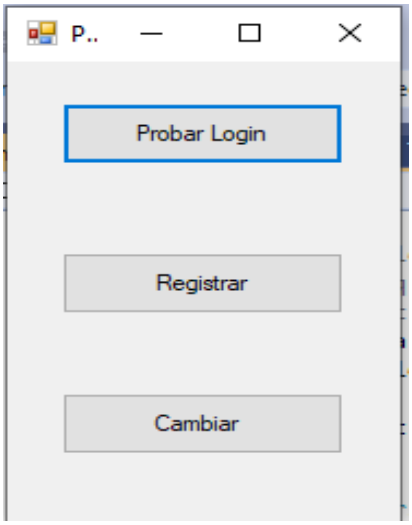

Figura 35. Formulario principal.

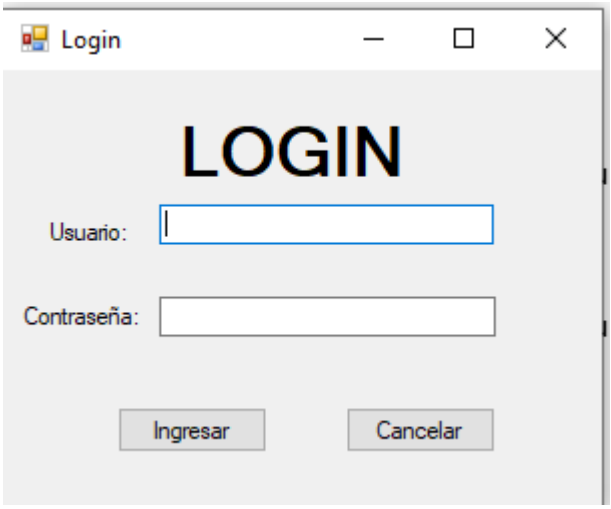

Figura 36. Formulario login.

B. Registrar

Para agregar, editar y eliminar se hace clic en el botón “Registrar” del menú principal.

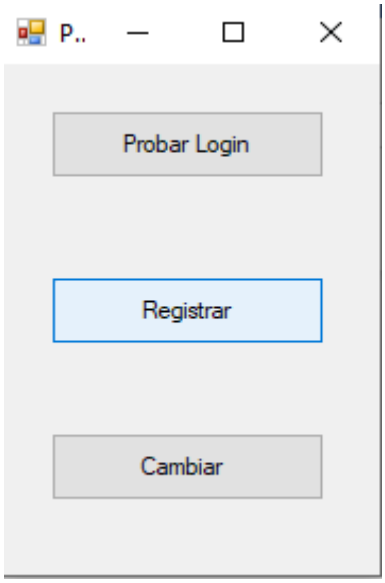

Figura 37. Formulario principal.

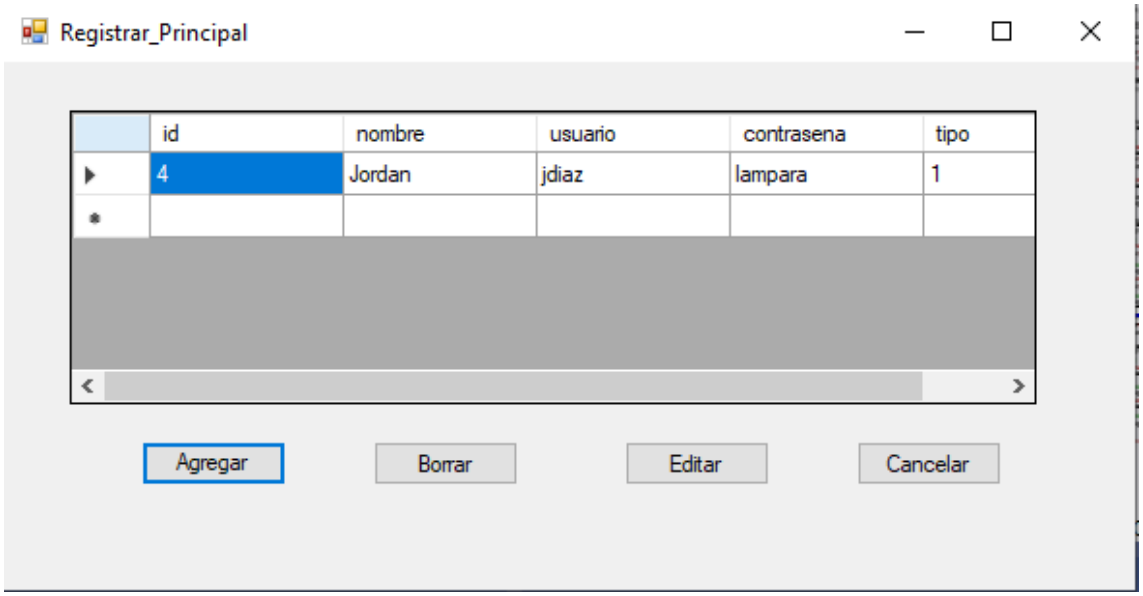

Figura 38. Formulario registrar principal.

Figura 39. Formulario agregar.

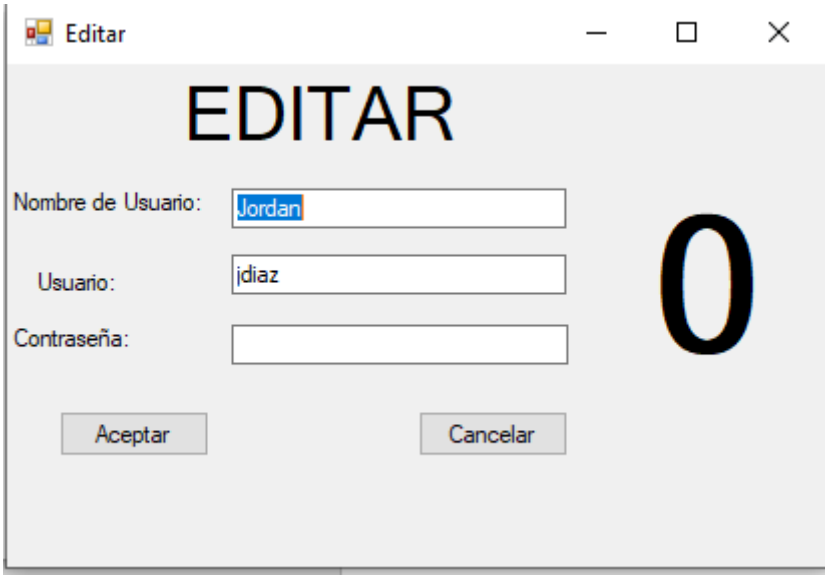

Figura 40. Formularioeditar.

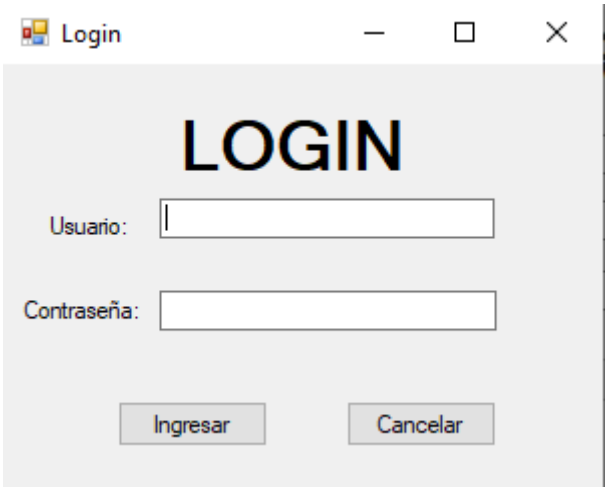

Figura 41. Formulario probar login.

