ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DISEÑO DE UNA INTERFAZ DE ACCESO, UTILIZANDO UN DISPOSITIVO BIOMÉTRICO LECTOR DEL IRIS DEL OJO, QUE PERMITA MEJORAR LA SEGURIDAD Y LA CONFIDENCIALIDAD EN SISTEMAS INFORMÁTICOS.

JOSÉ ANDRÉS PEÑAHERRERA OBREGÓN

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Mayo - 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **DISEÑO DE UNA INTERFAZ DE ACCESO, UTILIZANDO UN DISPOSITIVO BIOMÉTRICO LECTOR DEL IRIS DEL OJO, QUE PERMITA MEJORAR LA SEGURIDAD Y LA CONFIDENCIALIDAD EN SISTEMAS INFORMÁTICOS,** de responsabilidad del Ing. José Andrés Peñaherrera Obregón, ha sido minuciosamente revisado por los miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

Tribunal:

ING. JULIO FRANCISCO GUALLO PACA; Mag.
PRESIDENTE

JULIO FRANCISCO GUALLO PACA
Firmado digitalmente por JULIO FRANCISCO GUALLO PACA
Fecha: 2021.05.26 11:11:54 -05'00'

FIRMA

ING. DIEGO FRANCISCO CAISAGUANO VILLA. Mag.
DIRECTOR

DIEGO FRANCISCO CAISAGUANO VILLA
Firmado digitalmente por DIEGO FRANCISCO CAISAGUANO VILLA
Nombre de reconocimiento (DN): c=EC, serialNumber=0603060666, sn=CAISAGUANO VILLA, cn=DIEGO FRANCISCO CAISAGUANO VILLA, 1.3.6.1.4.1.37442.1.4=0603060666, givenName=DIEGO FRANCISCO, email=dfrancis@hotmail.com, st=CHIMBORAZO, l=RIOBAMBA, ou=Certificado de Clase 2 de Persona Física EC (FIRMA)
Fecha: 2021.05.26 01:00:18 -05'00'

FIRMA

ING. CARLOS ROBERTO VILLA PADILLA Mag.
MIEMBRO

FIRMA

ING. BRAULIO ADRIÁN CAISAGUANO VILLA Mag.
MIEMBRO

FIRMA

mayo,2020

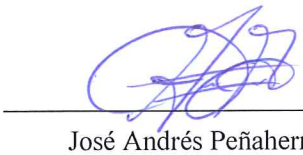
DERECHOS INTELECTUALES

Yo, José Andrés Peñaherrera Obregón, con cédula de identidad 0603961970 declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

José Andrés Peñaherrera Obregón
N° de cédula 0603961970

DECLARACIÓN DE AUTENTICIDAD

Yo, José Andrés Peñaherrera Obregón, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.
Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.



José Andrés Peñaherrera Obregón
Nº de cédula 0603961970

DEDICATORIA

Esta tesis va dedicada a mi familia que me ha brindado aliento positivo para que pueda seguir adelante en mis estudios y triunfe en mi propósito de superación, para poderme desenvolver como un buen profesional al servicio de mi patria.

José Andrés Peñaherrera Obregón

AGRADECIMIENTO

Agradezco a Dios por concederme la vida, darme capacidad y entendimiento para poder cumplir con mi meta deseada, a mis padres y hermano que me han apoyado en el transcurso de mis estudios con sus palabras de aliento y respaldo, a mis maestros catedráticos quienes, con mística profesional me han entregado sus conocimientos, en especial a mi tutor Ing. Diego Caisaguano quien con su vocación y profesionalismo me ha orientado para realizar esta tesis.

José Andrés Peñaherrera Obregón

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

Se propuso un modelo biométrico eficaz, para mejorar la seguridad y la confidencialidad en sistemas informáticos mediante el dispositivo biométrico EF-45, el mismo que interviene en el logueo del usuario receptando las señales del iris de los ojos y posteriormente almacenando la información en una base de datos conectada a cualquier sistema informático que requiera autentificación para salvaguardar la información y la seguridad de sus usuarios. El algoritmo utilizado para la elaboración de la interfaz de acceso a los sistemas informáticos, se basó en la configuración y conexión del software en la red por conexión ethernet, a través de direcciones IP en el segmento de red 192.168.1.1 con lo cual el dispositivo biométrico y el computador intercambian la información necesaria para iniciar la pre visualización, lectura, captura y comparación de datos, obtenidos de las características biométricas del usuario, por medio del dispositivo biométrico EF-45, basado en la tecnología más actual referente a biometría de iris, el cual recepta todos los datos necesarios del usuario, con la calidad óptima, normas de calidad basadas en estándares internacionales, características necesarias del iris del ojo y empleando la interfaz gráfica de acceso diseñada, la cual interactúa con su base de datos traduciendo cada dato obtenido para adecuarlo al modelo propuesto con procesamiento rápido y eficaz en la verificación y la coincidencia de datos obtenidos, que permiten el acceso al sistema informático en el que se encuentre instalado este modelo de control de acceso biométrico. Según el estudio realizado se puede concluir que el iris del ojo es una de las características biométricas más segura y viable que se puede obtener del ser humano en comparación con las demás características como el ADN y la retina que a pesar de ser características excelentes, son más complejas de procesar e implementar debido a costos y accesibilidad.

Palabras Clave: < SISTEMAS INFORMÁTICOS >, <BIOMETRÍA>, < DISPOSITIVO BIOMÉTRICO EF-45 >, <VULNERABILIDADES>, <CONFIDENCIALIDAD>, <APLICACIONES WEB>, <IRIS DEL OJO>

SUMARY

An effective biometric model was proposed to improve security and confidentiality in computer systems using the biometric device EF-45, the same one that intervenes in the user login by receiving the signals from the iris of the eyes and subsequently storing the information in a database. data connected to any computer system that requires authentication to safeguard the information and security of its users. The algorithm used for the elaboration of the access interface to the computer systems was based on the configuration and connection of the software in the network by ethernet connection, through IP addresses in the network segment 192.168.1.1 with which the device biometric and the computer exchange the necessary information to start the preview, reading, capture and comparison of data, obtained from the biometric characteristics of the user, by means of the EF-45 biometric device, based on the most current technology regarding iris biometry, which receives all the necessary data from the user, with optimal quality, quality standards based on international standards, necessary characteristics of the iris of the eye and using the designed graphic access interface, which interacts with its database, translating each data obtained to adapt it to the proposed model with fast and efficient processing in the verification and matching of data obtained, which allow access to the computer system in which this biometric access control model is installed. According to the study carried out, it can be concluded that the iris of the eye is one of the safest and most viable biometric characteristics that can be obtained from the human being compared to other characteristics such as DNA and the retina that, despite being excellent characteristics, are more complex to process and implement due to cost and accessibility.

Keywords: <COMPUTER SYSTEMS>, <BIOMETRY>, <BIOMETRIC DEVICE EF-45>, <VULNERABILITIES>, <CONFIDENTIALITY>, <WEB APPLICATIONS>, <EYE IRIS>

CAPÍTULO I

1 INTRODUCCIÓN

La presente investigación se refiere a la utilización de un dispositivo biométrico EF-45 que es capaz de capturar las señales de los dos iris de los ojos y la contextura facial del rostro de una persona para posteriormente compararla mediante una interfaz gráfica con datos almacenados en un base de datos y sirva como autenticación para el ingreso a cualquier sistema informático en el que se instale este modelo.

En la era de la tecnología se ha visto afectada de una manera muy significativa la vulnerabilidad a la confidencialidad en los sistemas ya sea por ataques informáticos, por descuido de la propia persona que entrega las contraseñas a dueños de centros de internet con el fin de recibir ayuda, sin entender que estas personas tranquilamente podrían acceder a sus datos, cuentas bancarias etc., y utilizar esa información para beneficio personal.

El interés para realizar esta investigación es ofrecer alternativas diferentes mucho más seguras a las comunes de acceso a las aplicaciones, que se utiliza para cualquier tipo de trámite que se realiza hoy en día. Se realizará una encuesta estructurada al inicio de la investigación a varios profesionales que se encuentren administrando sistemas informáticos con el fin de medir el nivel de seguridad con el que cuentan en este momento y después proponer el sistema biométrico y comprobar si aumenta o no el nivel de seguridad a la confidencialidad.

1.1 Planteamiento del problema

1.1.1 Situación problemática

A nivel mundial no es nada nuevo escuchar sobre los ciberataques, pero tendríamos que preguntarnos cuales son las instituciones favoritas por los ciberdelincuentes para realizar un ataque informático y además que repercusiones atrae a las personas que en si son la parte más importante dentro de la sociedad. Absolutamente todas las personas en este planeta, una de sus principales actividades diarias es el de obtener un beneficio económico en la mayoría de los casos para subsistir y en otros para seguir acumulando grandes fortunas. Si una persona no tiene dinero se ve limitada a progresar en todos los ámbitos de la vida, no es muy complicado entender que las instituciones financieras son las favoritas por los atracadores informáticos, para realizar robos económicos e información sensible tanto de la entidad bancaria como de los clientes, por supuesto

que no se puede dejar de lado las demás instituciones ya sea educativas, gubernamentales, militares, redes sociales, telefónicas y más. Está claro entonces que existe un problema generalizado a ser tomado en cuenta con mucha responsabilidad en el ámbito que a nosotros nos compete como es la seguridad de la información. El lector de iris de ojos y rostro EF-45 trata de ser una alternativa tecnológica biométrica a la confidencialidad de los sistemas informáticos y de esta manera reducir el problema de la suplantación de identidad. Solo para citar un ejemplo y dejar claro al problema grave al que se enfrenta todo el planeta mencionamos el reporte de la agencia efe tomada por el diario el comercio del 28 de marzo del 2018 en el que se publica el caso del ucraniano Denis K. considerado como un genio informático quien en un solo año consiguió desvalijar 1000 millones de dólares de entidades bancarias europeas infectando un virus informático que se propagaba a través de los correos electrónicos apropiándose del control del sistema del banco.

1.2 Formulación del problema

¿Se puede aumentar la confidencialidad a los sistemas informáticos mediante la implementación de una interfaz de acceso biométrico como es el iris del ojo?

1.3 Justificación de la investigación

1.3.1 Justificación teórica

La investigación sobre el uso de tecnología biométrica para autenticación en los sistemas informáticos se justifica plenamente aquí presentamos algunas ventajas:

- Reduce el fraude, mientras que los enfoques predominantes como nombre de usuario / contraseña / PIN pueden adquirirse ilícitamente por observación directa y luego repudiados, proporciona una autenticación de usuario más precisa y confiable;
- Recordar las contraseñas y los PIN ya no son necesarios, y
- La suplantación de identidad es un problema menor. (N.K. Ratha, 2001)

En una encuesta realizada se pudo identificar que el 92 por ciento de los consumidores del Reino Unido y el 69 por ciento de los consumidores estadounidenses prefieren que los bancos, las compañías de tarjetas de crédito, los proveedores de atención médica y las organizaciones gubernamentales adopten tecnologías biométricas, en comparación con otras medidas de protección, como lectores de tarjetas inteligentes, seguridad tokens o contraseñas / PIN para verificar con seguridad sus identidades.

Este número significa un número creciente de usuarios que reconocen la necesidad de métodos de autenticación más seguros (Cohn, 2007).

Un estudio reciente de Kaspersky Lab, en base a 320 profesionales encuestados de todo el mundo para investigar la prevalencia y el impacto de los ciberataques en sistemas de control de seguridad industrial, concluyó que más de la mitad (54%) de los encuestados que habían experimentado un ataque cibernético, en los 12 meses previos al estudio notó daños a sus productos o servicios. Además, el 40% detectó una pérdida de confianza del cliente y el 22% experimentó una pérdida de contratos u oportunidades de negocios. Estas estadísticas demuestran la importancia de encontrar nuevas formas de aumentar la seguridad en el control de acceso.

Mientras que las empresas deben implementar sistemas como firewalls para ayudar a prevenir ciberataques desde ubicaciones remotas, también necesidad de sistemas de seguridad física, especialmente interfaces hombre-máquina (HMI) y consolas de operador, de ciber delincuentes en el sitio. (Pricop, 2019)

La tecnología de seguimiento ocular ha mejorado mucho en los últimos años, y los sensores de iris, se han convertido en dispositivos baratos y portátiles que se pueden usar fácilmente en diferentes escenarios.

1.4 Objetivos

1.4.1 Objetivo General

Diseño de una interfaz de acceso, utilizando un dispositivo biométrico lector del iris del ojo, que permita mejorar la seguridad y la confidencialidad en sistemas informáticos.

1.4.2 Objetivos Específicos

- Comparar las principales características de seguridad y rendimiento de las tecnologías biométricas.
- Estudiar la tecnología biométrica como es el iris del ojo.
- Diseñar e Implementar un acceso de logueo para los sistemas informáticos utilizando el lector biométrico EF-45.
- Validar el módulo de acceso biométrico en un sistema informático.

1.5 Hipótesis

El diseño e implementación de una interfaz de acceso mediante un dispositivo biométrico del iris del ojo si mejorará la confidencialidad en los sistemas informáticos.

1.6 IDENTIFICACIÓN DE VARIABLES

Variable Independiente: Interfaz de acceso biométrico utilizando un lector biométrico del iris del ojo.

Variable dependiente: Incrementar la seguridad a la confidencialidad de los sistemas informáticos.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes del problema

Los sistemas biométricos están compuestos por un hardware y un software; el primero captura la particularidad concreta del individuo y el segundo interpreta la información y determina su aceptabilidad o rechazo, todo en función de los datos que han sido almacenados según un registro inicial de la característica biométrica que mida el dispositivo (Chiavenato, 2018).

En los primeros se incluye el análisis de dinámica de la firma y el golpe en el teclado; los segundos se encuentra la huella dactilar, la geometría de la mano y el dedo, la termografía facial y la exploración del iris o la retina. El reconocimiento de la voz es un parámetro biométrico basado en los dos análisis, el fisiológico que determina la zona vocal y el de comportamiento del lenguaje y las palabras usadas. Es decir, aquellos dispositivos que se basen en el comportamiento necesitan de la cooperación del usuario, mientras se pueda identificar fisiológicamente a cualquiera sin su cooperación e incluso sin su conocimiento, como por ejemplo la imagen captada por una videocámara (Chiavenato, 2018).

El desarrollo de un prototipo de unidad de iris comienza en el año 1993. La Agencia Nuclear de defensa empezó a trabajar con IriScan, Inc. para poner a prueba una unidad de reconocimiento de iris de prototipo (Hernàndez Reyes, 2016).

El primer algoritmo de reconocimiento del iris patentado se inserta en 1994 por el Dr. John Daugman para su reconocimiento de iris algoritmos. Propiedad de Iridian Technologies, el sucesor de IriScan, Inc., esta patente es la piedra angular más comercial en productos de reconocimiento de iris hasta hoy (Hernàndez Reyes, 2016).

