Percepciones y Desafíos en la Adopción de Biometrías: Un Enfoque Integral desde la Población Estándar y la Perspectiva de Expertos en Identidad Digital en Colombia

Elaborado por:

Ricardo Sánchez Sepúlveda

Jackson Alejandro Sierra Ortiz

Universidad EAN

Especialización Gerencia de Proyectos

Seminario de Investigación de Pregrado

Bogotá

27/11/2023

Tabla de contenido

Planteamiento del Problema

En la actualidad, Colombia ha crecido favorablemente hacia el comercio electrónico (LaRepublica.co, 2022), debido a las necesidades para el acceso de adquisición de productos y/o servicios de manera virtual o interacción no presencial, donde la pandemia por Covid-19 fue el principal actor para la aceleración de incorporar nuevos tipos de servicios digitales, como también para que el consumidor empezar a interactuar con ellas; debido a esta situación, el consumidor, de modo mandatorio, inicio el viaje a la inclusión del comercio electrónico, para poder adquirir servicios y/o productos de forma virtual.

Sobre lo anterior en Colombia, el Estado ha establecido marcos legales (MinTIC, 2023), para incorporar y promover el uso herramientas de seguridad, protección y confianza para ser aplicadas a las soluciones de comercio electrónico; con el objetivo de que los procesos de identificación y autenticidad a los usuarios que ingresan a estas plataformas tengan la mayor capa de seguridad de protección de la identidad digital al realizar sus transacciones. Sin embargo los emprendedores, los fabricantes y dueños de estas aplicaciones, no incorporan estas herramientas ya sea por múltiples variables, como el desconocimiento de estas herramientas, por evitar un incremento en el precio del servicio, como también captura sin incluir buenas prácticas de seguridad, como la omisión de responsabilidad del usuario final o consumidor de ceder este tipo de sus datos, desconociendo los derechos que ofrece el Estado de protección y seguridad a realizar sus transacciones electrónicas, entregando su información pública o privada a un tercero que no controla y protege esta información; como ejemplo la ley 1581 de 2012, que relaciona la protección de datos personales, es una herramienta legal que tiene el consumidor, que por la omisión de este derecho al no leer o entender que reglas está permitiendo usar su información sin control, antes de aceptar los términos y condiciones al querer tener acceso al uso de las aplicaciones móviles.

Como consecuencias, la información del consumidor que lo llamaremos en adelante Metadato puede ser administrada sin ningún otro consentimiento por el tercero, llegando a ser vendido el a otras organizaciones o llegar al punto de vulnerabilidad que permitan ser hurtados digitalmente, usando esta información para hacer fraudes (TransUnion, 2022), como la suplantación de identidad.

Lo anterior identifica el problema desde el usuario final, pero también queremos llegar a que este tipo de novedades aplica para los fabricantes de estas aplicaciones móviles, porque al no implementar soluciones legales y tecnológicas para la identificación y autenticación de los usuarios que están registrando, también son vulnerables al fraude y robo información sensible que están recolectando, llegando a tener penalidades severas con el Estado por no proteger este tipo de información, haciendo que sus negocios no sean sostenibles por temas de seguridad y pago de penalidades legales.

Descripción del problema.

La identificación y autenticación de usuarios es un mecanismo realizado por la mayoría de aplicaciones móviles, como inclusión de buenas prácticas para la seguridad en el comercio electrónico, por ello los usuarios para el acceso a ellas es necesario realizar este tipo de registros con ayuda de mecanismos de autenticación; debido a ello las aplicaciones móviles deben asegurarse que los mecanismos de autenticación que utilizan no sólo sean resistentes a los ataques, sino también fáciles de usar, escalables y rentables (Anani & Ouda, 2017); y de ahí se identifica la necesidad de incluir una investigación con una metodología cualitativa, porque los mecanismos usados actualmente en Colombia, no protegen completamente el metadato del usuario y usan procesos de autenticación manuales para validar que la persona es la que dice ser, y por ello la Registraduría Nacional del Estado Civil (RNEC), está a próximo a ejecutar el proyecto donde la validación de la autenticación se hará por reconocimiento facial, aplicando procesos automáticos, simplificando los riesgos de fraude o robo de identidad

(Portafolio, 2023), de ahí debemos identificar sus ventajas y viabilidad de implementación a las aplicaciones móviles que se usan en Colombia.