C. Cambiar contraseña

Para cambiar de contraseña directamente se hace clic en el botón “Cambiar” del menú principal luego se autentica en el login para poder editar los datos en el formulario.

Figura 42. Formulario cambiar contraseña.

CAPÍTULO V
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

5.1 Análisis e interpretación de resultados

5.1.1 Resultados descriptivos e inferenciales

A) Población y muestra

Muestra

Como muestra se eligió 30 procesos de autenticación de personal de la empresa SEVEROX PERÚ S.A.C

Población

El presente trabajo se conforma con la población de todos los procesos de autenticación de personal en la empresa del sector de seguridad informática.

Unidad muestral

El proceso de autenticación de personal de la empresa SEVEROX PERÚ S.A.C.

5.1.2 Análisis e interpreta de los resultados

Resultados

En esta tabla de datos, se encuentran los resultados de los 3 indicadores establecidos para la investigación. Consta de datos de “post prueba del grupo de control” y “post prueba del grupo experimental” realizados con y sin el sistema de biometría de la dinámica del tecleo.

Tabla 24

Resultados de post prueba del grupo de control y grupo experimental

Indicador 1 Número de incidentes registrados		Indicador 2 Costo por incidentes (Soles)		Indicador 3 Exactitud de autenticación (Porcentaje)	
Grpo	Grpo exp	Grpo ctrl	Grpo exp	Grpo ctrl	Grpo exp
14	5	543	175	0.35	0.75
17	10	575	163	0.53	0.60
19	5	595	99	0.52	0.80
16	5	551	101	0.51	0.67
10	6	529	132	0.49	0.69
18	7	637	115	0.35	0.71
18	7	518	87	0.59	0.84
10	7	517	189	0.39	0.74
11	4	624	178	0.42	0.75
13	2	536	132	0.47	0.86
18	1	560	128	0.50	0.75
15	2	559	122	0.44	0.66
16	5	609	148	0.38	0.74
13	5	534	147	0.54	0.82
16	3	507	132	0.41	0.71
16	7	511	103	0.58	0.69
20	7	567	198	0.40	0.67
12	5	562	136	0.36	0.82
16	9	606	107	0.57	0.65
13	4	577	150	0.44	0.86
15	7	564	131	0.39	0.64
10	8	515	148	0.53	0.61
12	9	643	160	0.52	0.71
11	4	590	155	0.46	0.65
15	6	538	88	0.30	0.89
12	4	567	93	0.43	0.76
18	9	522	182	0.47	0.80
12	10	554	177	0.53	0.64
17	10	577	158	0.47	0.89
17	9	592	187	0.38	0.84

5.1.3 Nivel de confianza y grado de significancia

El presente trabajo tubo un nivel de confianza del 95%, a lo que por ende se podrá obtener un 5% de margen de error.

5.1.4 Prueba de normalidad

Post pruebas (Grupo de control)

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro primer indicador, en la fase de “Post prueba del Grupo de Control”. Estos datos nos enseñan que el valor “p” es mayor a 0.05, corroborando que se tiene un comportamiento normal.

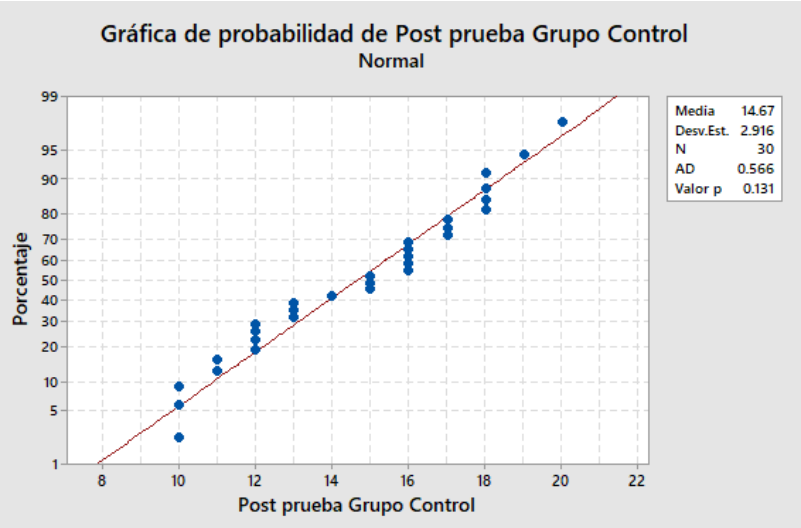

Figura 43. Prueba de normalidad indicador 1: Número de incidentes registrados - Post pruebas Grupo de control.

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro segundo indicador, en la fase de “Post prueba del Grupo de Control”. Estos datos nos enseñan que el valor “p” es mayor a 0.05, corroborando que se tiene un comportamiento normal.

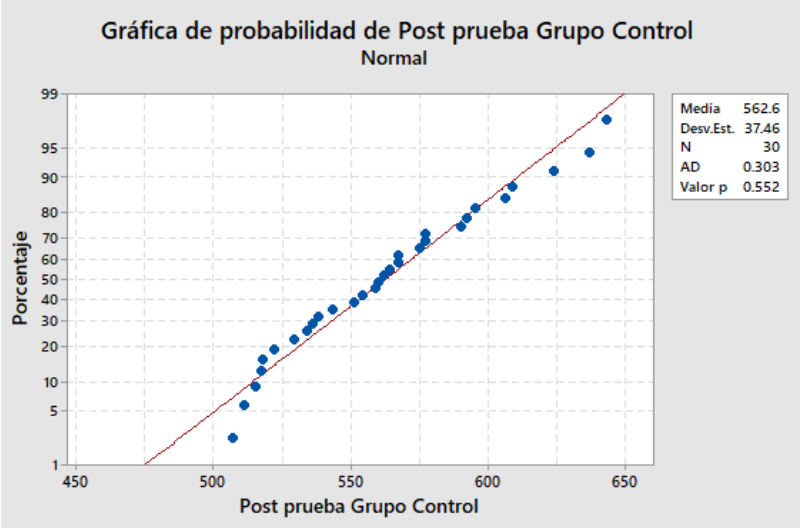

Figura 44. Prueba de normalidad Indicador 2: Costo por incidentes (Soles) – Post pruebas grupo de control.

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro tercer indicador, en la fase de "Post prueba del Grupo de Control". Estos datos nos enseñan que el valor "p" es mayor a 0.05, corroborando que se tiene un comportamiento normal.

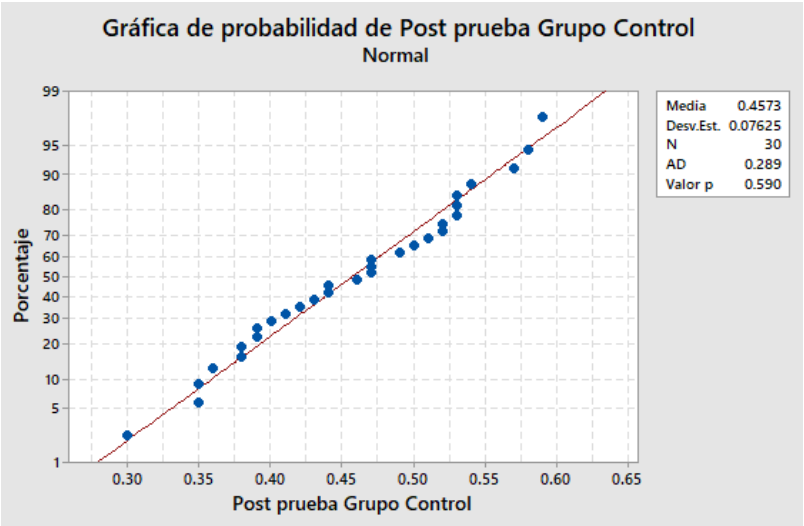

Figura 45. Prueba de normalidad indicador 3: Exactitud de autenticación (Porcentaje) – Post pruebas grupo de control.