El proyecto conjunto entre la Agencia de defensa Nuclear y Iriscan dio lugar a la disponibilidad del primer producto comercial de iris y este vuelva a estar disponible en 1995. (Hernàndez Reyes, 2016)

Según Cantoni, 2017 se presenta una encuesta de métodos biométricos basados en el seguimiento ocular. Algunas técnicas biométricas se han subdividido en cinco grupos, según el principio de interacción utilizado. (Sistemas tipo ATM) y sobre el tipo de datos oculares que se tienen en

cuenta (fijación y análisis scanpath, velocidad de ojo / mirada, tamaño de la pupila, características oculomotoras y orientación de la cabeza).

Se explica que potencialmente, el campo biométrico puede beneficiarse enormemente de este nuevo tipo de enfoques de verificación y autenticación, especialmente cuando se utilizan como complemento de los métodos de autenticación habituales (como los basados en contraseñas y PIN) (Virginio Cantoni, 2017).

Se propone un algoritmo basado en la fusión de transformación 2DMWT y radón para la extracción de características del iris para autenticación de persona. El sistema utiliza una distancia euclidiana como clasificador para obtener la distancia mínima entre dos iris como imágenes de la misma persona. El algoritmo fue probado en base de datos KVKRG_iris en la que se capturan imágenes de iris con la ayuda de I SCAN 2 Dual Iris Capture Scanner.

El trabajo propuesto, logró la precisión general de 86.052%. Los futuros trabajos se centrarán en reducir el tamaño del vector de características y el tiempo de ejecución, esto para aumentar la precisión en conjunto de datos. (M. R. Rajput, 2018)

2.2 Bases Teóricas

2.2.1 Sistemas Biométricos

Son métodos de reconocimiento de individuos basado en las características fisiológicas o su comportamiento. Este se trata de un proceso similar al que normalmente realiza una persona reconociendo e identificando a sus congéneres por su físico, su voz, su forma de andar, etc. (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

La tecnología nos ha permitido automatizar y perfeccionar los procesos de reconocimiento biométrico, de forma que tienen infinidad de aplicaciones y finalidades, especialmente aquellas relacionadas con la seguridad (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.2 Características biométricas

Propiedades de las características biométricas empleadas:

a) Universalidad: todos los sujetos las tienen
b) Singularidad o univocidad: distinguen a cada persona
c) Permanencia en el tiempo y en distintas condiciones ambientales

d) Medibles de forma cuantitativa

Las tecnologías para medir estas características proporcionan:

a) Rendimiento: nivel de exactitud
b) Aceptación: por parte del usuario
c) Resistencia al fraude y usurpación

Generalmente para poder ser usado los sujetos deben registrar su identidad en el sistema, por medio de, la captura de varios parámetros biométricos. Este es el denominado proceso de registro, que se compone de tres fases distintas: (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

Figura 1-2 Proceso de registro

Fuente: (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016)

Captura de los parámetros biométricos.

Procesamiento: estableciendo una plantilla con las peculiaridades personales de los parámetros capturados.

Inscripción de la plantilla: procesada guardándola en un medio de almacenamiento apropiado. Cuando la inscripción está completa, el sistema puede autenticar a las individuos mediante el uso de la plantilla (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.3 Modos de Operación

A través del proceso de autenticación se captura una muestra biométrica del sujeto que será comparada con las plantillas ya registradas, la cual, puede realizarse de dos formas diferentes:

2.2.3.1 Identificación

Esta trata de la comparación según la muestra recogida del individuo frente a una base de datos de características biométricas registradas previamente. No se precisa de identificación inicial del sujeto, ya que, el único dato recogido en el momento de uso es la muestra biométrica, sin un nombre de usuario u otro tipo de reconocimiento. Para este método se necesita de un proceso de cálculo complejo, porque se ha de comparar esta muestra con cada una de las anteriormente almacenadas para encontrar una coincidencia (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.3.2 Verificación

Siendo el primer paso del proceso la identificación del sujeto mediante algún nombre de usuario, tarjeta o algún otro procedimiento. Se selecciona de la base de datos el patrón que anteriormente se ha registrado para dicho individuo. Posterior a ello, el sistema recoge la característica biométrica y las compara con la que tiene recolectada. Es un proceso rápido, al comparar únicamente dos muestras, siendo el resultado positivo o negativo.

2.2.3.3 Evaluación

Es una ramificación de la caracterización donde el sistema biométrico afirma que un sujeto en particular no pertenece a una lista de coincidencias mediante la realización de comparaciones 1: N (uno a muchos) en toda la base de datos. En los ejemplos de aplicaciones encierran seguridad aeroportuaria, actividades de vigilancia, lugar público y público seguridad de eventos etc.

2.2.4 Tecnologías biométricas fisiológicas

Estas tecnologías se distinguen por considerar parámetros originarios de la medición directa de algún rasgo estrictamente físico del cuerpo humano a la hora de identificar sujetos.

2.2.4.1 Reconocimiento del iris

Figura 2-2 Reconocimiento de iris

Fuente: (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016)

El iris es la parte matizada del ojo, esta se encuentra entre la córnea y el cristalino. La abertura redonda y central del iris se denomina pupila. Los músculos muy pequeños dentro del iris hacen que la pupila se haga más pequeña y más grande para controlar la cantidad de luz que entra al ojo. Esto permite ver bien en condiciones más iluminadas o más oscuras (Hernàndez Reyes, 2016).

Se usa las características del iris humano con el fin de comprobar la identidad de un humano. Los esquemas de iris vienen marcados desde el nacimiento y rara vez cambian. Son enormemente complejos, contienen mucha información y tienen más de 200 propiedades únicas.

El escaneo del iris del ojo se realiza con una cámara de infrarrojos experta situada muy cerca del individuo que ilumina el ojo haciendo una fotografía de alta resolución. Este proceso ocurre en uno o dos segundos y provee los detalles del iris que se localizan, registran y almacenan para realizar futuras verificaciones (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.4.2 Huella dactilar

Figura 3-2 Huella dactilar

Fuente: (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016)

La huella dactilar está conformada por una serie de líneas oscuras que incorporan las crestas y una serie de espacios blancos que representan los valles.

La caracterización con huellas dactilares está basada principalmente en la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, valles y crestas.

2.2.4.3 Reconocimiento facial

Figura 4-2 Reconocimiento facial

Fuente: (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016)

La técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía es el reconocimiento facial. Para esto, se utilizan programas de cálculo que analizan imágenes de rostros humanos.

Los aspectos más relevantes empleados para la comparación son: la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.4.4 Reconocimiento de la geometría de la mano

Este método es más efectivo que el reconocimiento por huellas dactilares, porque al leer la mano de forma completa, permite capturar muchas más variables como imágenes individuales de algunos dedos y extraer datos como longitudes, anchuras, alturas, posiciones referentes y articulaciones entre otras (CORTÉS & MEDINA , 2010).

2.2.4.5 Reconocimiento de retina

El escáner biométrico de la retina se fundamenta en la utilización del patrón de los vasos sanguíneos incluidos en la misma. Siendo cada patrón único (incluso en gemelos idénticos al ser independiente de factores genéticos) y que se mantenga invariable a lo largo del tiempo, la convierten en una técnica eficaz para entornos de alta seguridad (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

2.2.4.6 Reconocimiento vascular

En la biometría vascular se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo (o de las muñecas). A diferencia de la huella dactilar el patrón biométrico es interno, por esta razón no deja traza y sólo se puede conseguir en presencia del hombre. Es por tanto muy difícil el robo de identidad (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016).

Por estas características es principalmente indicado para entornos de alta seguridad, así como en escenarios en que la superficie del dedo pueda estar en mal estado, erosionada o poco limpia.

2.2.4.7 Otras formas de biometría fisiológica

Existen además otras técnicas que analizan:

a) Líneas de la palma de la mano
b) Forma de las orejas
c) Piel, textura de la superficie dérmica
d) ADN, patrones personales en el genoma humano
e) Composición química del olor corporal.

2.2.5 Aplicaciones

Los sistemas biométricos se diseñaron más para las estructuras que buscan métodos de autenticación más seguros para el acceso del beneficiario, para comercio electrónico y otras aplicaciones de seguridad

Las más conocidas son las huellas dactilares, reconocimiento de cara y reconocimiento de iris. En la tabla 2:1 se maneja las diferentes tecnologías, las posibles aplicaciones y los principales mercados que se pueden utilizar sean estos en el sector privado o público que ofrece la industria biométrica (Hernàndez Reyes, 2016).

Los nuevos usos de estas técnicas todavía se aumentarán más dado que la fiabilidad del sistema está presentada como un ejemplo en año 2016 se maneja el sistema de autenticación de iris y huella digital en un Smartphone (Hernàndez Reyes, 2016).

Tabla 1-2 Diferente tecnologías biométricas

Tecnología	**Aplicación Horizontal**	**Principales mercados verticales**
Reconocimiento de iris (ojo)	Acceso a sistemas	Industria manufacturera
AFIS/Lifescan	Controles de Vigilancia	Servicios policiales y militares
Reconocimiento de cara	Identificación sin contacto	Farmacéuticas, Hospitales, Industria pesada y Obras
Geometría de Mano	Identificación Criminal	Hospitales y Sector Salud
Reconocimiento de Voz	Acceso a instalaciones	Viajes y Turismo
Escritura y Firma	Vigilancia	

Fuente: (Hernàndez Reyes, 2016)

2.2.6 Comparativo de sistemas

Tabla 2-2 Recolección de las diferentes características de los sistemas biométricos.

Características	Aceptación del Usuario	Facilidad de uso	Cote	Utilidad (identificación)	Utilidad (Verificación)	Estabilidad	Intrusismo	Fiabilidad
ADN	Baja	Baja	Alto	✓	✓	Alta	Muy alto	Alta
Dinámica de escritura	Alta	Alta	Bajo	✗	✓	Baja	No	Baja
Firma	Media	Alta	Bajo	✗	✓	Media	No	Baja
Geometría de la mano	Media	Alta	Alto	✗	✓	Media	No	Media
Huella dactilar	Media	Alta	Bajo	✓	✓	Alta	No	Alta
Iris	Media	Media	Alto	✓	✓	Alta	No	Alta
Reconocimiento facial	Media	Media	Bajo	✗	✓	Media	Bajo	Media
Retina	Media	Baja	Alto	✓	✓	Alta	Alto	Alta
Voz	Alta	Alta	Bajo	✗	✓	Media	No	Baja

Fuente: (Hernàndez Reyes, 2016)

Tabla 3-2 Recolección de nivel de seguridad para las diferentes características de los sistemas biométricos

Característica	Nivel de Seguridad	Ratio de error	Precisión	Errores	Falso Positivo	Falso Negativo
Iris	Alto	1/131,000	4	Iluminación inadecuada.	4	4
ADN	Alto	Sin datos	4	No conocido.	5	5
Dinámica de escritura	Medio	Sin datos	1	Lesiones de mano, cansancio.	4	1
Firma	Medio	1/50	2	Cambios de escritura.	2	1
Geometría de la mano	Medio	1/500	3	Edad, lesiones varias.	4	2
Huella dactilar	Alto	1/500	4	Sequedad, suciedad, edad.	5	5
Reconocimiento facial	Medio	Sin datos	3	Pelo, gafas, edad, iluminación	3	1
Retina	Alto	1/10^6	4	Gafas, lentillas	5	5
Voz	Medio	1/50	2	Ruidos ronquera, resfriado	2	1

Fuente: (Hernàndez Reyes, 2016)

2.3 Tecnología biométrica iris del ojo

2.3.1 ¿Qué es la Iris?

El color del iris establece el color de ojos (azul, verde, marrón…etc.). El iris es una estructura fina y circular del ojo, que controla el diámetro y tamaño de la pupila y regula la cantidad de luz que penetra (NUO, 2015).

2.3.2 Escaneo de Iris

La información del iris la conseguimos a través de una cámara de alta resolución con una sutil iluminación infrarroja que retrata las imágenes de la estructura del iris.

Las imágenes son convertidas en plantillas digitales y se almacenan en una base de datos en el propio lector. Estas plantillas biométricas proporcionan una representación matemática del iris, las cuales coinciden con una identificación positiva e inequívoca de un individuo (NUO, 2015).

El reconocimiento de Iris es la más extendida y utilizada, por ser la menos intrusiva, muchas organizaciones gubernamentales y edificios corporativos ya utilizan el escaneo de iris como un medio de restringir el acceso a ciertas áreas de alta seguridad.

2.3.3 Características de la Iris

Potencialidad para la Identificación:

- Mayor unicidad que la huella
- Parámetros accesibles desde el exterior, a través de protección dada por la córnea
  - ✓ Textura del iris
  - ✓ Acceso visual a la retina a través de la pupila
- Órgano estable (en muchos de sus parámetros):
  - ✓ Con la edad
  - ✓ Frente a accidentes (debido a la córnea)
- Fácil detección de sujeto vivo
  - ✓ Por variaciones del tamaño de la pupila frente a cambios de iluminación

- Manipulación compleja
    - ✓ Conllevaría potenciales riesgos en la visión del individuo (Ávila, 2012)

Inconvenientes:

- Utilización de elementos externos por parte de los usuarios (Ávila, 2012)

2.3.4 Fases del sistema de identificación

Las principales etapas de un sistema de este tipo son:

- ✓ Captura de los datos
- ✓ Reprocesado de dichos datos
- ✓ Extracción de características
- ✓ Verificación o comparación del vector de características formado con el patrón almacenado previamente.

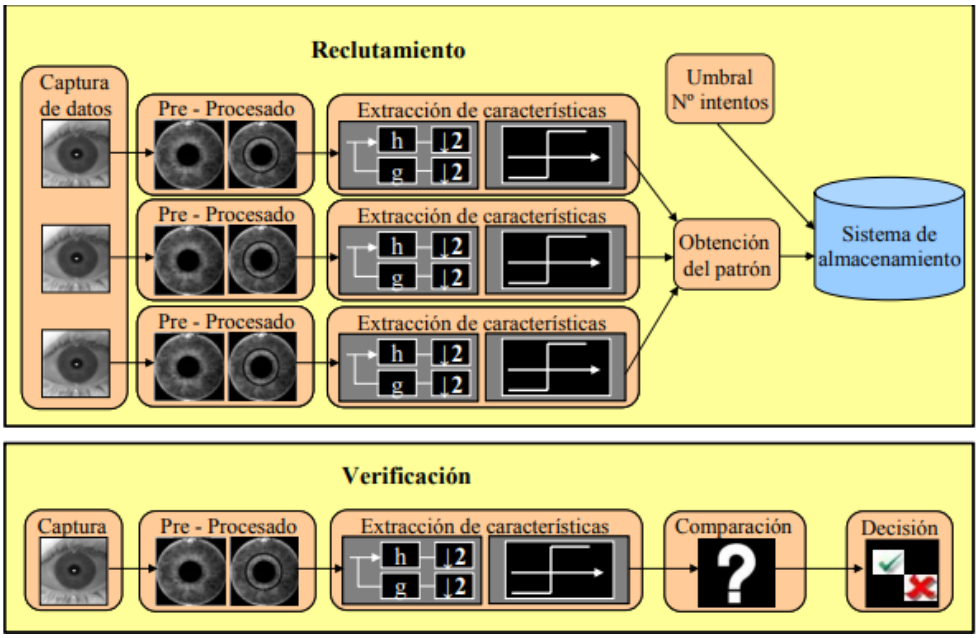


Figura 5-2 Etapas de un sistema de identificación biométrica por iris

Fuente: (Ávila, 2012)

2.3.4.1 Captura de la imagen

Se pueden usar cámaras con luz infrarroja, con lo que las imágenes ya son capturadas en blanco y negro.