Post Pruebas (Grupo de Experimental)

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro primer indicador, en la fase de “Post prueba del Grupo Experimental”. Estos datos nos enseñan que el valor “p” es mayor a 0.05, corroborando que se tiene un comportamiento normal.

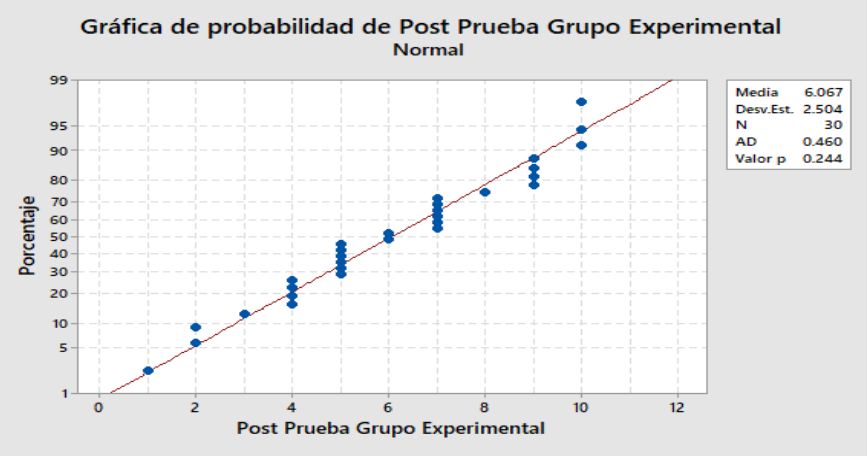

Figura 46. Prueba de normalidad Indicador 1: Número de incidentes registrados – Post pruebas grupo de experimental.

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro segundo indicador, en la fase de “Post prueba del Grupo Experimental”. Estos datos nos enseñan que el valor “p” es mayor a 0.05, corroborando que se tiene un comportamiento normal.

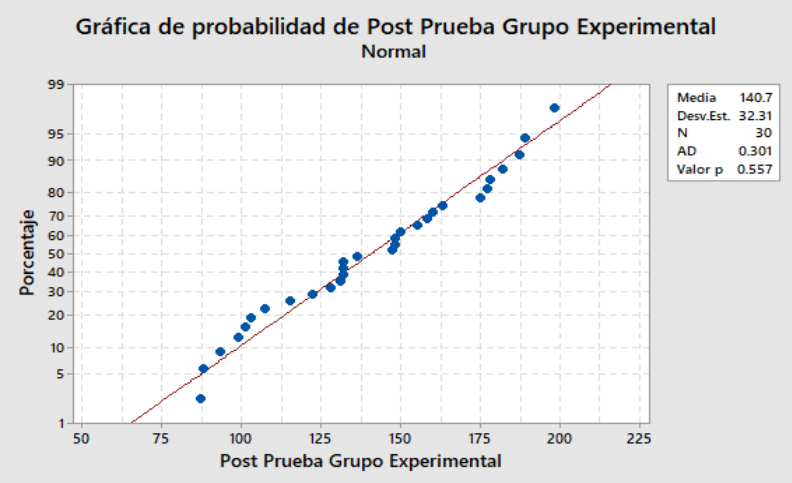

Figura 47. Prueba de normalidad indicador 2: Costo por incidentes (Soles) – Post pruebas grupo de experimental.

En la presente figura contemplamos los resultados obtenidos realizados a través de la prueba de normalidad con los datos recopilados de nuestro tercer indicador, en la fase de “Post prueba del Grupo Experimental”. Estos datos nos enseñan que el valor “p” es mayor a 0.05, corroborando que se tiene un comportamiento normal.

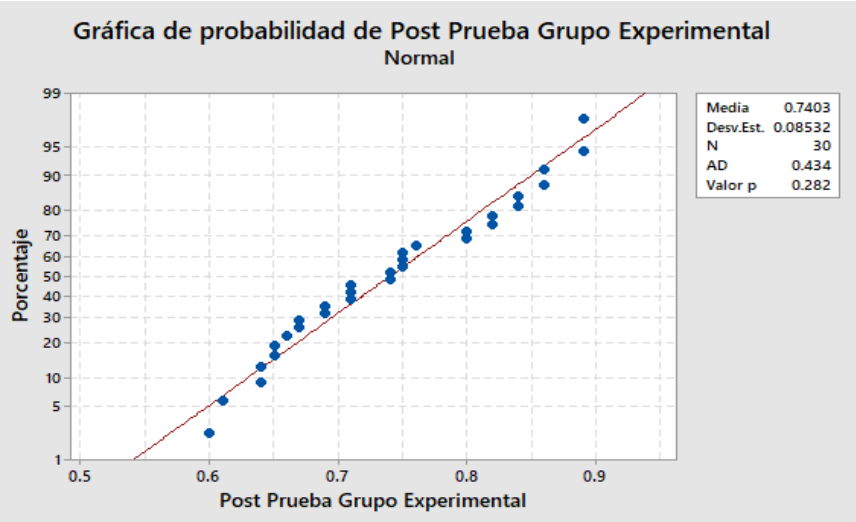

Figura 48. Prueba de normalidad Indicador 3: Exactitud de autenticación (Porcentaje) – Post pruebas grupo de experimental.

5.2 Análisis de resultados

Tabla 25

Indicador 1: Numero de Incidentes registrados.

	Post Prueba Grupo Ctrl		Post Prueba Grupo Exp	
	14	5	5	5
	17	10	10	10
	19	5	5	5
	16	5	5	5
	10	6	6	6
	18	7	7	7
	18	7	7	7
	10	7	7	7
	11	4	4	4
	13	2	2	2
	18	1	1	1
	15	2	2	2
	16	5	5	5
	13	5	5	5
	16	3	3	3
	16	7	7	7
	20	7	7	7
	12	5	5	5
	16	9	9	9
	13	4	4	4
	15	7	7	7
	10	8	8	8
	12	9	9	9
	11	4	4	4
	15	6	6	6
	12	4	4	4
	18	9	9	9
	12	10	10	10
	17	10	10	10
	17	9	9	9
Promedio	14.67		6.07	
Meta Planteada N° menor al Promedio		16	14	30
% menor al Promedio		53.33%	46.67%	100%

El **53.33%** de los **Números de incidentes registrados** en la PostPrueba del Grupo Experimental del primer indicador fueron menores a su promedio.

El **46.67%** de los **Números de incidentes registrados** en la PostPrueba del Grupo Experimental primer indicador fueron menores de la meta propuesta.

El **100%** de los **Números de incidentes registrados** en la PostPrueba del Grupo Experimental del primer indicador fueron menores a su promedio en la PostPrueba del Grupo de Control.