Para el sistema de captura hay que tener en cuenta los siguientes puntos:

a) Se debe de precisar de una cámara que tenga una gran resolución.
b) Centrar la captura a la característica a medir, es decir, en este caso que salga únicamente el ojo y nada más, concentrando de esta manera toda la calidad de la imagen en la captura de lo que nos interesa.
c) No debe de encontrarse la cámara demasiado cerca del sujeto a medir, puesto que esto le produciría una situación incómoda y sentirse amenazado.
d) La adquisición a la distancia elegida no debe de suponer una deformación de la imagen capturada. (Herrero, 2012)

2.3.4.2 Pre-procesado

El pre-procesado tiene una gran importancia, ya que, es necesario adaptar la captura a los requisitos de extracción de características y se debe hacer una serie de procesos:

a) La detección del borde externo del iris, es decir, la frontera con la esclerótica.
b) La detección del borde interno del iris, o lo que es lo mismo, el límite con la pupila.
c) Eliminación de las partes de la imagen no deseadas, es decir, todo lo que no esté dentro del iris.
d) Adaptar la imagen a la técnica de extracción de características a realizar, es decir, recoger los datos y disponerlos según un vector (conocido como array en inglés), una matriz, etc. (Herrero, 2012).

- Detección del borde exterior del iris

Es el primer paso en la detección del iris y se debe al cambio brusco de contraste entre el iris y la esclerótica, que es blanca. Antes de ejecutar esta detección hay que afirmar que la imagen se encuentra en blanco y negro para su mejor procesado. Una vez cargada la imagen en escala de grises se procede a ejecutar los siguientes pasos en dicho orden:

- ✓ Se crea y se copia de la imagen obtenida cuatro veces menor para mejorar su procesado (cuando se quiera obtener la detección fina se procede a realizar la búsqueda sobre la imagen grande original).
- ✓ Se eliminan las partes de la imagen sobre-expuestas debido a puntos de luz producidos por un flash, por ejemplo. Esta eliminación se realiza mediante un umbral establecido.
- ✓ Se buscan candidatos a ser centros mediante búsqueda de puntos negros agrupados. Esto se establece mediante una cuadrícula en cuyos puntos se situarán los centros que se utilizarán en el algoritmo de detección de bordes, el punto que determine el mejor borde será tomado como el centro del iris.
- ✓ Por cada uno de los puntos de la cuadrícula, que son los posibles centros, se toma uno a uno como origen de coordenadas y a partir de él se va incrementando el radio (Δ_r) y el ángulo (Δ_θ), y buscando el múltiplo n de Δr que maximiza el parámetro D en la siguiente ecuación:
- ✓

$$D = \sum_{m} \sum_{k=1}^{5} (I_{n,m} - I_{(n-k),m})$$

$$I_{i,j} = I(x_o + i \cdot \Delta_r \cdot \cos(j \cdot \Delta_\theta)\,, y_o + i \cdot \Delta_r \cdot \sin(j \cdot \Delta_\theta))$$

- ✓ Una vez que se ha encontrado el punto de la cuadrícula que proporciona el máximo D, se crea una nueva cuadrícula, con mayor resolución y que solo abarca el cuadrado formado por los puntos comprendidos entre los dos extremos del punto elegido, tanto en el eje horizontal como en el vertical.
- ✓ Se vuelve a realizar el mismo proceso de detección por cuadrícula, pero sobre la imagen de gran resolución con el punto elegido y así se obtiene el centro de forma más refinado.
- ✓ Una vez localizado correctamente el centro, se disminuye el factor de Δ_r para tener una mayor precisión a la hora de sacar el borde, y se determina la distancia del centro al borde mediante " $n \cdot \Delta_r$ siendo n el valor que da el máximo valor a D (Herrero, 2012).

- ➢ Detección del borde interior del iris

Este paso es similar al anterior proceso con la diferencia de que el sistema de detección ha de ser más sensible porque en el campo infrarrojo el primer cambio brusco se ocasiona entre pupila e iris. Por ello se detecta primero la pupila y luego el iris. No se puede usar el mismo centro puesto que la pupila y el iris no son concéntricos, aunque a simple vista lo parezca, suele estar desplazada ligeramente hacia abajo y hacia la nariz. En algunos casos, esta desviación llega a ser del 15%.

Por lo tanto, no se realizará el mismo procedimiento de nuevo, basta con crear una cuadrícula alrededor del centro del iris que abarque el ±20% del tamaño del iris. En este paso se vuelve aplicar el mismo sistema que el anterior pero únicamente solo con la cuadrícula determinada anteriormente.

El resultado será un centro de la pupila similar al del iris y un radio menor que el del iris.

Después de realizado ambos procesos se ejecuta la eliminación de la información apreciable que es todo lo que no se encuentre entre el borde interior y exterior del iris. Se efectúa un estiramiento del histograma, con lo que se logra el iris aislado del resto de la imagen (Herrero, 2012).

2.3.4.3 Extracción de características de la captura

- Adaptación del iris detectado: Cuando logremos el iris aislado, es decir, sin parpados o esclerótica, se debe considerar las variaciones del tamaño del iris por dilatación o contracción.

Los antecedentes para poder manipularlos con libertad han de tener dos condiciones indispensables que se asignarán independientemente del tamaño del iris:

- ✓ Estén suprimidos los conos superior e inferior.
- ✓ El tamaño de los datos sea el mismo siempre.
- Algoritmo de extracción de características: después de haber obtenido la matriz rectangular de datos de la captura de iris, se procede a sacan las características. (Herrero, 2012)

Para ello se aplica el filtro de Gabor para la extracción de características determinada por la siguiente ecuación:

$$g(x, y, \varphi_k, \lambda) = exp\left\{-\frac{1}{2}\cdot\left[\frac{(x\cdot cos\varphi_k + y\cdot sin\varphi_k)^2}{\sigma_x^2} + \frac{(-x\cdot sin\varphi_k + y\cdot cos\varphi_k)^2}{\sigma_y^2}\right]\right\}\cdot$$

$$exp\left\{\frac{2\pi(x\cdot cos\varphi_k + y\cdot sin\varphi_k)}{\lambda}\right\}$$

- Comparación: Se debe practicar mediante la comparación de las características obtenidas con el patrón previamente almacenados. El sistema que se usa para la comparación de características se basa en el cálculo de la distancia de Hamming. Este método es "prácticamente" el definitivo hoy en día. Particularmente los buenos resultados obtenidos y su simplicidad hacen que en un sistema, como el desarrollado en este proyecto, sólo

precise de una imagen para identificar al usuario correctamente. Esto hace que el sistema sea de gran aprobación por el usuario (Herrero, 2012).

La distancia de Hamming hace referencia a la efectividad de los códigos de bloque y depende de la diferencia entre una palabra de código válida y otra (Herrero, 2012).

Por ejemplo, la distancia de Hamming de 101111 y 100110 es 2.

Simplemente se realiza una comparación de los bits que hay de la característica tomada por captura del usuario con la de la base de datos considerada la correcta, y por cada bit que haya diferente en la misma posición que el otro se asigna un valor de 1 en un array de la misma dimensión que el código a comparar, si el bit es el mismo, entonces se le asigna un 0. En el ejemplo anterior por tanto, sería: 001001 (Herrero, 2012).

Después ese valor puede gestionarse como se crea conveniente. En el caso de este proyecto se optó por un valor porcentual. Se calcula de la siguiente forma:

$$Acierto\% = 100 - \frac{valores\ distintos}{valores\ comparados} \cdot 100$$

CAPÍTULO III

3 METODOLOGÍA DE INVESTIGACIÓN

En este apartado es fundamental detallar el proceso usado o la metodología implementada en la investigación realizada. Se mencionan a detalle los métodos, técnicas, mediciones que ayudan a recopilar la información pertinente así lograr identificar la comprobación de la hipótesis planteada en este trabajo investigativo.

Con el propósito de implementar un sistema biométrico lector del iris del ojo, que permita mejorar la seguridad y la confidencialidad en sistemas informáticos.

3.1 Tipo y Diseño de la Investigación

3.1.1 Tipo de Investigación

La investigación es de tipo cuantitativa por lo que asigna valores numéricos a la investigación analizada, con el propósito de estudiar con métodos estadísticos posibles relaciones entre las variables y generalizar a una población.

También se cataloga a esta investigación de tipo científico ya que se profundiza con arduo y recóndito estudio de arte para el análisis, interpretación, opiniones, resultados opiniones que describen en cada una de sus investigaciones los autores citados en la recopilación bibliográfica.

3.1.2 Diseño de la Investigación

La presente investigación del tipo experimental con un enfoque de carácter científico, donde un conjunto de variables se mantiene constantes, mientras que el otro conjunto de variables se mide como sujeto del experimento. Se utilizan los siguientes tipos de estudio:

- ✓ **Estudios exploratorio**

Los estudios exploratorios nos ayudan a familiarizarnos con fenómenos desconocidos y obtener más información para poder realizar una investigación completa, identificar variables o conceptos, establecer preferencias para futuras investigaciones o sugerir aseveraciones o principios. Este estudio será de gran importancia al inicio del estudio para la recolección de información y selección de herramientas.

- ✓ **Estudios descriptivos**

Este tipo de estudios se basan en la recolección de datos como muestra de un fenómeno, hecho, fenómeno o alguna particularidad que ocurre. Es ideal para investigaciones de tipo cuantitativo.

Por este motivo, la etapa de extracción de características es la específica para la definición del modelo.

3.2 Métodos y Técnicas De Investigación

3.2.1 Métodos

Los métodos de investigación científica a utilizar siguen los siguientes:

El método hipotético – deductivo

Este método es empleado ya que la investigación inicia a raíz de la observación de resultados de proyectos realizados, por medio de lo cual se genera hipótesis y luego se obtienen las conclusiones a partir de resultados.

Método de Análisis y Síntesis

Utilizado en la investigación sobre el estado del arte, la adopción de medidas a implementarse y la adquisición de parámetros sobre datos.

3.2.2 Técnicas

1. Consulta en base a documentos (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).
2. Experimentación: Se recrearán distintas circunstancias en un ambiente controlado para la ejecución de pruebas, las cuales proveerán los resultados para la toma de decisiones y la definición del prototipo.
3. Análisis de la información.
4. Observación de campo: se harán distintas mediciones a los fenómenos recreados para la toma de decisiones.

3.3 Instrumentos

Los instrumentos son las diferentes herramientas usadas para realizar la implementación del modelo de seguridad biométrico en las aplicaciones web facilitando el estudio y el progreso de pruebas dentro del escenario propuesto.

Primarios:

- Hardware
- Software

HARDWARE

Figura 6-3 EF-45™ Sistema de Reconocimiento de Iris

DESCRIPCIÓN

El sistema de reconocimiento de iris dual CMITECH ef-45 de próxima generación proporciona una facilidad de uso sin precedentes a través de un enfoque de posicionamiento del usuario altamente innovador e intuitivo. Los sujetos verán su propia cara en una pantalla a color frontal de alta resolución de 5.0 pulgadas dentro de la interfaz gráfica en tiempo real. Las imágenes biométricas del iris se recopilan automáticamente, siempre que se cumplan las métricas de calidad.

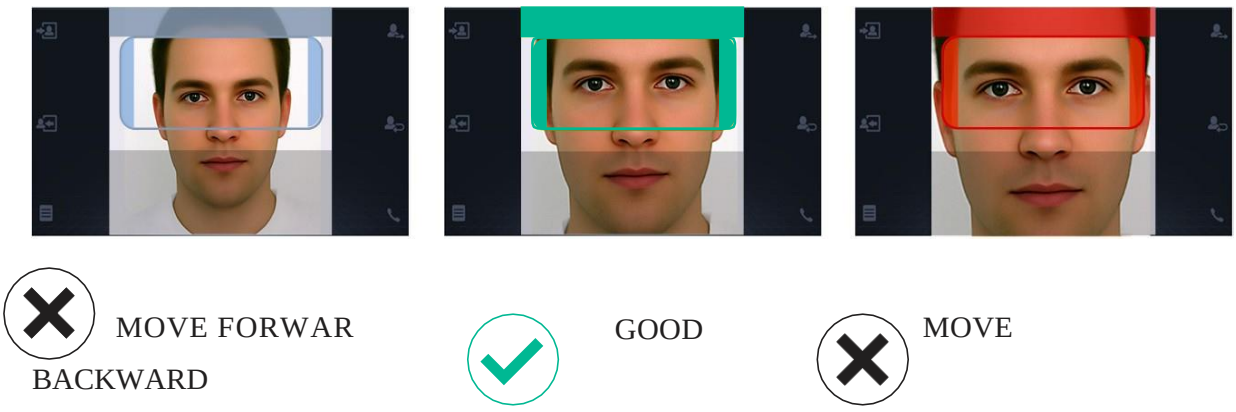


Figura 7-3 Incluye señales visuales en color para una distancia adecuada

Tabla 4-3 Especificaciones técnicas

CPU integrada	Procesador de cuatro núcleos ARM Cortex A9
Algoritmo Iris incorporado para codificar y hacer coincidir	Estándar en todas las configuraciones
Configuraciones del kit de desarrollo de software flexible (SDK)	SDK de alto nivel, se ofrece en versiones C # (.NET) y C ++. Incluye la aplicación del lado del host para conectarse a la capa de servicios
Autenticación de doble factor con reconocimiento de iris	Opciones de tarjeta inteligente y PIN para una autenticación más segura
Salida de imagen de iris	Cumple con los estándares de imágenes de iris ISO 19794-6 2011 e ISO 29794-6
Resolución en píxeles de imagen de iris	640 x 480 píxeles, profundidad de 8 bits, admite múltiples formatos
FAR Ajustable (tasa de aceptación falsa)	El umbral del algoritmo de iris se puede modificar para ajustar entre 10-8 y 10-14
Localización ocular estereoscópica avanzada y patentada	El EF-45 localiza con precisión y en tiempo real la posición de ambos ojos en 3D para la precisión y la facilidad de posicionamiento del sujeto y la calidad de la imagen del iris. Esta característica permite los indicadores de posicionamiento de distancia de sujetos rápidos y fiables que se seleccionan como códigos de color azul, verde o rojo.
Interfaz de red, estándar	10/100 Base-T Ethernet (conector RJ45)

Secundarios:

Archivos digitales.

3.4 Fuentes de Información

Dentro de las fuentes de obtención de información utilizadas en la presente investigación se mencionan:

Primaria:

Esta información es obtenida por medio de las pruebas del sistema.

Secundaria:

Diversa bibliografía como revistas, artículos publicados, libros, páginas de internet, entre otras.

3.5 Planteamiento de la Hipótesis

3.5.1 Hipótesis General

El diseño de una interfaz de acceso biométrico mediante el iris del ojo, mejorará la seguridad y confidencialidad de la información en sistemas informáticos.

3.5.2 Identificación de variables

Variable Independiente: Sistema de seguridad biométrico mediante el iris del ojo.

Variable Dependiente: Nivel de confiabilidad de seguridad del sistema.

3.5.3 Operacionalización Conceptual de Variables

Tabla 5-3 Operacionalización Conceptual de Variables

Hipótesis	Variables	Indicadores
El diseño de este sistema de seguridad biométrico mediante el iris del ojo lograra reducir las vulnerabilidades a la confidencialidad de la información en sistemas informáticos.	Independiente: Sistema de seguridad biométrico mediante el iris del ojo. Dependiente: Nivel de confiabilidad de seguridad del sistema.	-Extracción de características de usuarios - Porcentaje de autenticaciones efectivas -Porcentaje de vulnerabilidades -Robustez respecto a otros sistemas de control de acceso.

3.5.4 Operacionalización Metodológica de Variables

Tabla 6-3 Operacionalización Metodológica de Variables

Formulación del problema	Objetivo General	Hipótesis General	Variables	Indicadores	Índice	Técnicas	Instrumentos
¿Cómo se puede mejorar la confidencialidad de acceso de usuarios en sistemas informáticos con la implementación de un sistema de seguridad biométrico, mediante el iris del ojo?	Diseñar un sistema de seguridad biométrico mediante el iris del ojo para reducir las vulnerabilidades a la confidencialidad de la información en sistemas informáticos.	H0: El diseño de este sistema de seguridad biométrico mediante el iris del ojo lograra reducir las vulnerabilidades a la confidencialidad de la información en sistemas informáticos. H1: El diseño de este sistema de seguridad biométrico mediante el iris del ojo no lograra	**Variable Independiente:** Sistema de seguridad biométrico mediante el iris del ojo.	-Extracción de características de usuarios - Porcentaje de autenticaciones efectivas -Porcentaje de vulnerabilidades	-Bits/bytes -pixeles -Tanto por ciento % -Tanto por ciento %	-Observación -Observación -Observación	-Software -Software -Software

		reducir las vulnerabilidades a la confidencialidad de la información en sistemas informáticos.					
			Variable Dependiente: Nivel de confiabilidad de seguridad del sistema	-Robustez respecto a otros sistemas de control de acceso.	-Tanto por ciento %	- Observación	-Software

3.6 Población y Muestra

3.6.1 Población

La población son los principales ataques que afectan la confidencialidad en el control de acceso de usuarios a un sistema informático.

3.6.2 Selección de la muestra

Se realizará un estudio de toda la población de ataques seleccionados.

- Ataques de presentación
- Ataques de procesamiento
- Vulnerabilidad de software y de red
- Ataques sociales
- Vulnerabilidades basadas en burlarse o saltarse el sistema
- Factores ambientales

Las fases para analizar las vulnerabilidades presentes son:

1) Generación de ataques.
2) Análisis del vulnerabilidad de información
3) Aplicación del sistema biométrico.
4) Análisis comparativo de los resultados de los escenarios de prueba.

3.7 Instrumentos de recolección de datos

Tabla 7-3 Recolección de datos

Factores ambientales	Iris del ojo
Nivel de sonido ambiente	
Polvo	X
Variaciones	X
Variaciones de voltaje	
Humedad atmosférica	
Vibraciones	X
Ruido electromagnético	X
Temperatura	

Primarios:

La tecnología o software especializado como base de datos.

Secundarios:

Archivos digitales.

3.8 Instrumentos para Procesar Datos Recopilados

Se plantea la utilización de un dispositivo biométrico el EF-45 para que recepte las señales del iris de los dos ojos

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Presentación de resultados

La investigación realizada referente al diseño de una interfaz gráfica que nos sirva de medio para enlazarnos a los sistemas informáticos por medio de un dispositivo biométrico arroja como resultado que el iris del ojo es la técnica biométrica más segura para realizarlo, esto se puede manifestar ya que el primer objetivo específico se refiere justamente al análisis de las principales técnicas biométricas. En este capítulo se trata de comprobar que efectivamente si utilizamos una interfaz conectada a un dispositivo biométrico como es el lector del iris de los ojos lograremos reducir los ataques a la confidencialidad en los sistemas informáticos.

4.2 Plan de recolección de información

Al tratarse de una investigación innovadora por lo menos aquí en el país se realizó una investigación de campo, es decir extrayendo datos e información directamente con los profesionales que se encuentran administrando sistemas informáticos a través de encuestas y entrevistas, se planteó la idea de realizar una investigación en donde se enfrenten escenarios validados con el lector del iris del ojo frente a uno que no realice el acceso con dispositivos biométricos, pero se constató que en el país no existe ninguna entidad conocida que disponga de este tipo de dispositivo EF-45.

Tabla 8-4 Matriz de recolección de información

N°	Técnicas de recolección de Información	Medios	Objetivo Alcanzado
1	Encuestas	Correos electrónicos Personal Online	Recoger los criterios técnicos y especializados de los profesionales encargados de la seguridad de la información en sus diferentes empresas específicamente referente a la confidencialidad.
2	Entrevistas	Estructurada Focalizada	Dialogo directo referente a las seguridades empleadas en sus empresas, funcionalidad y presentación de una nueva alternativa a ser implementada en sus sistemas informáticos.
3	Observación no experimental	Guía de observación o de campo	Se ha visitado directa y personalmente varias empresas que mantienen sistemas informáticos para evidenciar que tipos de seguridades tienen instaladas.
4	Análisis documental	Libros Boletines Revistas Folletos Periódicos	Recopilar toda la información posible como características específicas del dispositivo, especificaciones técnicas, funcionamiento, soporte, utilidad y más del EF-45 para la construcción de la interfaz de acceso biométrica a los sistemas informáticos

Elaborado por: Peñaherrera, Andrés 2020

4.3 Plan de procesamiento de información

- Esbozo del material de recolección de información.
- Aplicación de la encuesta.
- Exploración de la información, elección de la información útil para en la investigación.
- Tabulación según variables de la hipótesis, manejo de la información, estudio estadístico de los datos para la presentación de resultados.
- Demostración de hipótesis
- Conclusiones y recomendaciones.

4.4 Análisis e interpretación de resultados

El proyecto de investigación plantea la construcción e implementación de una interfaz de acceso biométrica que ayude a fortalecer la seguridad de la confidencialidad de los sistemas informáticos, sean estos sistemas web, sistemas de escritorio, cajeros automáticos, sistemas de control y todos las aplicaciones que necesiten credenciales de acceso para su ingreso, con estos antecedentes se elaboró un cuestuario que trate de recoger los principales conceptos de la seguridad de la información en uno de sus tres pilares fundamentales como es la confidencialidad pero con la utilización de dispositivos biométricos.

Se ejecutó la codificación de las respuestas del cuestionario, obteniendo resultados cuantitativos, mismos que servirán para el análisis e interpretación, siendo ineludibles para la comprobación de hipótesis.

4.4.1 Cuestionario aplicado a profesionales dedicados a la seguridad de la información.

Tabla 9-4 Cuestionario aplicado a profesionales dedicados a la seguridad de la información.

No	Ítem o Enunciado
1	¿Puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?
2	¿Se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?
3	¿El iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?
4	¿La identificación única del iris de ojo de cada individuo no es susceptible a suplantación?
5	¿Puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?
6	¿Se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?

7	¿Se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?
8	¿Puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?
9	¿La tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?
10	¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son imposibles de falsificar y alterar?

Elaborado por: Peñaherrera, Andrés 2020

Tabla 10-4 Pregunta N° 1.

¿Puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?

Alternativas	Frecuencia	Porcentaje
SI	20	67%
NO	10	33%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

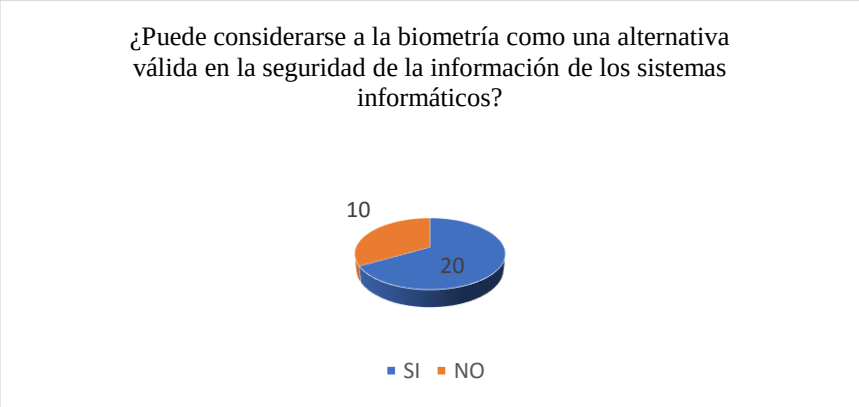


Gráfico 1-4 Pregunta N° 1.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

En un 67% de aceptación afirman que la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos. Mientras que el 33% rechazan a un sistema biométrico debido a las vulnerabilidades existentes.

Tabla 11-4 Pregunta N° 2

¿Se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?

Alternativas	Frecuencia	Porcentaje
SI	27	90%
NO	3	10%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

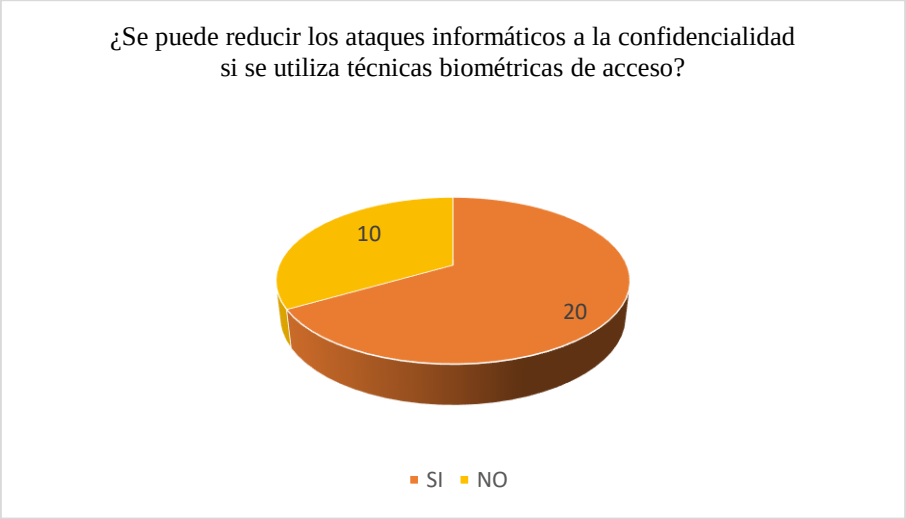


Gráfico 2-4 Pregunta N° 2.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

El 90 % de las personas encuestadas afirman que un sistema biométrico puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso.

Tabla 12-4 Pregunta N° 3

¿El iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?

Alternativas	Frecuencia	Porcentaje
SI	27	90%
NO	3	10%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

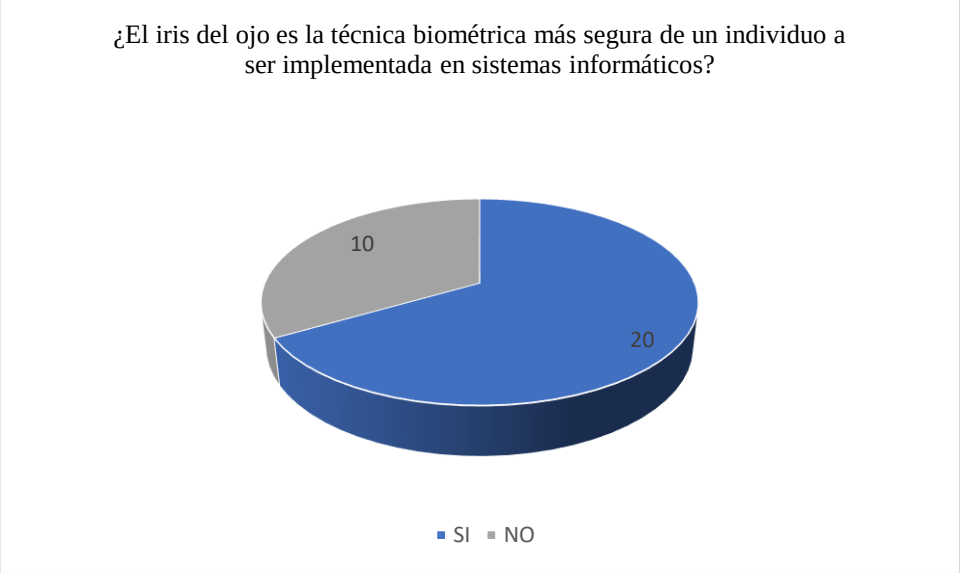


Gráfico 3-4 Pregunta N° 3.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

Se afirma que el iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos arrojando un 90 % de resultados que afirman esta propuesta. Mientras que un 10 % rechazan esta propuesta siendo un valor relativamente bajo.

Tabla 13-4 Pregunta N° 4.

¿La identificación única del iris de ojo de cada individuo no es susceptible a suplantación?

Alternativas	Frecuencia	Porcentaje
SI	5	17%
NO	25	83%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

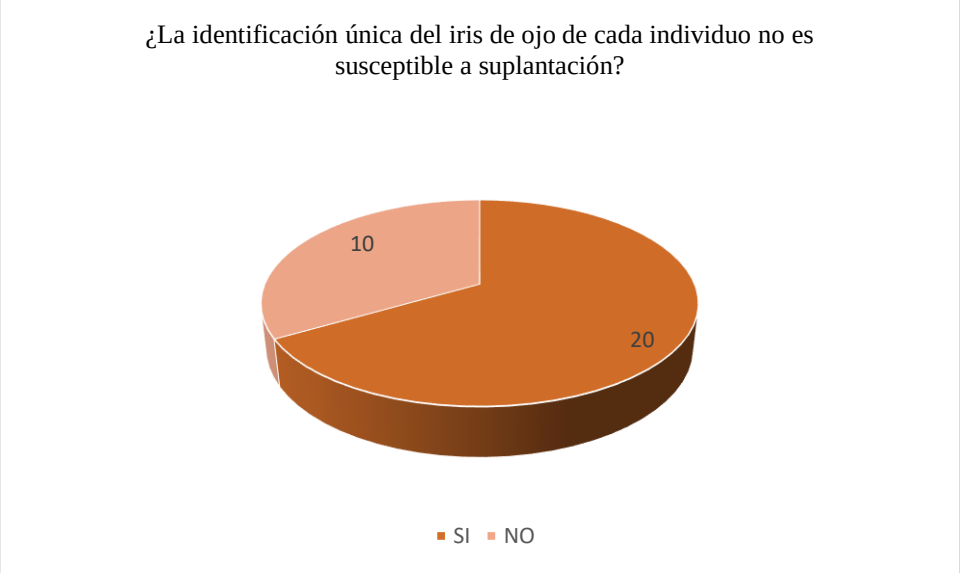


Gráfico 4-4 Pregunta N° 4.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

El 83 % de las personas afirman que la identificación única del iris de ojo de cada individuo no es susceptible a suplantación debido a que los rasgos físicos de identificación son únicos para cada individuo iris del ojo, huella dactilar etc.