Tabla 26

Indicador 2: Costos por incidentes (soles)

	Post Prueba Grupo Ctrl	Post Prueba Grupo Exp		
	543	175	175	175
	575	163	163	163
	595	99	99	99
	551	101	101	101
	529	132	132	132
	637	115	115	115
	518	87	87	87
	517	189	189	189
	624	178	178	178
	536	132	132	132
	560	128	128	128
	559	122	122	122
	609	148	148	148
	534	147	147	147
	507	132	132	132
	511	103	103	103
	567	198	198	198
	562	136	136	136
	606	107	107	107
	577	150	150	150
	564	131	131	131
	515	148	148	148
	643	160	160	160
	590	155	155	155
	538	88	88	88
	567	93	93	93
	522	182	182	182
	554	177	177	177
	577	158	158	158
	592	187	187	187
Promedio	562.63		140.70	
Meta Planteada			150	
N° menor al Promedio		15	19	30
% menor al Promedio		50.00%	63.33%	100%

El **50.00%** de los **Costos por incidentes** en la PostPrueba del Grupo Experimental del segundo indicador fueron menores que su promedio.

El **63.33%** de los **Costos por incidentes** en la PostPrueba del Grupo Experimental del segundo indicador fueron menores que la meta planteada.

El **100.00%** de los **Costos por incidentes** en la PostPrueba del Grupo Experimental del segundo indicador fueron menores que su promedio en la PostPrueba del Grupo de Control.

Tabla 27

Indicador 3: Exactitud de autenticación (Porcentaje)

	Post Prueba Grupo Ctrl	Post Prueba Grupo Exp		
	0.35	0.75	0.75	0.75
	0.53	0.60	0.60	0.60
	0.52	0.80	0.80	0.80
	0.51	0.67	0.67	0.67
	0.49	0.69	0.69	0.69
	0.35	0.71	0.71	0.71
	0.59	0.84	0.84	0.84
	0.39	0.74	0.74	0.74
	0.42	0.75	0.75	0.75
	0.47	0.86	0.86	0.86
	0.50	0.75	0.75	0.75
	0.44	0.66	0.66	0.66
	0.38	0.74	0.74	0.74
	0.54	0.82	0.82	0.82
	0.41	0.71	0.71	0.71
	0.58	0.69	0.69	0.69
	0.40	0.67	0.67	0.67
	0.36	0.82	0.82	0.82
	0.57	0.65	0.65	0.65
	0.44	0.86	0.86	0.86
	0.39	0.64	0.64	0.64
	0.53	0.61	0.61	0.61
	0.52	0.71	0.71	0.71
	0.46	0.65	0.65	0.65
	0.30	0.89	0.89	0.89
	0.43	0.76	0.76	0.76
	0.47	0.80	0.80	0.80
	0.53	0.64	0.64	0.64
	0.47	0.89	0.89	0.89
	0.38	0.84	0.84	0.84
Promedio	0.46		0.74	
Meta Planteada			0.80	
N° mayor al Promedio		16	10	30
% mayor al Promedio		53.33%	33.33%	100%

El **53.33%** de la **Exactitud de autenticación** en la PostPrueba del Grupo Experimental del tercer indicador fueron mayores que su promedio.

El **33.33%** de la **Exactitud de autenticación** en la PostPrueba del Grupo Experimental del tercer indicador fueron mayores que la meta planteada.

El **100%** de la **Exactitud de autenticación** en la PostPrueba del Grupo Experimental del tercer indicador fueron mayores que su promedio en la PostPrueba del Grupo de Control.

5.3 Contrastación de la hipótesis

Tabla 28

Media de indicadores

Indicador	PostPrueba (Media X1)	PostPrueba (Media X2)
1. Número de incidentes registrados	14.67	6.07
2. Costos por incidentes	562.6	140.7
3. Exactitud de autenticación	0.45	0.74

a) Contrastación para el indicador 1: Número de incidentes registrados

Se valida como influye la implementación del Sistema de Biometría de la Dinámica del Tecleo en las cantidades de Número de incidentes registrados llevada a realizarse en la muestra. Realizaron las mismas pruebas para obtener las cantidades de datos que aplicara el grupo de control (Post prueba) y el grupo experimental (Post prueba).

Planteamiento de la hipótesis:

μ1 = Poblacional obtenida en los Número de incidentes registrados del Grupo de Control.

μ2 = Poblacional obtenida en los Número de incidentes registrados del Grupo experimental.

Ho: μ1 ≤ μ2

Ha: μ1 > μ2

Criterio de decisión:

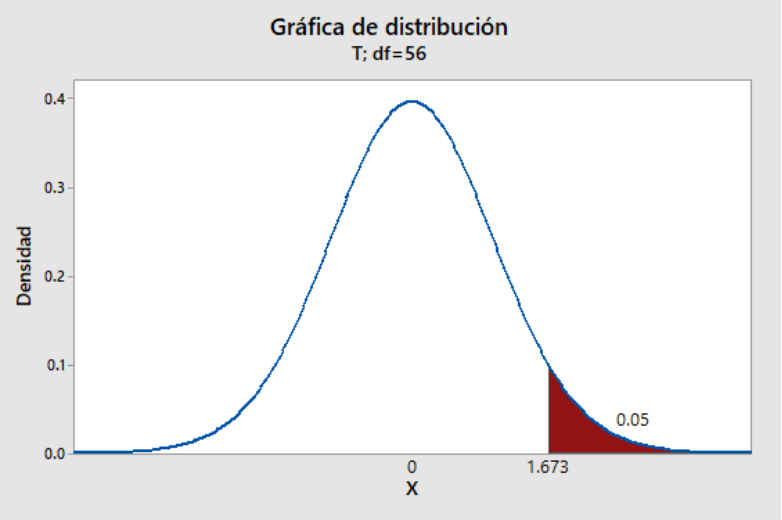

Figura 48. Grafica de distribución.

Calculo: Promedio poblacional *t* e IC de dos muestras

Método

Diferencia: μ1 - μ2

Estadística descriptiva:

Tabla 29

Estadística descriptiva indicador 1

Muestra	N	Media	Desv. Est.	Error estándar de la media
Pre – Prueba	30	14.67	2.92	0.53
Post – Prueba	30	6.07	2.50	0.46

Estimación de diferencia

Tabla 30

Estimación de diferencia indicador 1

Diferencia	Limite Superior de 95% para la diferencia
8.600	(7.194 ; 10.006)

Prueba

Hipótesis nula: H0: $\mu_1 - \mu_2 = 0$

Hipótesis alterna: H1: $\mu_1 - \mu_2 \neq 0$

Tabla 31

Prueba de Indicador 1

Valor T	GL	Valor P
12.25	56	0.000

Decisión Estadística:

Observando que el valor p = 0.000 < α = 0.05, los resultados nos dan bastante certeza como para rechazar la hipótesis nula (Ho), y la hipótesis alternativa (Ha) es cierta.

b) Contrastación para el indicador 2: Costos por incidentes

Se valida como influye la implementación del Sistema de Biometría de la Dinámica del Tecleo en las cantidades de Costos por incidentes llevada a realizarse en la muestra. Realizaron las mismas pruebas para obtener las cantidades de datos que aplicara el grupo de control (Post prueba) y el grupo experimental (Post prueba)

Planteamiento de la hipótesis:

µ1 = Poblacional obtenida en los **Costos por incidentes** del Grupo de Control.