Tabla 14-4 Pregunta N° 5.

¿Puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?

Alternativas	Frecuencia	Porcentaje
SI	2	7%
NO	28	93%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

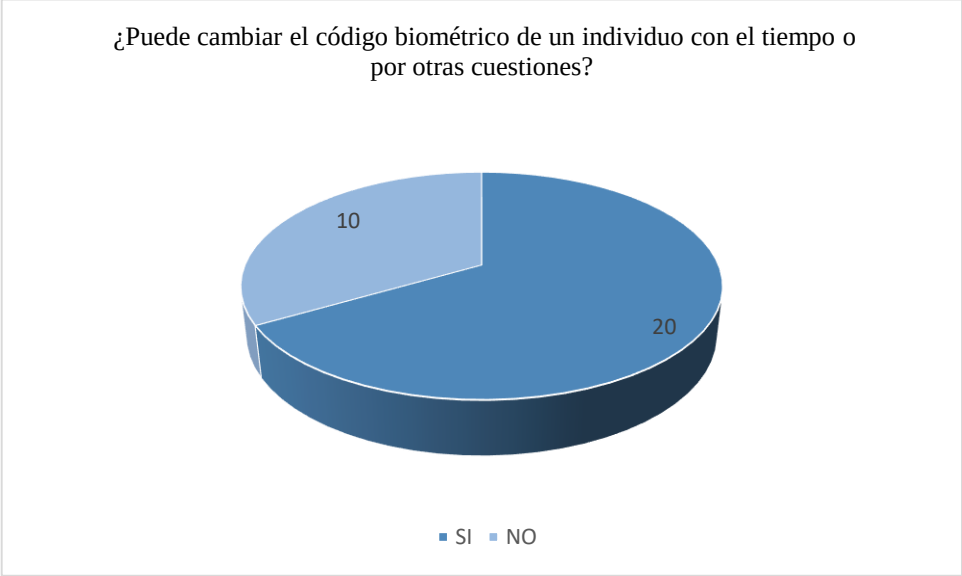


Gráfico 5-4 Pregunta N° 5.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

Un 93 % de individuos rechazan que el código biométrico de un individuo puede cambiar con el tiempo o por otras cuestiones. Mientras que el 7% de respuestas afirman que si puede existir dicho cambio en el código biométrico.

Tabla 15-4 Pregunta N° 6.

¿Se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?

Alternativas	Frecuencia	Porcentaje
SI	10	33%
NO	20	67%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

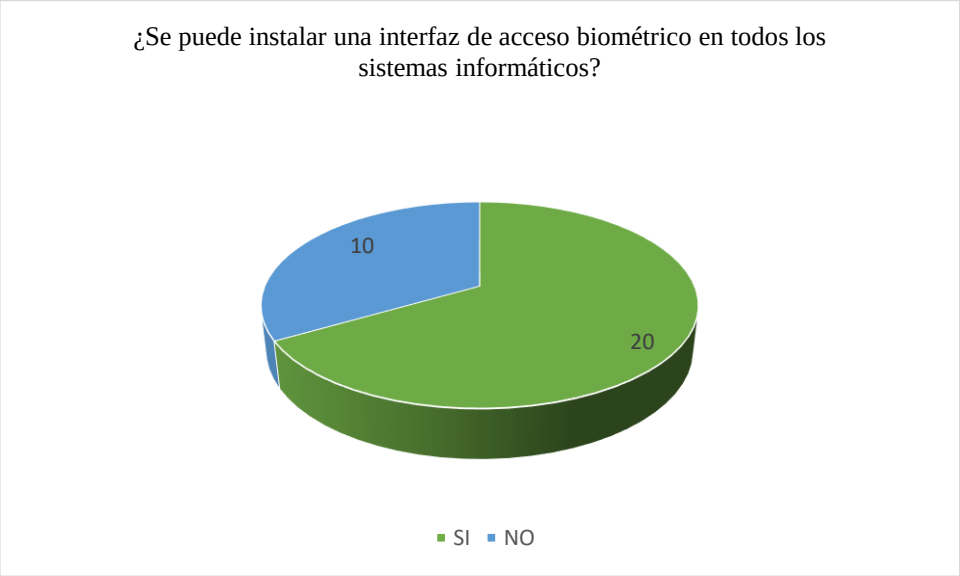


Gráfico 6-4 Pregunta N° 6.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

El 67% de las personas encuestadas rechazan la instalación de una interfaz de acceso biométrico en todos los sistemas informáticos. El 33 % por lo contrario aceptan la instalación de una interfaz de acceso biométrico.

Tabla 16-4 Pregunta N° 7.

¿Se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?

Alternativas	Frecuencia	Porcentaje
SI	23	77%
NO	7	23%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

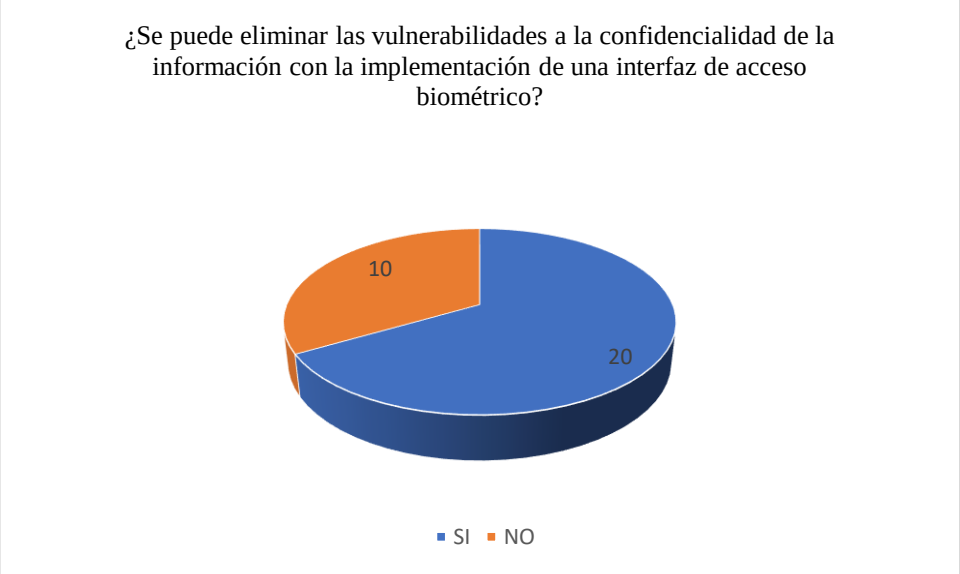


Gráfico 7-4 Pregunta N° 7.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

Se conoce de una aceptación alta equivalente a 77 % las cuales afirman la instalación de un sistema biométrico puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico.

Tabla 17-4 Pregunta N° 8.

¿Puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?

Alternativas	Frecuencia	Porcentaje
SI	10	33%
NO	20	67%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

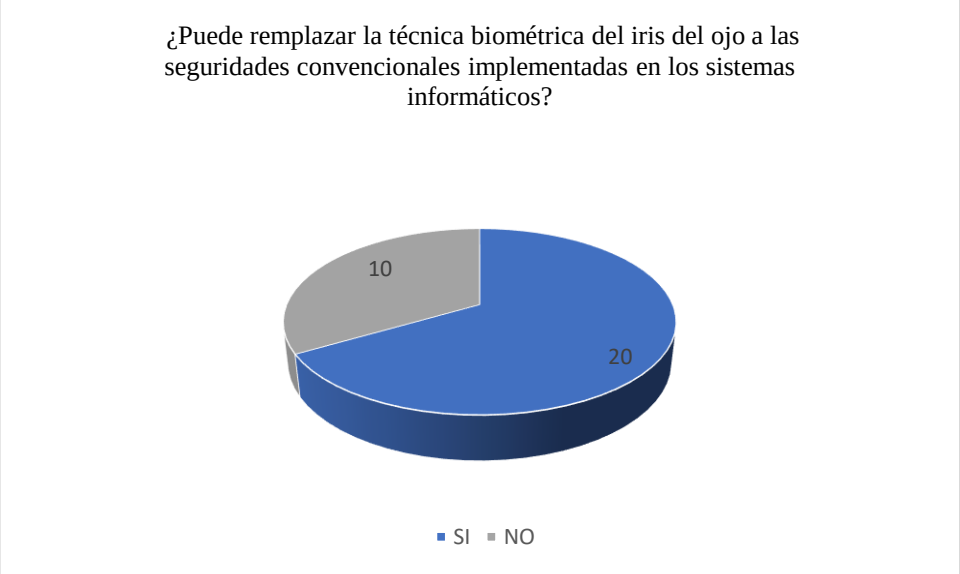


Gráfico 8-4 Pregunta N° 8.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

No existe la suficiente aceptación de remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos

Tabla 18-4 Pregunta N° 9.

¿La tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?

Alternativas	Frecuencia	Porcentaje
SI	8	27%
NO	22	73%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

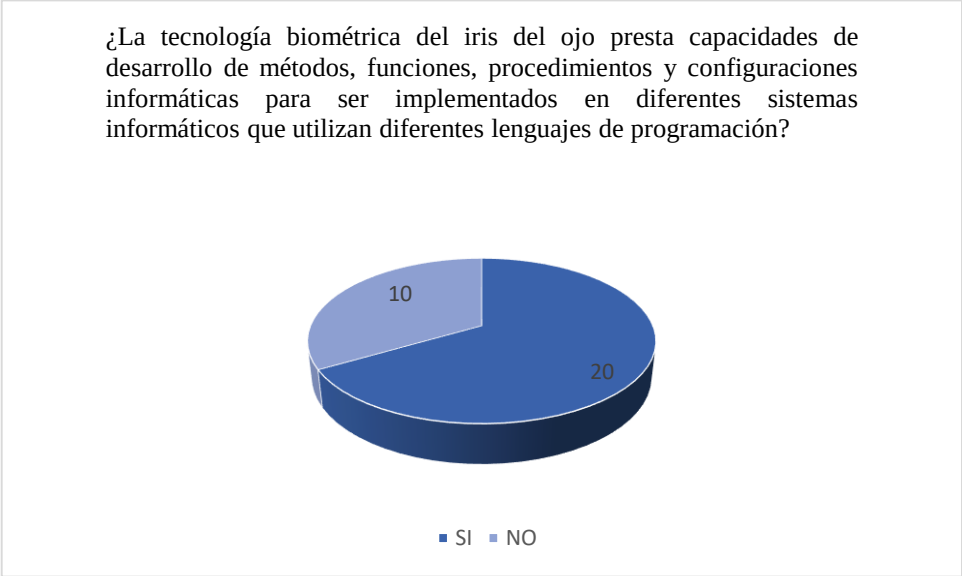


Gráfico 9-4 Pregunta N° 9.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

El 73% de las personas encuestadas rechazan la tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación

Tabla 19-4 Pregunta N° 10.

¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son imposibles de falsificar y alterar?

Alternativas	Frecuencia	Porcentaje
SI	26	87%
NO	4	13%
TOTAL	30	100%

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

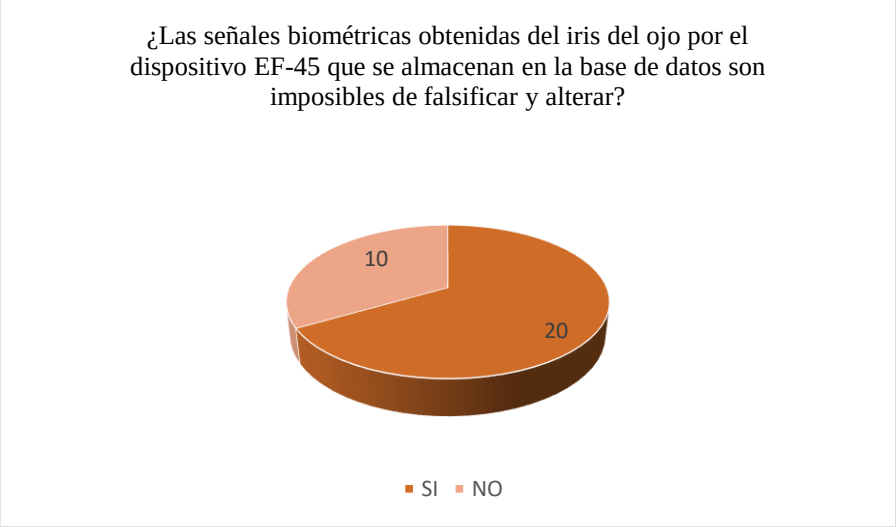


Gráfico 10-4 Pregunta N° 10.

Fuente: Encuesta Estructurada
Elaborado por: Peñaherrera, Andrés 2020

Análisis e interpretación de resultados:

Existe un 87% de aceptación en las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son imposibles de falsificar y alterar comprobando de esta manera que este sistema biométrico es seguro.

Para la comprobación de la hipótesis de la investigación realizada se utilizará el estadístico chi cuadrado que es una medida de la divergencia entre la distribución de los datos y una distribución esperada o hipotética seleccionada, entonces se procederá a calcular las frecuencias esperadas aplicando la siguiente fórmula.