µ2 = Poblacional obtenida en los **Costos por incidentes** del Grupo experimental.

Ho: µ1 ≤ µ2

Ha: µ1 > µ2

Criterio de decisión:

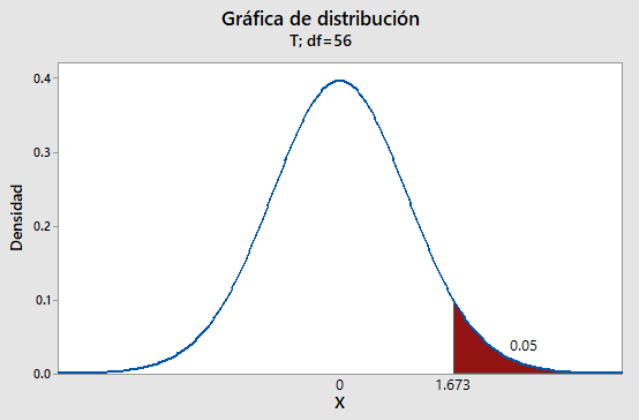

Figura 49. Grafica de distribución.

Calculo: Promedio poblacional *t* e IC de dos muestras

Método

Diferencia: µ1 - µ2

Estadística descriptiva:

Tabla 32

Estadística descriptivo indicador 2

Muestra	N	Media	Est.	Desv.	Error estándar de la media
Pre – Prueba	30	562.6		37.5	6.8
Post – Prueba	30	140.7		32.3	5.9

Estimación de diferencia

Tabla 33

Estimación de diferencia indicador 2

Diferencia	Limite Superior de 95% para la diferencia
421.93	(403.84 ;440.03)

Prueba:

Hipótesis nula: H0: $\mu_1 - \mu_2 = 0$

Hipótesis alterna: H1: $\mu_1 - \mu_2 \neq 0$

Tabla 34

Prueba del indicador 2

Valor T	GL	Valor P
46.72	56	0.000

Decisión Estadística:

Puesto que el valor p = 0.000 < α = 0.05, los resultados otorgan bastante certeza como para negar la hipótesis nula (Ho), y la hipótesis alternativa (Ha) es cierta.

c) Contrastación para el indicador 3: Exactitud de autenticación

Se valida como influye la implementación del sistema de biometría de la dinámica del tecleo en las cantidades de exactitud de autenticación llevada a realizarse en la muestra. Realizaron las mismas pruebas para obtener las cantidades de datos que aplicara el grupo de control (Post prueba) y el grupo experimental (Post prueba)

Planteamiento de la hipótesis:

- μ1 = Poblacional obtenida en la **Exactitud de autenticación** del Grupo de Control.
- μ2 = Poblacional obtenida en la **Exactitud de autenticación** del Grupo experimental.

Ho: μ1 ≤ μ2
Ha: μ1 > μ2

Criterio de decisión:

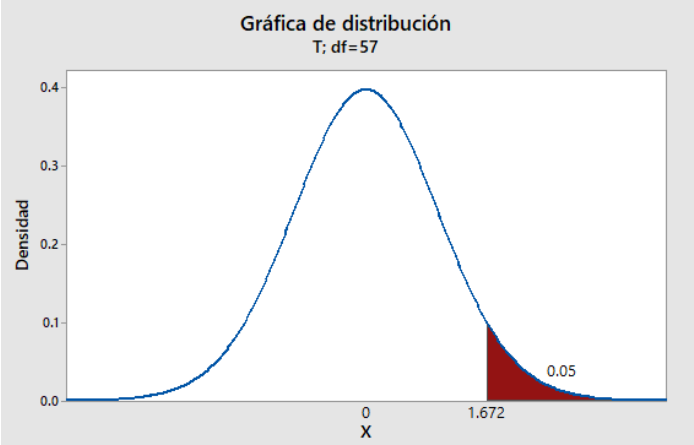

Figura 50. Grafica de distribución.

Calculo: Promedio poblacional *t* e IC de dos muestras

Método

Diferencia: µ1 - µ2

Estadística descriptiva:

Tabla 35

Estadística descriptiva indicador 3

Muestra	N	Media	Desv. Est.	Error estándar de la media
Pre – Prueba	30	0.45	0.07	0.014
Post – Prueba	30	0.74	0.08	0.016

Estimación de diferencia

Tabla 36

Estadística diferencial indicador 3

Diferencia	Limite Superior de 95% para la diferencia
-0.2830	(-0.3248 ; -0.2412)

Prueba:

Hipótesis nula: H0: $\mu_1 - \mu_2 = 0$

Hipótesis alterna: H1: $\mu_1 - \mu_2 \neq 0$

Tabla 37

Prueba del indicador 3

Valor T	GL	Valor P
-13.55	57	0.000

Decisión Estadística:

Puesto que el valor p = 0.000 < α = 0.05, los resultados otorgan bastante certeza como para negar la hipótesis nula (Ho), y la hipótesis alternativa (Ha) es cierta.

CAPÍTULO VI
DISCUSIONES, CONCLUSIÓN Y RECOMENDACIONES

6.1 Discusiones

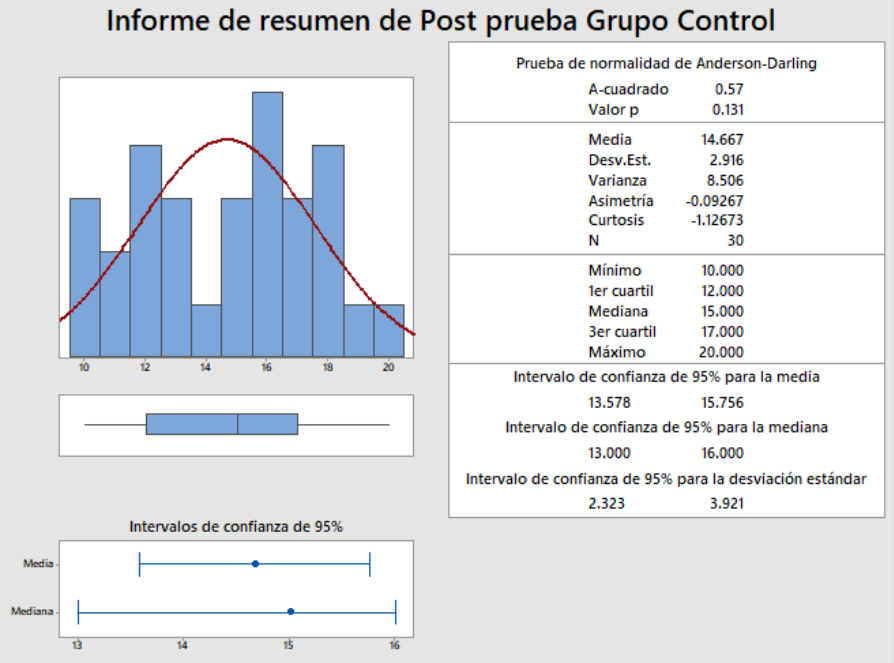

Figura 51. Informe de resumen del Indicador 1 en PostPrueba.

Grupo de control

El promedio de distancia obtenida del primer indicador “Números de incidentes registrados” del grupo de control con relacion a la media marca 2.91 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Números de incidentes registrados” del grupo de control, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 13.57 y 15.75 de puntaje.

- El primer cuartil (Q1) es igual a 12.00 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Números de incidentes registrados” es menor o igual a este valor.

- El tercer cuartil (Q3) es igual a 17.00 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Números de incidentes registrados” es menor o igual a este valor.

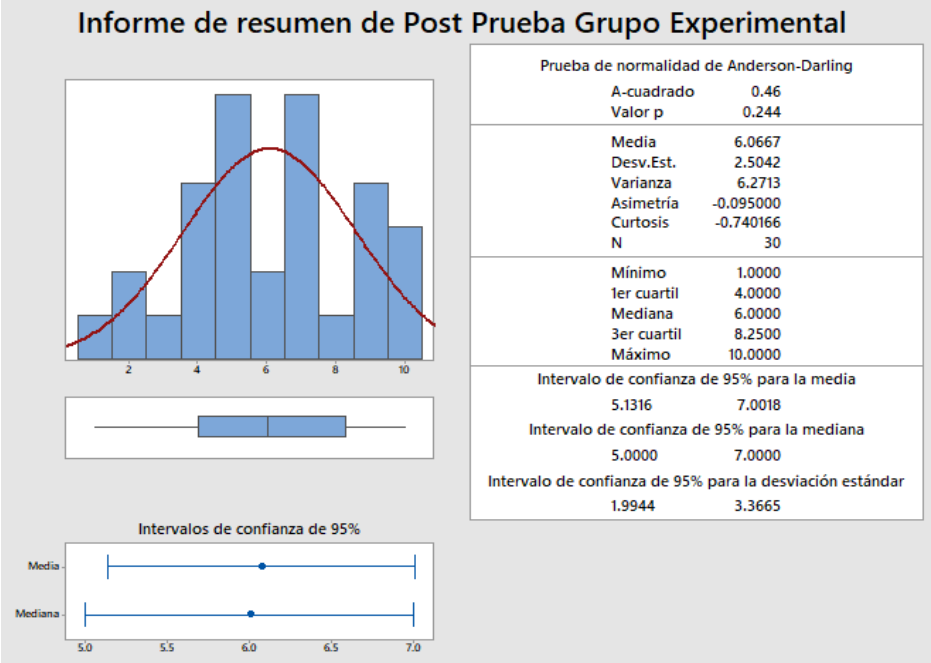

Figura 52. Informe de resumen del Indicador 1 en Postprueba Grupo Experimental.

- El promedio de distancia obtenida del primer indicador “Números de incidentes registrados” del grupo experimental con respecto a la media marca 2.50 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Números de incidentes registrados” del grupo experimental, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 5.13 y 7.00 de puntaje.

- El primer cuartil (Q1) es igual a 4.00 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Números de incidentes registrados” es menor o igual a este valor.

- El tercer cuartil (Q3) es igual a 8.25 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Números de incidentes registrados” es menor o igual a este valor.

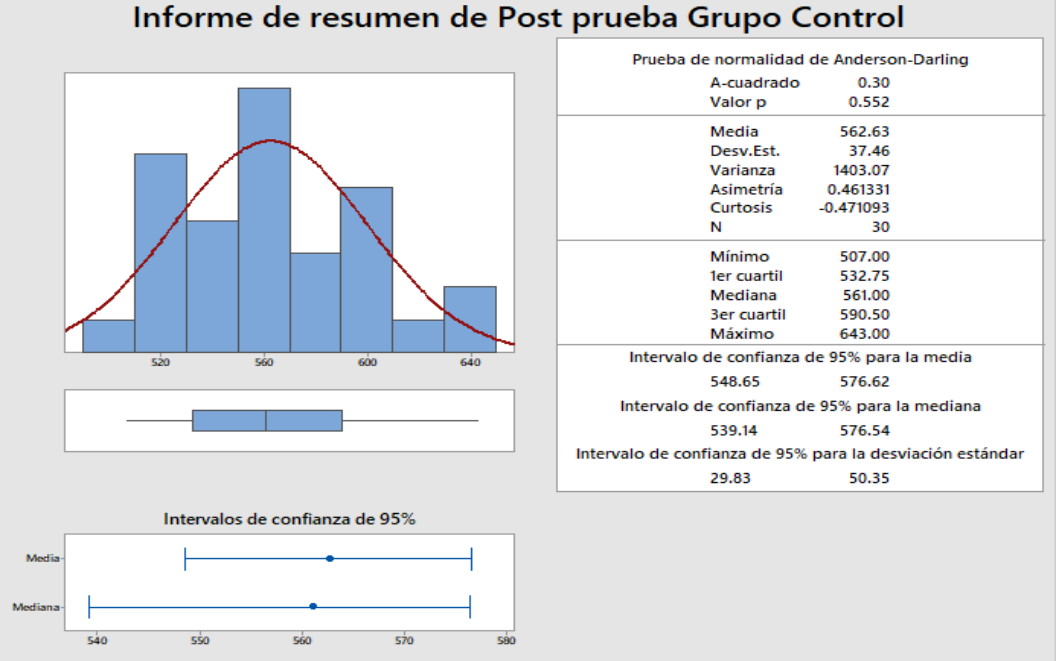

Figura 53. Informe de resumen del Indicador 2 en PostPrueba Grupo de Control.

- El promedio de distancia obtenida del segundo indicador “Costos por incidentes” del grupo de control con respecto a la media marca 37.46 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Costos por incidentes” del grupo de control, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 548.65 y 576.62 de puntaje.

- El primer cuartil (Q1) es igual a 532.75 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Costos por incidentes” es menor o igual a este valor.

- El tercer cuartil (Q3) es igual a 590.50 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Costos por incidentes” es menor o igual a este valor.

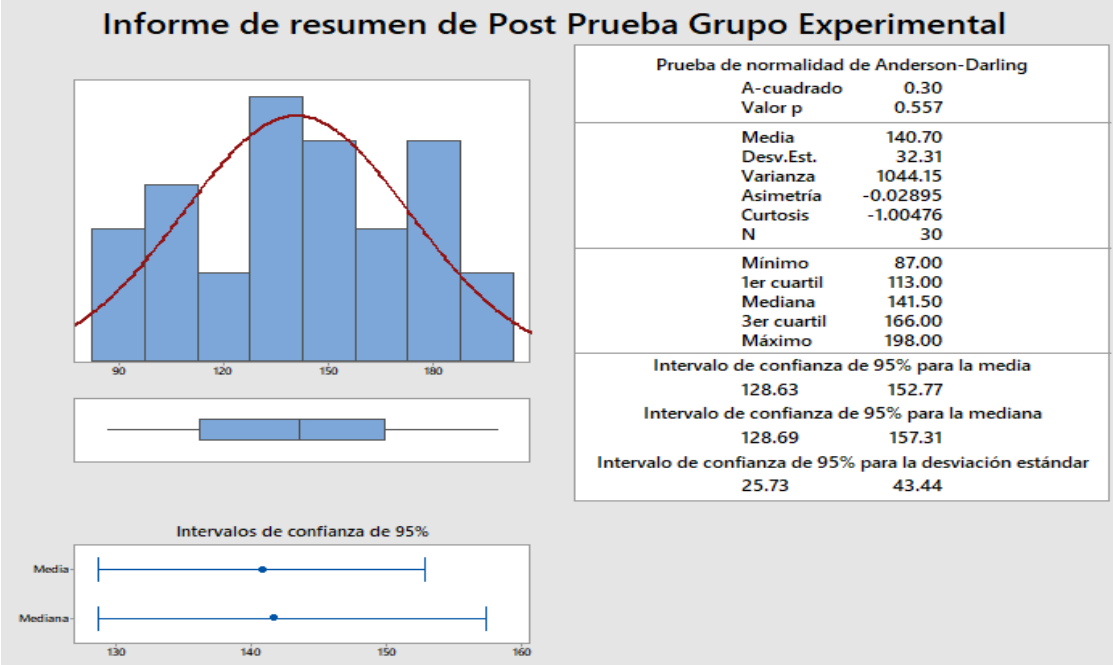

Figura 54. Informe de resumen del Indicador 2 en Postprueba Grupo Experimental.