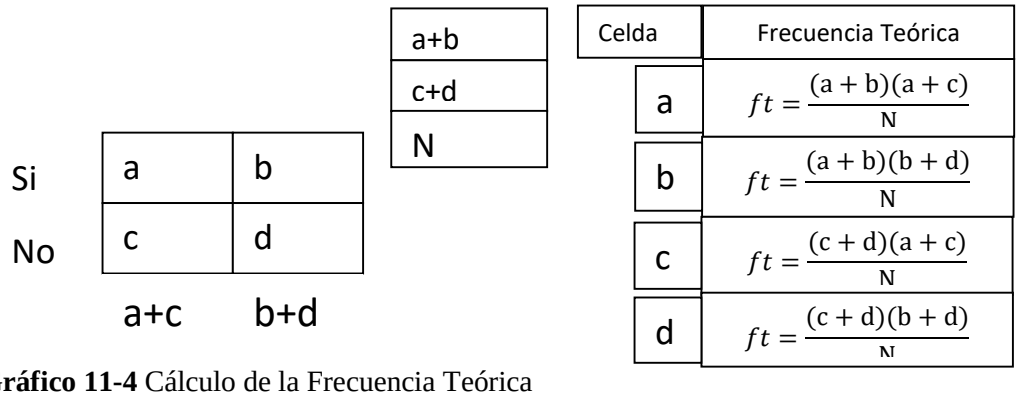


Gráfico 11-4 Cálculo de la Frecuencia Teórica

Fuente: Morales Vallejo, Pedro (2008) Estadística aplicada a las Ciencias Sociales. Madrid: Universidad Pontificia Comillas (edit@pub.upcomillas.es)

Tabla 20-4 Cálculo de frecuencias Esperadas con respuesta afirmativa

N°	Ítem o Enunciado	Alternativas y Resultados antes de la Implementación de la interfaz biométrica (valoración máxima puntos 30)		Alternativas y Resultados después de la Implementación de la interfaz biométrica (valoración máxima puntos 30)		Frecuencia Esperada (Fe) Positivas
		SI	**NO**	**SI**	**NO**	
1	¿Puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?	20	10	25	5	81
2	¿Se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?	27	3	29	1	84
3	¿El iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?	27	3	27	3	45
4	¿La identificación única del iris de ojo de cada individuo no es susceptible a suplantación?	5	25	3	27	6
5	¿Puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?	2	28	1	29	4.5
6	¿Se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?	10	20	2	28	45.5

7	¿Se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?	23	7	29	1	73.5
8	¿Puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?	10	20	20	10	16.5
9	¿La tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?	8	22	13	17	33.15
10	¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son posibles de falsificar y alterar?	26	4	3	27	24

Elaborado por: Peñaherrera, Andrés 2020

Tabla 21-4 Cálculo de frecuencias Esperadas con respuesta negativa

N°	Ítem o Enunciado	Alternativas y Resultados antes de la Implementación de la interfaz biométrica (valoración máxima puntos 30)		Alternativas y Resultados despúes de la Implementación de la interfaz biométrica (valoración máxima puntos 30)		Frecuencia Esperada (Fe) Negativas
		SI	**NO**	**NO**	**SI**	
1	¿Puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?	20	10	5	25	9
2	¿Se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?	27	3	1	29	6
3	¿El iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?	27	3	3	27	45
4	¿La identificación única del iris de ojo de cada individuo es susceptible a suplantación?	5	25	27	3	84
5	¿Puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?	2	28	29	1	85.5
6	¿Se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?	10	20	28	2	43.5

7	¿Se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?	23	7	1	29	16.5
8	¿Puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?	10	20	10	20	40.5
9	¿La tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?	8	22	17	13	51
10	¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son posibles de falsificar y alterar?	26	4	27	3	51

Elaborado por: Peñaherrera, Andrés 2020

Tabla 22-4 Tabla de Contingencia

Pregunta	**Fo**	**Fe**	**Fo-Fe**	**$(Fo-Fe)^2$**	**$\frac{(Fo-Fe)^2}{Fe}$**
¿Puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?	25	81	*-56*	*3136*	*38.7*
¿Se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?	29	84	*-55*	*3025*	*36.01*
¿El iris del ojo es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?	27	45	*-18*	*324*	*7.2*
¿La identificación única del iris de ojo de cada individuo es susceptible a suplantación?	3	6	*-3*	*9*	*1.5*
¿Puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?	1	4.5	*-3.5*	*12.25*	*2.7*
¿Se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?	2	45.5	*-43.5*	*1892.2*	*41.58*
¿Se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?	29	73.5	*-44.5*	*1980.25*	*26.9*
¿Puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?	20	16.5	*3.5*	*12.25*	*0.74*
¿La tecnología biométrica del iris del ojo presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?	13	33.15	*-20.15*	*406*	*12.24*

¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos son posibles de falsificar y alterar?	3	24	*-21*	*441*	*18.37*
¿No se puede considerarse a la biometría como una alternativa válida en la seguridad de la información de los sistemas informáticos?	5	9	*-4*	*16*	*-1.7*
¿No se puede reducir los ataques informáticos a la confidencialidad si se utiliza técnicas biométricas de acceso?	1	6	*-5*	*25*	*-4.1*
¿El iris del ojo no es la técnica biométrica más segura de un individuo a ser implementada en sistemas informáticos?	3	45	*-42*	*1764*	*-39.2*
¿La identificación única del iris de ojo de cada individuo es susceptible a suplantación?	27	84	*-57*	*3249*	*-38.67*
¿Si se puede cambiar el código biométrico de un individuo con el tiempo o por otras cuestiones?	29	85.5	*-56.5*	*3192.2*	*-37.3*
¿No se puede instalar una interfaz de acceso biométrico en todos los sistemas informáticos?	28	43.5	*-15.5*	*240.25*	*-5.58*
¿No se puede eliminar las vulnerabilidades a la confidencialidad de la información con la implementación de una interfaz de acceso biométrico?	1	16.5	*-15.5*	*240.25*	*-14.5*
¿No se puede remplazar la técnica biométrica del iris del ojo a las seguridades convencionales implementadas en los sistemas informáticos?	10	40.5	*-30.5*	*930.25*	*-22.96*
¿La tecnología biométrica del iris del ojo no presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones informáticas para ser implementados en diferentes sistemas informáticos que utilizan diferentes lenguajes de programación?	17	51	*-34*	*1156*	*-22.66*

¿Las señales biométricas obtenidas del iris del ojo por el dispositivo EF-45 que se almacenan en la base de datos si son posibles de falsificar y alterar?	27	51	*-24*	*576*	*-11.29*
	TOTAL				*12.02*

Elaborado por: Peñaherrera, Andrés 2020

4.2 Verificación de la hipótesis

En la verificación de hipótesis es necesario utilizar, un estadígrafo conocido como Chi – Cuadrado, este es un método útil para probar las hipótesis relacionadas con la discrepancia entre el conjunto de frecuencias observadas en una muestra y el conjunto de frecuencias teóricas y esperadas de la misma muestra.

Adicionalmente, se establece la hipótesis de investigación *Hi* y la hipótesis nula *Ho* a ser consideradas.

- **Hi:** La implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en los sistemas informáticos.
- **Ho:** La implementación de un modelo de seguridad biométrica no incrementará el nivel de confidencialidad en los sistemas informáticos.

En este tipo de problemas el estadístico de prueba es:

$$X^2 = \Sigma \frac{(Fo - Fe)^2}{Fe}$$

En dónde:

X^2 = Chi-cuadrado
Σ= Sumatoria
Fo = Frecuencia observada de realización de un acontecimiento determinado. (Se puede medir físicamente)
Fe = Frecuencia esperada o teórica. (El resultado que se desea obtener de un experimento)

La aplicación de esta ecuación requiere lo siguiente:

- ✓ Hallar la diferencia entre cada frecuencia observada y la correspondiente frecuencia esperada.
- ✓ Elevar al cuadrado estas diferencias.
- ✓ Dividir cada diferencia elevada al cuadrado entre la correspondiente frecuencia esperada.

- ✓ Sumar los cocientes restantes.

Se utilizó un margen de error del 5% el cual se convierte en un nivel de confianza de 0.05 con el que se buscan los datos en la tabla chi-cuadrado.

El grado de libertad se conseguirá a través de la formula.

$$G1 = (f - 1)(c - 1)$$

Dónde:

- G1= Grado de libertad
- F=Filas
- C= Columnas.

Para conseguir el chi-cuadrado según la tabla se inquirió el grado de libertad y el nivel de confianza y así se logró la chi-cuadrado tabla (Xt) que se compara con el chi-cuadrado calculado (Xc).

De acuerdo con criterio se estableció si el Xc es mayor o igual que el Xt se reconoció la hipótesis de trabajo y se refutó la hipótesis nula.

Si el Xt es mayor que el Xc se rechaza la hipótesis de trabajo y se acepta la hipótesis nula

Hipótesis

La implementación de un modelo de seguridad biométrica incrementará el nivel de confidencialidad en los sistemas informáticos.

- **Variable independiente:** Modelo de seguridad biométrico.
- **Variable dependiente:** Incrementar el nivel de confidencialidad en los sistemas informáticos.

4.2.1 Cálculo de las frecuencias Esperadas

Al existir un solo criterio de clasificación dividido en varias categorías el cálculo de las frecuencias teóricas esperadas es sencillo:

Fe = N/K
N= número de eventos
K=número de oportunidades
En este caso todos tienen la misma oportunidad

Cuando existen dos criterios de clasificación como en nuestro caso (cuadros de doble entrada), la frecuencia teórica de cada casilla es igual al producto de las sumas marginales dividido por el número total de sujetos. En el caso de dos categorías con dos niveles de clasificación (podrían ser más) tendríamos:

Chi-Cuadrado Calculado $X^2c = 12.02$

Ahora Calculamos Chi-Cuadrado Tabla

Grado de libertad

Gl: (f-1) (c-1) **f**= número de filas y **c** = número de columnas
(6-1) (2-1)
(5) (1) = 5

Gl: 5

Nivel de confianza=0.05
Chi-Cuadrado Tabla.

X^2t = **11.07** Valor encontrado en la tabla de probabilidad Chi Cuadrado

$$X^2c = 12.02 > X^2t = 11.07$$

Con estos resultados se comprueba que el chi-cuadrado calculado es mayor que la chi-cuadrado tabla, por lo tanto, se acepta la Hi y se rechaza la Ho, Es decir **"**El diseño e implementación de

una interfaz de acceso mediante un dispositivo biométrico del iris del ojo si mejorará la confidencialidad en los sistemas informáticos”

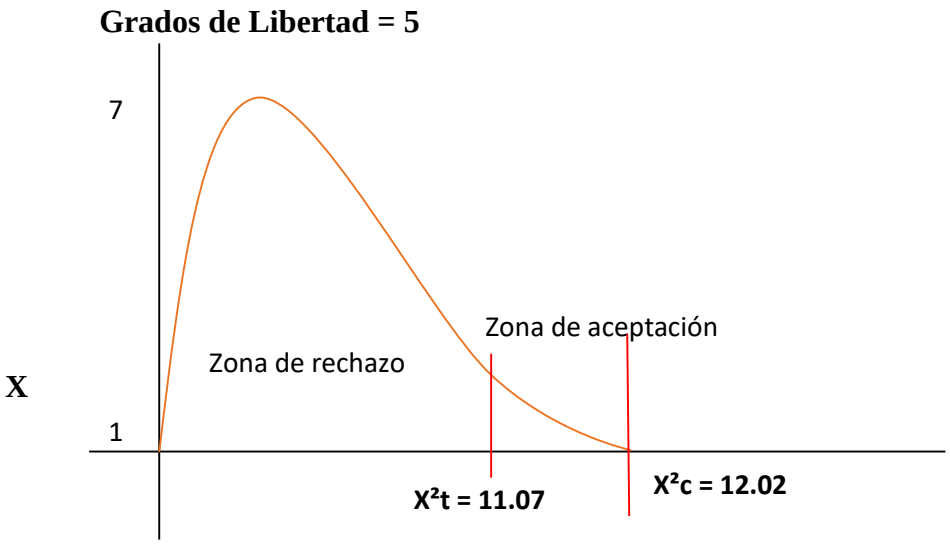


Gráfico 12-4 Comprobación de la Hipótesis

Elaborado por: Peñaherrera, Andrés 2020

V/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

CAPÍTULO V

5. PROPUESTA

5.1 Determinación de la propuesta

En la era digital actual utilizar tecnología biométrica para acceder a los sistemas informáticos, dispositivos electrónicos ya sean móviles o no, lugares restringidos puede parecernos que es cosa de un futuro lejano, pero no estas tecnologías se encuentran entre nosotros desde hace algunos años y son utilizadas en el día a día, en esta investigación se propone la utilización de una de ellas, específicamente se plantea la utilización de un dispositivo biométrico el EF-45 para que recepte las señales de los iris de los dos ojos que se almacena en una base de datos que esté conectada a un sistema informático, luego de cual nos servirá como medio de logueo en la aplicación que se ha implementado la interfaz de acceso.

5.2 Descripción del ef-45

Figura 8-5 EF-45 Lector de iris de ojo

Fuente: https://sticard.com/dload/folleto-IRIS-EF-45.pdf

El sistema de imágenes de iris dual de próxima generación EF-45 proporciona atributos sin precedentes con una facilidad de uso a través de un altamente enfoque de posicionamiento de usuario innovador e intuitivo. Este dispositivo detecta automáticamente al usuario sin necesidad

de contacto físico con el terminal y es tan intuitivos para el usuario como tomarse una fotografía "selfie" con su móvil.

El EF-45 es un escáner de iris dual y rostro para enrolamiento e identificación de personal que puede fungir como control de acceso y asistencia, cuenta con una distancia de escaneo de 35cm a 45cm y cumple con la directiva RoHS de materiales peligrosos. Las imágenes del iris son capturadas con una resolución de 640 x 480 pixeles y puede contener una base de datos de hasta 10,000 sujetos (enrolados con ambos iris). El Lector es capaz de operar con temperaturas de entre 0°C y 40°C, con una humedad relativa de 10% a 90% sin condensación. Requiere una alimentación eléctrica de 110 a 240 V AC y da una salida de 12 V DC a 3.0 A. El EF-45 cuenta con conexiones Wiegand (in/out), RS 232, RS 485, USB, RJ 45, relé de contacto seco y un sistema de LED's indicador para el posicionamiento al momento de capturar. (https://tienda.autentikt.com/ef-45.html)

5.3 Principales características

Tabla 23-5 Principales características del EF-45

	Captura simultánea de imagen facial y reconocimiento de iris dual		Optimizado para control de accesos y presencia, en combinación con tarjeta RFID o PIN
	Detección automática del usuario sin necesidad de contacto físico con el terminal e interfaz de reconocimiento similar a tomar un “selfie” con móvil		Display de detección facial para un correcto posicionamiento del usuario con “deep learning”
	Cámara auto basculante para un ajuste automático del enrolamiento / verificación		Detección automática de caras incluso con máscaras (hospital), gafas de protección, visión o sol, escafandras o velo religioso.

Fuente: https://sticard.com/dload/folleto-IRIS-EF-45.pdf

5.4 Especificaciones técnicas

Tabla 24-5 Características del EF-45

RANGO OPERATIVO	35-45 cm. modo enrolamiento / 30-45 cm. reconocimiento (óptico)
ESTÁNDAR IRIS	ISO 19794-6 2011 estándar de 4.0 lp/mm. al 60% de contraste
TECNOLOGÍAS	Reconocimiento de iris / facial (opcional) / tarjeta MiFare / PIN
RANGO ALTURA	40 cm. (+25º / -20º auto basculante
USUARIOS	10.000 (40.000 opcional)
COMUNICACIÓN	Ethernet (TCP/IP) y USB a PC local soportado Wiegand (I/O), RS-485, RS-232, TTL input y relé
DISPLAY	Pantalla LCD táctil de 5” TFT (480 x 854 pixels)
IDIOMA	Soporte multi lenguaje en pantalla y comandos de voz (consultar)
RANGO TEMPERATURA	-20º a 45º C.
HUMEDAD OPERATIVA	Hasta 95% sin condensación
WIFI (opcional)	Dongle USB WIFI
OPCIONES SDK	C#, .NET y C++ para Windows)
PESO	630 gr. (sin incluir la pletina de montaje sobre la pared)
DIMENSIONES	166 x 166 x 43 mm. (ancho x alto x fondo)

Fuente: https://sticard.com/dload/folleto-IRIS-EF-45.pdf

5.5 Posicionamiento frente al dispositivo ef-45

Además de las características antes mencionadas, contamos con el posicionamiento del usuario frente al dispositivo, con un color para cada acción por ejemplo el color azul significa que se acerque al dispositivo, el color rojo que se aleje y el color verde significa que se encuentra en un

posicionamiento adecuado, después de lo cual las imágenes biométricas del iris se recopilan automáticamente, siempre que se satisfagan las métricas de calidad de imagen en tiempo real.