- El promedio de distancia conseguida del segundo indicador “Costos por incidentes” del grupo experimental con relación a la media marca 32.31 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Costos por incidentes” del grupo experimental, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 128.63 y 152.77 de puntaje.

- El primer cuartil (Q1) es igual a 113.00 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Costos por incidentes” es menor o igual a este valor.

- El tercer cuartil (Q3) es igual a 166.00 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Costos por incidentes” es menor o igual a este valor.

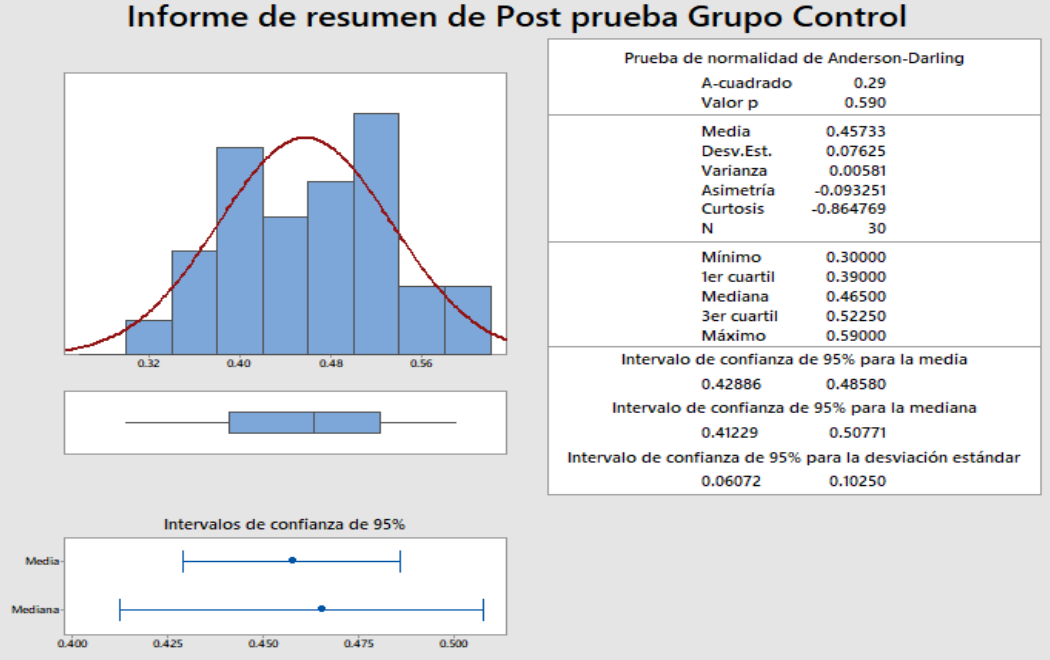

Figura 55. Informe de resumen del Indicador 3 en Postprueba Grupo de Control.

- El promedio de distancia conseguida del tercer indicador “Exactitud de autenticación” del grupo de control con relación a la media marca 0.07 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Exactitud de autenticación” del grupo de control, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 0.42 y 0.48 de puntaje.

- El primer cuartil (Q1) es igual a 0.39 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Exactitud de autenticación” es mayor o igual a este valor.

- El tercer cuartil (Q3) es igual a 0.52 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Exactitud de autenticación” es mayor o igual a este valor.

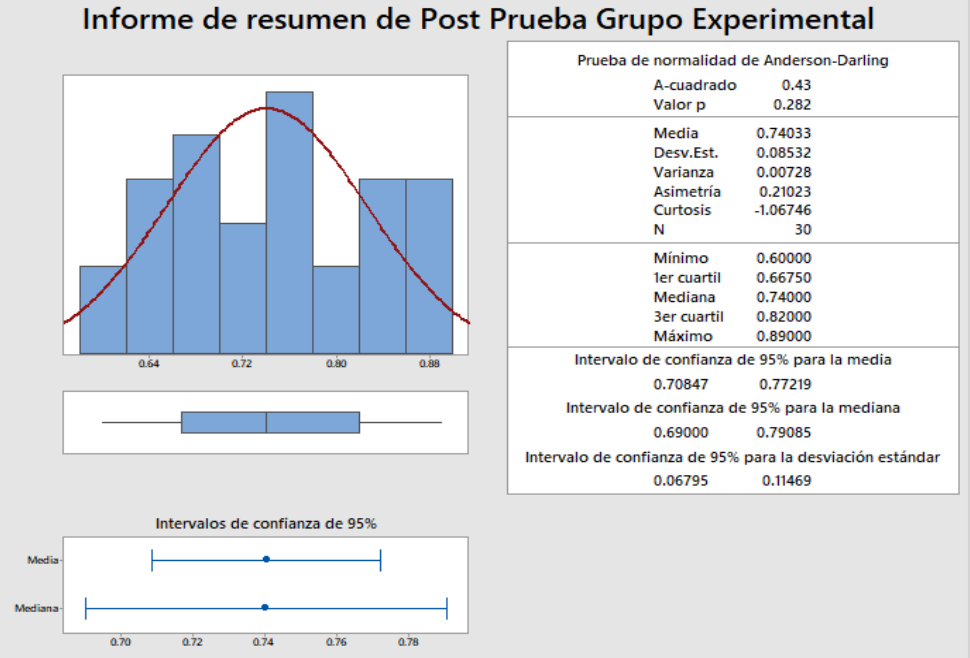

Figura 56. Informe de resumen del Indicador 3 en Postprueba Grupo Experimental.

- El promedio de distancia conseguida del tercer indicador “Exactitud de autenticación” del grupo experimental con relacionV a la media marca 0.08 puntos.

- Alrededor del 95% de las cantidades obtenidas en el indicador de “Exactitud de autenticación” del grupo experimental, se encuentran dentro de 2 desviaciones estándar de la media, las cuales están entre 0.70 y 0.77 de puntaje.

- El primer cuartil (Q1) es igual a 0.66 puntos, este resultado nos indica que el 25% de las cantidades que se consiguieron en el indicador “Exactitud de autenticación” es mayor o igual a este valor.

- El tercer cuartil (Q3) es igual a 0.82 puntos, este resultado nos indica que el 75% de las cantidades conseguidas en el indicador “Exactitud de autenticación” es mayor o igual a este valor.

6.2 Conclusiones

- Se comprueba que la creación y la implementación de un sistema de biometría de la dinámica del tecleo, apresuro y modernizo el proceso de autenticación del Personal de la empresa SEVEROX PERÚ S.A.C.

- Se consigue apreciar que, la implementación de un sistema de biometría de la dinámica del tecleo, disminuyo un 70.00% el número de incidentes registrados.

- Se consigue observar que, la implementación de un sistema de biometría de la dinámica del tecleo redujo un 78.46% el costo por incidentes.

- Se consigue apreciar que, la implementación de un sistema de biometría de la dinámica del tecleo, incremento un 83.33% exactitud de autenticación después de la implementación.

6.3 Recomendaciones

- Se recomienda la creación de un manual de usuario para el sistema, en caso de la llegada de nuevo personal o administrativo que no llegase a entender el sistema.

- Se informa que, si adjuntaran nuevos requerimientos funcionales que influyan en el proceso de la autenticación del personal, realizar una documentación con las nuevas funcionalidades a solicitar para la actualización del sistema correspondiente.

- Se suscita que, para posibles futuras de fallas del sistema acudir con el administrador o tener un plan de contingencia. En caso contrario se pondrá en suspensión el sistema hasta repararlo.

- Se informa que, habrá un plan de prueba que se realizará en cada actualización requerida.

REFERENCIAS

Acosta, F. D. y Torres, A. L. (2008). Sistema de Protección de Datos usando Dinámica de Tecleo. *Universidad Juárez Autónoma de Tabasco.* Recuperado de https://cupdf.com/document/biometria-de-tecleo.html

Adams, W. R. (2017). High-accuracy detection of early Parkinson's Diseaseusing multiple characteristics of finger movement while typing. *PloSone*, *12*(11). Recuperado de https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0188226

Arribas, E. & Puente, L. A. (2009). *Back-End for A Biometric Extended Experiment Platform (Beep)* (Tesis de pregrado). Recuperado de https://ravelpruebas.uc3m.es/handle/10016/6625

García, C. y García, I. (2007). *Sistemas de Autenticación Biométricos.* Sabia. Recuperado de http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/Sistemas%20de%20autenticacion%20biometricos.pdf

Iglesias, G. (2007). *Sistema De Autenticacion Para Dispositivos Moviles Basado En Biometrıa De Comportamiento De Tecleo* (Tesis de pregrado). Recuperado de http://delta.cs.cinvestav.mx/~francisco/tesisIglesias.pdf

Marquez, P. Y. (2018). *Patrones De Digitacion Para Evitar La Suplantacion De Identidad En El Sistema Transaccional De Una Universidad Privada* (Tesis de pregrado). Recuperado de http://repositorio.uncp.edu.pe/handle/20.500.12894/5111

Morales, A., Fierrez, J., Vera, R., y Ortega, J. (2015). Autenticación Web de Estudiantes Mediante Reconocimiento Biométrico. En *III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad*. Recuperado de http://atvs.ii.uam.es/atvs/files/2015_CINAIC_Keystroke_Aythami.pdf

Nieto, S., Gómez, Y. A., López, A. y Rojas, C. A. (2015). Captura de datos para análisis de la dinámica del tecleo de números para sistema operativo Android. *Research in Computing Science*, *92*(2015), 147-156.

Obaidat, M. S. y B. Sadoun, B. (1997). Verification of computer users using keys-troke dynamics. En *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 27*(2), 261-269. Recuperado de https://ieeexplore.ieee.org/document/558812

Ortega, J., Fernández, F. A., y Coomonte, R. (2008). Biometria y Seguridad. *Universidad Politécnica de Madrid*. Recuperado de https://www.researchgate.net/publication/280722075_Seguridad_Biometrica

Pecharromán, S. (2007). *Reconocimiento Deescritor Independientede Texto Basado Encaracterísticas Detextura* (Tesis de pregrado). Recuperado de http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20071031SusanaPecharroman.pdf

Restrepo, L. (2007). De Pearson a Spearman. *Revista Colombiana de Ciencias Pecuarias*, *20*(2), 183-192. Recuperado de https://revistas.udea.edu.co/index.php/rccp/article/view/324135

Rivilla, F. (2017). *Autenticación y verificación de usuarios mediante dinámica del tecleo* (Tesis de pregrado). Recuperado de https://eprints.ucm.es/id/eprint/44424/

Ruíz, M., Rodriguez, J. C. y Olivares, J. C. (2009). Una mirada a la biometria*. Avances en Sistemas e Informatica*, *6*(2), 29-38. Recuperado de https://revistas.unal.edu.co/index.php/avances/article/view/20295/21415

Ugarte, S. E. (2018). *Método De Autenticación Basado En La Dinámica De Tecleo* (Tesis de pregrado). Recuperado de https://repositorio.umsa.bo/handle/123456789/17483?show=full

ANEXOS

SEVEROX PERU
PASIÓN E INGENIO

AUTORIZACION DEL DESARROLLO DE LA INVESTIGACION

Institución: SEVEROX PERU SAC
Investigador: Jordan Alexander Diaz Diaz

La empresa SEVEROX PERU SAC con RUC 20605834788 en representación de su Gerente General el Ing. Lennon Rojas Sanz con DNI 73249257 autoriza al Bachiller Jordan Alexander Diaz Diaz identificado con DNI 45640657 para el uso de la información he instalaciones de la empresa para su investigación titulada "**SISTEMA BASADO EN BIOMETRIA DE LA DINAMICA DE TECLEO, APLICANDO RUP, PARA LA AUTENTICACIÓN DE PERSONAL EN LA EMPRESA SEVEROX PERU S.A.C**" desde las fechas 01/01/2021 al 31/03/2021.

Atentamente.

ING. LENNON POUL ROJAS SANZ
GERENTE GENERAL
SEVEROX PERU S.A.C

AV. MIGUEL GRAU 578 ACEQUIA - ALTA CAYMA
+51924829083
hola@severox.com
www.severox.com

	Rioja Trabajo del estudiante	
10	Submitted to Universidad Autonoma del Peru Trabajo del estudiante	<1%
11	repositorio.eiposgrado.edu.pe Fuente de Internet	<1%
12	repositorio.unp.edu.pe Fuente de Internet	<1%
13	Submitted to Universidad Nacional del Centro del Peru Trabajo del estudiante	<1%
14	cip.org.pe Fuente de Internet	<1%
15	oa.upm.es Fuente de Internet	<1%
16	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	<1%
17	repositorio.uigv.edu.pe Fuente de Internet	<1%
18	repositorio.unfv.edu.pe Fuente de Internet	<1%
19	vsip.info Fuente de Internet	<1%

TESIS JORDAN D

INFORME DE ORIGINALIDAD

13%	10%	0%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	4%
2	repositorio.uncp.edu.pe Fuente de Internet	2%
3	www.scribd.com Fuente de Internet	1%
4	repositorio.autonoma.edu.pe Fuente de Internet	1%
5	docplayer.es Fuente de Internet	1%
6	issuu.com Fuente de Internet	1%
7	repositorio.ucv.edu.pe Fuente de Internet	1%
8	www.slideshare.net Fuente de Internet	<1%
9	Submitted to Universidad Internacional de la	<1%

20	MARÍA ISABEL MUNDI SANCHO. "MÉTODOS Y MODELOS PARA LA PLANIFICACIÓN DE OPERACIONES EN CADENAS DE SUMINISTRO CARACTERIZADAS POR LA FALTA DE HOMOGENEIDAD EN EL PRODUCTO. APLICACIÓN AL SECTOR CERÁMICO", Universitat Politecnica de Valencia, 2016 Publicación	<1%
21	dspace.sti.ufcg.edu.br:8080 Fuente de Internet	<1%
22	repositorio.une.edu.pe Fuente de Internet	<1%
23	biblioteca.icap.ac.cr Fuente de Internet	<1%
24	dx.doi.org Fuente de Internet	<1%
25	futur.upc.edu Fuente de Internet	<1%
26	www.northwestgeorgianews.com Fuente de Internet	<1%
27	www.researchgate.net Fuente de Internet	<1%