Figura 9-5 Posicionamiento frente al dispositivo EF-45

Fuente: https://sticard.com/dload/folleto-IRIS-EF-45.pdf

5.6 Componentes de la interfaz de acceso

La interfaz de acceso está programada en C#, el motor de base de datos que utiliza es PostreSql y el lector biométrico del iris de ojos EF-45 que además capta el rostro del usuario.

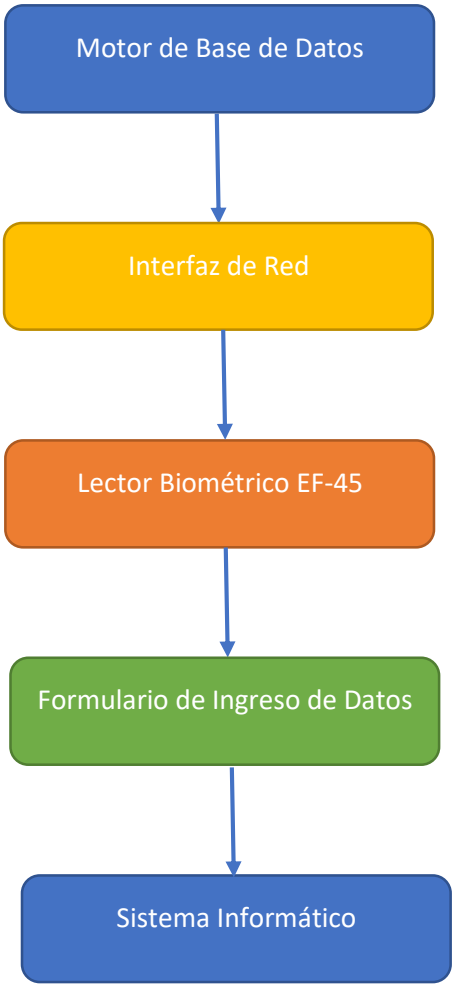


Figura 10-5 Componentes del acceso biométrico al sistema informático

Elaborado por: Peñaherrera, Andrés 2020

5.6.1 Motor de base de datos

El motor de base de datos utilizado es Postgresql, dentro de las varias ventajas podemos enumerar algunas: es de código abierto (open source), multiplataforma, alto volumen es decir puede manejar grandes cantidades de información sin ningún problema, fácil manejo ya que con la interfaz gráfica PgAdmin se puede realizar las operaciones gráficamente, seguridad en la información Hot-Standby permite que los usuarios puedan acceder a las tablas en *modo lectura* mientras que se realizan los procesos de backup o mantenimiento.

5.6.2 Interfaz de red

Para realizar la conectividad entre el EF-45 y la computadora se ha utilizado el protocolo de red IPv4 formado por un cable de red utp categoría 6 directo con direcciones ip 192.168.1.1 en el dispositivo EF-45 y 192.168.1.3 en la computadora, como dato importante se puede mencionar que el dispositivo biométrico tiene como característica adicional una tarjeta inalámbrica para realizar las conexiones de red en caso de así requerirlo.

5.6.3 Lector biométrico de iris de ojo ef-45

Es la parte más importante de la propuesta es un dispositivo de última generación que fue diseñado y construido recién el 2019. El terminal EF-45N es el primer sistema de reconocimiento dual de iris del mercado que emplea el posicionamiento del usuario basado en el reconocimiento facial. Además, ahora incorpora el sensor TOF para una detección aún más rápida y efectiva del sujeto que, junto con el algoritmo para la detección de caras patentado de CMITECH, mejora la experiencia de usuario del EF-45N, haciéndola más rápida, fluida y altamente intuitiva.

5.6.3.1 Funcionamiento

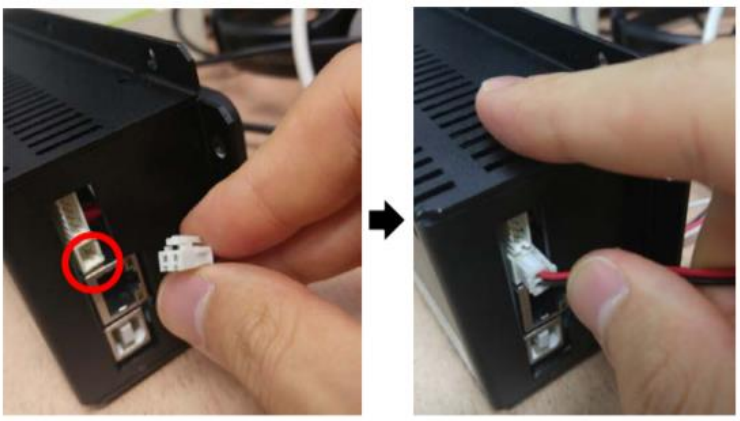


Figura 11-5 Conexión fuente de poder

Fuente: CppWinSDK_forEF45_V1.4.2.2/doc/EF-45M_QuickSetupGuide_20170707.pdf

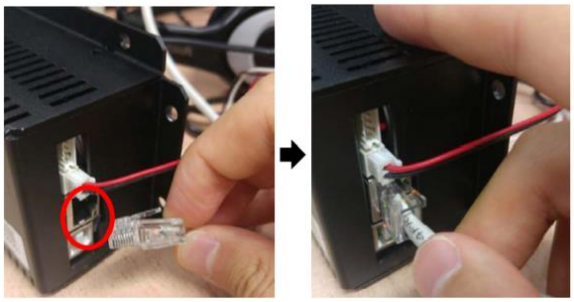


Figura 12-5 Conexión LAN

Fuente: CppWinSDK_forEF45_V1.4.2.2/doc/EF-45M_QuickSetupGuide_20170707.pdf

- Ejecute EF-45 ConfigurationUtility.exe. Haga clic en el botón Buscar del dispositivo y haga clic en la fila que muestra el número de serie del EF-45

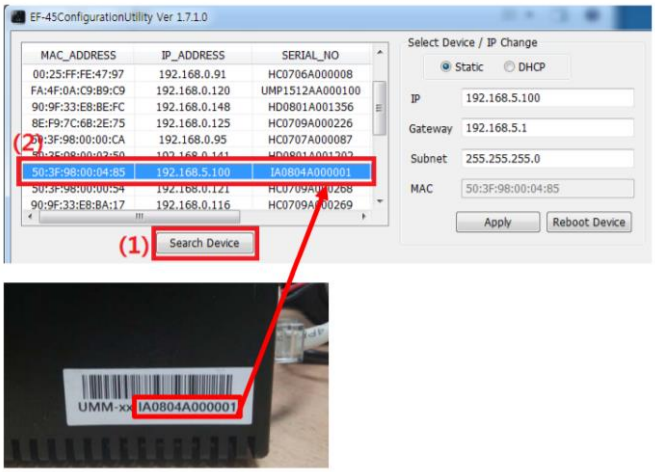


Figura 13-5 Número de serie del dispositivo

Fuente: CppWinSDK_forEF45_V1.4.2.2/doc/EF-45M_QuickSetupGuide_20170707.pdf

- Seleccione DHCP y haga clic en Aplicar si no desea poner un IP estática. Aparecerá el mensaje de éxito de cambio de IP.

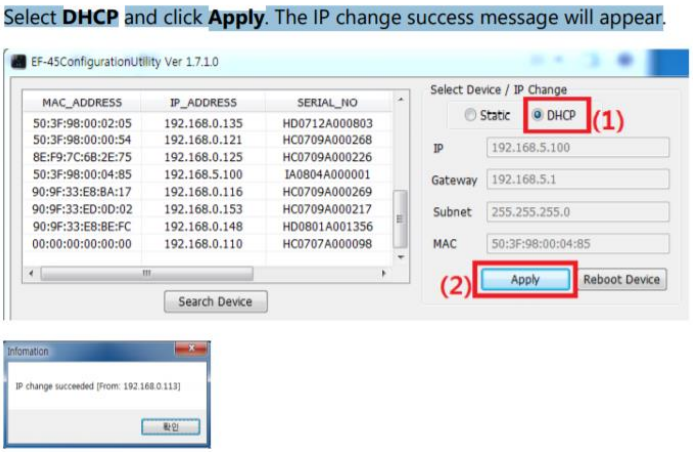


Figura 14-5 Número de serie del dispositivo

Fuente: CppWinSDK_forEF45_V1.4.2.2/doc/EF-45M_QuickSetupGuide_20170707.pdf

5.7 Propuesta del diseño de una interfaz de acceso biométrico para reducir las vulnerabilidades a la confidencialidad en sistemas informáticos.

A continuación, se presenta el algoritmo utilizado para la elaboración de la interfaz de acceso a los sistemas informáticos:

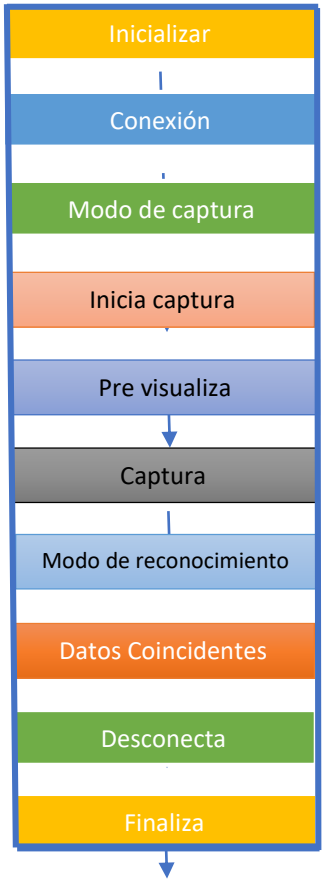


Figura 15-5 Seudo código del funcionamiento de la interfaz de acceso

Elaborado por: Peñaherrera, Andrés 2020

- **Inicializar:** etapa en la que se conecta todos los elementos físicos a utilizar en la propuesta.

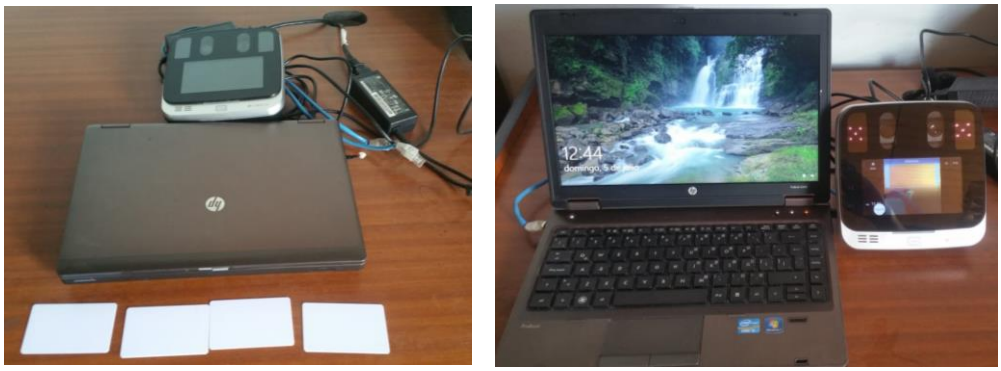


Figura 16-5 Preparación y encendido de los elementos físicos para el acceso biométrico

Elaborado por: Peñaherrera, Andrés 2020

- **Conexión:** en esta fase se digitaliza las IPs en los dos dispositivos que se encuentran en la red, cabe indicar que la conexión se la puede realizar también utilizando un dispositivo más

de red que sirva como switch en caso de la necesidad de conectar varios dispositivos a la vez que redirijan sus datos a la base de datos, las IPs asignadas en esta conexión son 192.168.1.3 para la computadora y 192.168.1.2 para el EF-45.

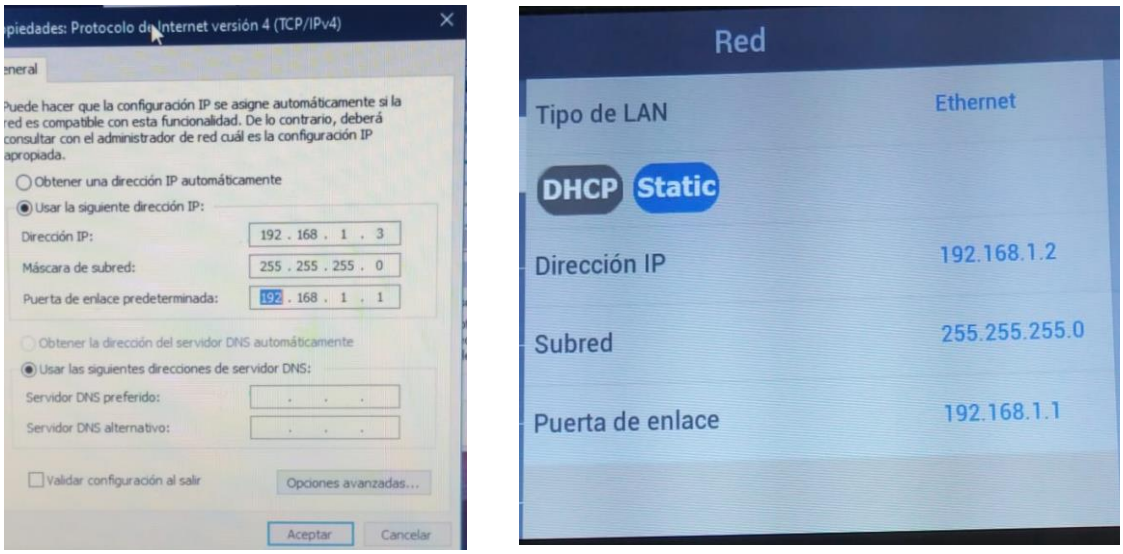


Figura 17-5 Asignación de IPs a los dispositivos de red

Elaborado por: Peñaherrera, Andrés 2020

- **Modo de captura:** el modo de captura nos indica la distancia posición en la que se tiene que ubicar el individuo para lograr receptar las señales de los dos ojos y del rostro.

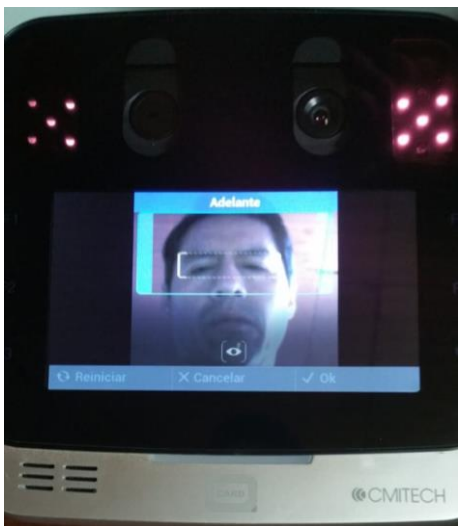


Figura 18-5 Posición ideal para captura de iris de ojo

Elaborado por: Peñaherrera, Andrés 2020

- **Inicio de Captura:** es el momento en que el depósito biométrico EF-45 recepta las señales del iris de los dos ojos y del rostro y los lleva al sistema.

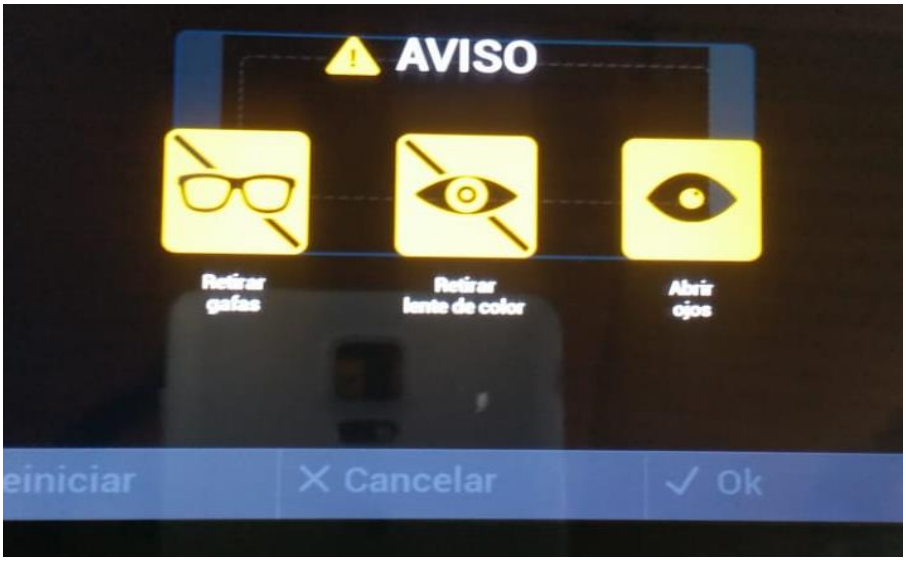
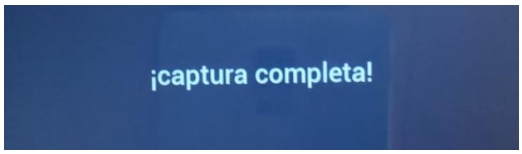


Figura 19-5 Primera pantalla de indicaciones antes de la captura

Elaborado por: Peñaherrera, Andrés 2020

Figura 20-5 Captura de iris

Elaborado por: Peñaherrera, Andrés 2020



- **Pre visualiza en la interfaz de acceso:** una vez que el dispositivo ha capturado las señales del iris y del rostro las lleva a través de la red a la interfaz de acceso biométrica.

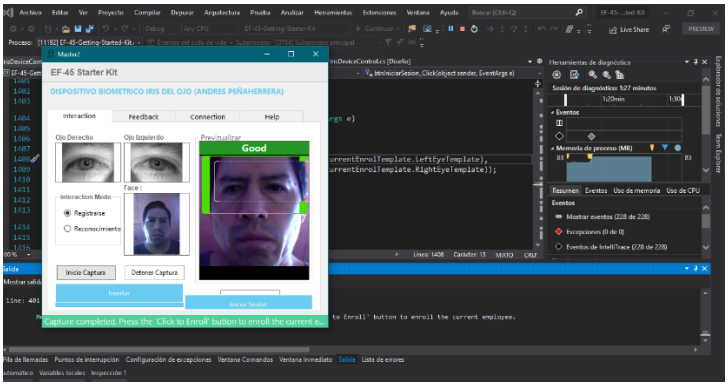


Figura 21-5 Captura del iris y rostro en el sistema interfaz de acceso

Elaborado por: Peñaherrera, Andrés 2020

- **Captura las imágenes del dispositivo y los lleva al sistema:** en este paso ya se almacena la información capturada en la base de datos.

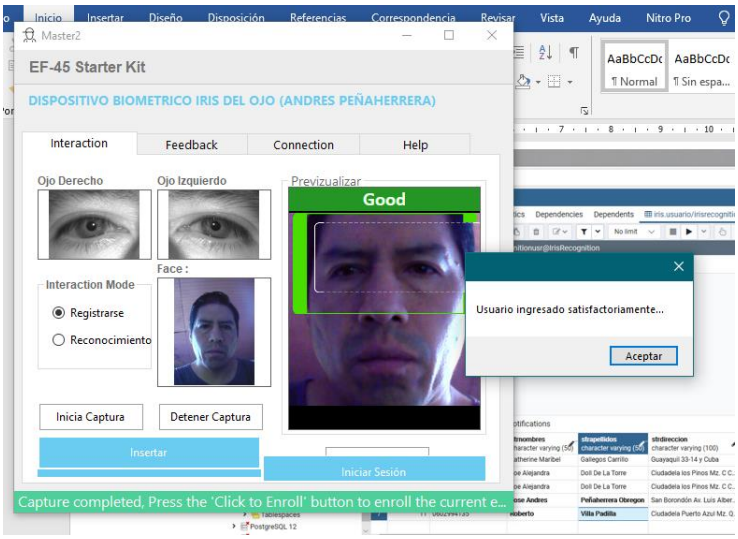


Figura 22-5 Datos almacenados satisfactoriamente

Elaborado por: Peñaherrera, Andrés 2020

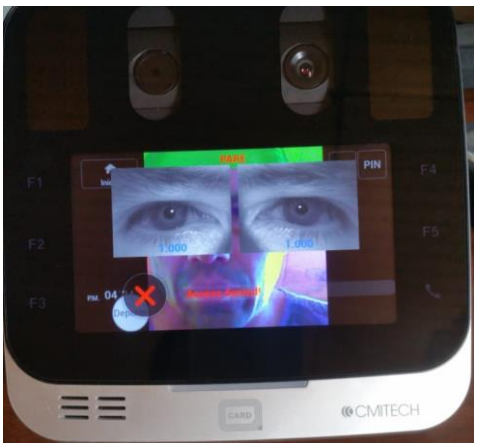


Figura 23-5 Captura errónea

Elaborado por: Peñaherrera, Andrés 2020

- **Modo de reconocimiento:** este es el momento en que la interfaz de acceso compara los datos del usuario que se encuentra en la captura con los datos registrados en la base de datos y compara si tienen coincidencias.

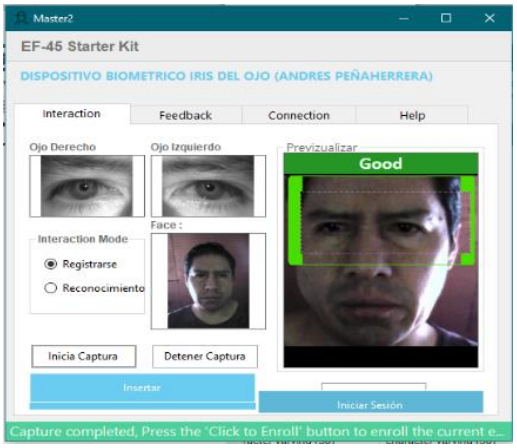


Figura 24-5 Compara coincidencias

Elaborado por: Peñaherrera, Andrés 2020

- **Datos coincidentes:** verifica si existe en la base de datos elementos iguales para permitir el acceso al sistema informático en la que se encuentre instalado este módulo.

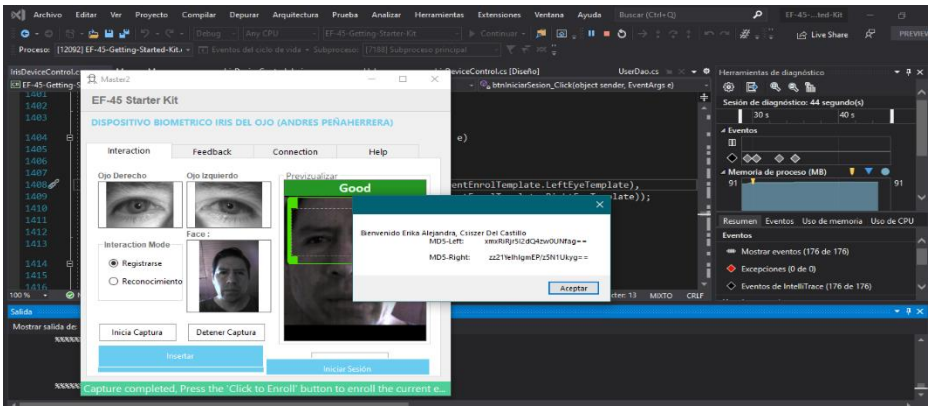


Figura 25-5 Logueo exitoso

Elaborado por: Peñaherrera, Andrés 2020

A continuación, se presenta los tipos de datos que se almacena en la base de datos haciendo imposible el hackeo de estos ya que son de tipo bytea

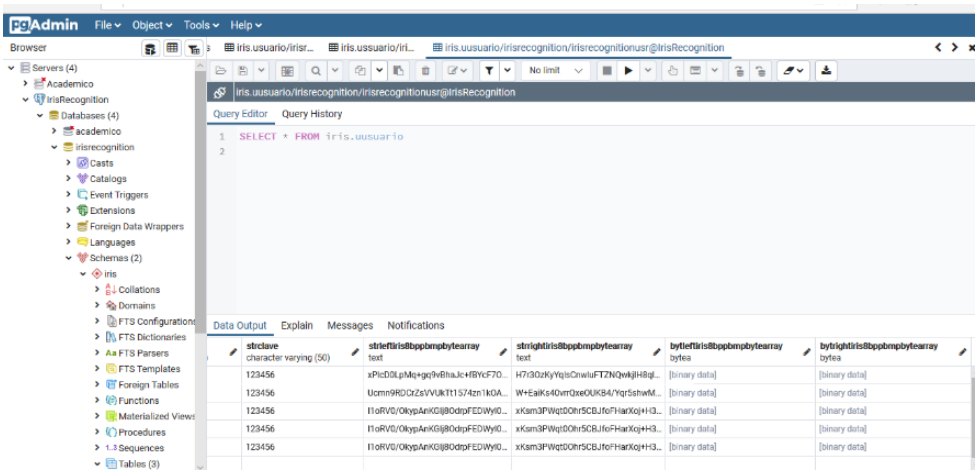


Figura 26-5 Cómo se almacena la información en la base de datos

Elaborado por: Peñaherrera, Andrés 2020

CONCLUSIONES

- Según el estudio realizado se puede concluir que el iris del ojo es una de las características biométricas más seguras que se puede obtener del ser humano en comparación con las demás características.

- El iris del ojo posee varios parámetros que le convierten en el órgano ideal para interactuar con los dispositivos biométricos, de fácil interacción, no cambia con la edad, acceso visual a través de la retina, cubierto por la córnea lo que conlleva a permanecer siempre intacto.

- El dispositivo biométrico EF-45 es una de las mejores alternativas para la recepción de señales biométricas del iris del ojo ya que no exige una posición estricta para captar los datos del individuo, además de ser de fácil uso y poseer tecnología de punta y actualizada.

- Existe poca información referente al funcionamiento del EF-45 en los sistemas informáticos, siendo el principal limitante en las aplicaciones, que solo cuenta con librerías dll para la conexión con el sistema operativo con el lenguaje de programación c#.

RECOMENDACIONES

- Se recomienda realizar una difusión masiva a todas las empresas particulares y gubernamentales sobre la utilidad y utilización de la interfaz de acceso biométrico indicando que con bajo costo se puede eliminar casi por completo el robo de credenciales de todos los funcionarios de las instituciones.

- Al momento de decidirse por una tecnología biométrica se recomienda utilizar el iris del ojo del ser humano, ya que su nivel de vulnerabilidad es menor que las demás partes del cuerpo que se puede utilizar como identificación de identidad.

- La inversión en un dispositivo biométrico en este caso para el iris del ojo se justifica por completo ya que al no necesitar de una interacción física con el usuario precautelamos la propagación de gérmenes entre usuarios.

- Se ínsita a seguir con la construcción de la interfaz de acceso biométrica a ser implementada en los sistemas informáticos con la premisa de que puede ser migrado a un lenguaje de código libre como java por ejemplo y con eso evitarnos el pagar licencias por los IDE utilizados.

BIBLIOGRAFÍA

Abdu Gumaei, R. S.-S. (2019). Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. *Journal of Parallel and Distributed Computing*.

Alaa S. Al-Waisy, R. Q.-F. (2015). A Fast and Accurate Iris Localization Technique for Healthcare Security System. *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*.

Ávila, C. (2012). *Aplicaciones de la Biometría a la Seguridad.* Obtenido de http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf

Castro, C. (Diceimbre de 2017). MODELO DE SEGURIDAD PARA GARANTIZAR . Ecuador. Recuperado el Septiembre de 2019, de http://dspace.espoch.edu.ec/bitstream/123456789/7842/1/20T00952.pdf

Chiavenato, I. (2018). *Administración de recursos humanos.* Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/458/1/T-UTC-1027.pdf

CMITECH. (Febrero de 2019). *CMI-TECH*. Obtenido de https://www.cmi-tech.com/wp-content/uploads/2018/06/cmitech-data_sheet-ef-45-2019.pdf

Cohn, M. (2007). Biometrics: Key to securing consumer trust. *Biometric Technology Today*, 8-9.

CORTÉS, J., & MEDINA , F. (Diciembre de 2010). *SISTEMAS DE SEGURIDAD BASADOS EN BIOMETRÍA.* Obtenido de SECURITY SYSTEMS BASED ON BIOMETRICS : https://www.redalyc.org/pdf/849/84920977016.pdf

David Menotti, G. C. (2015). Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. *IEEE Transactions on Information Forensics and Security*.

Hernàndez Reyes, J. C. (Diciembre de 2016). *AUTENTICACIÓN BIOMÉTRICA A TRAVÉS DE HUELLAS DIGITALES E IRIS EN UNA EMPRESA INDUSTRIAL.* Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/64996/JUAN%20CARLOS%20HERN%C3%81NDEZ%20REYES-split-merge.pdf?sequence=3&isAllowed=y

Hugo Proença, J. C. (2018). A Reminiscence of "Mastermind": Iris/Periocular Biometrics by "In-Set" CNN Iterative Analysis. *IEEE Transactions on Information Forensics and Security*.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2016). *Tecnologías biométricas aplicadas a la ciberseguridad.* Obtenido de

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Laura Florian Cruz, F. C. (2006). RECONOCIMENTO DEL IRIS. *TÓPICOS ESPECIALES EN PROCESAMIENTO GRÁFICO*.

M. R. Rajput, G. S. (2018). Iris Biometric Technique for Person Authentication Based on Fusion of Radon and 2D Multi-Wavelet Transform. *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*.

Md. Sabbir Ejaz, M. A. (2018). Performance Comparison of Partition Based Clustering Algorithms on Iris Image Preprocessing. *2017 2nd International Conference on Electrical & Electronic Engineering (ICEEE)*.

N.K. Ratha, J. C. (2001). Enhancing security and privacy in biometrics-based. *IBM Systems Journal*.

NUO. (20 de mayo de 2015). *Reconocimiento de iris y escaneo de retina.* Obtenido de Reconocimiento de iris y escaneo de retina: https://nuoplanet.com/blog/reconocimiento-de-iris-y-escaneo-de-retina/

P. Steffi Vanthana, A. M. (2015). Iris authentication using Gray Level Co-occurrence Matrix and Hausdorff Dimension. *2015 International Conference on Computer Communication and Informatics (ICCCI)*.

Pricop, E. (2019). Biometrics the secret to securing industrial control systems. *Biometric Technology Today*.

Virginio Cantoni, N. N. (2017). Capítulo 9 - Autenticación biométrica para acceder a áreas controladas a través del seguimiento ocular. *Reconocimiento humano en entornos sin restricciones*.