Pregunta de investigación.

¿Cuáles son los desafíos que se presentan para implementar mecanismos de identificación y de autenticación en aplicaciones móviles de manera que se evite la suplantación y la pérdida de datos?

Objetivo general.

Evaluar la percepción y comprensión de la población estándar sobre las biometrías, así como identificar sus inquietudes y expectativas en el contexto de la identidad digital, contrastando estos hallazgos con la perspectiva de expertos en identidad digital en Colombia.

Objetivos específicos.

- Explorar el entendimiento de la población estándar sobre los mecanismos de seguridad biométrica en aplicaciones móviles, específicamente la biometría facial.
- Identificar cuál es la comprensión de términos y usos relacionados con la protección de la identidad por parte del usuario final.
- Investigar el cambio de tendencia en la percepción del usuario final desde un interés inicial positivo hacia una preocupación, analizando posibles factores influyentes.
- Identificar las inquietudes de los usuarios en relación con el uso de la biometría facial en aplicaciones móviles.
- Evaluar la importancia y desafíos en la implementación de métodos biométricos, con énfasis en la biometría facial en aplicaciones móviles.
- Comparar las conclusiones obtenidas de la población estándar con las conclusiones extraídas de las entrevistas a expertos e Identificar áreas de concordancia y discrepancia entre las percepciones de estos dos grupos.

- Evaluar la viabilidad de la biometría facial como identidad digital en el contexto colombiano, considerando tanto las percepciones de la población estándar como las recomendaciones de expertos.

Justificación

En la actualidad, nosotros como consumidores de productos y servicios, buscamos alternativas de canales para el acceso a ellos de modo remoto o virtual, ya sea por temas de bioseguridad o por evitar desplazamientos de distancias largas para acceso de lo requerido (que se localiza fuera de la ciudad, departamento o país), tramites y pagos de servicios como otros. Gracias a estas necesidades el mercado brinda diferentes opciones para estos accesos con ayuda de los dispositivos móviles, que permiten que, desde cualquier lugar y momento, se pueda hacer revisión, operación, solicitud o compra de algún producto y servicio; donde lo que se requiere es validar que el usuario que está realizando el trámite o solicitud del bien o servicio, es quien dice ser protegiendo la privacidad de su identidad, es a ello que se le conoce como la Identidad Digital.

Por lo anterior es importante que no se minimice la importancia de la Identidad Digital, dado a que es un valor intangible que identifica y autentica al usuario en la virtualidad, y que debe ser protegida como cualquier credencial física que le da una validación de existencia a la persona, para evitar suplantaciones o fraude. Con estas bases, en la investigación se profundizará tres pilares importantes para la protección de la identidad digital, que son la Identificación, la autenticación y la legalización, donde se tomará como metodología las buenas prácticas de la normativa ISO 27000, utilizando herramientas de identificación y autenticación como la biometría facial, pero siendo cotejado antes las bases de la Registraduría Nacional de Estado Civil (RENEC).

Marco Teórico

Antecedentes

Siguiendo la línea de la investigación sobre la identidad digital, se debe tener en referencia que es necesario incluir un componente o una característica que aplique como una prueba no repudiable para autenticar la identificación del usuario, y por ende este tipo de componente no se viene aplicando en decanas sino en siglos atrás (Alicebiometrcis.com, 2021), donde no había tecnología digital, y la comunicación a distancia era muy interpersonal, que era necesario aplicar estrategias de identificación para hacer tramites comerciales, contratos, ordenes militares y otro tipo de documentos que tenían que viajar largas distancias y validar la autenticidad de ellos o de la persona que los envió, con ello sus primeras implementaciones eran usando sellos distintivos de familias reales o que identificaban las compañías, acompañadas con una huella dactilar tomada con tinta, donde se brindaba una capa de seguridad de validación en esas épocas.

Ya con el paso del tiempo, evolucionaron las investigaciones para nuevas aplicaciones de identificación y autenticación, como obras de arte ya sea plasmando el rostro de la persona un una pintura o escultura, pero era una herramienta fácil para los usuarios identificar y relacionar estos componentes con la persona que se desea identificar, por ello a continuación se describe una línea de tiempo sobre las investigaciones que se realizaron hasta la fecha, donde es un punto importante para las actividades que realice el usuario:

línea de tiempo de la historia de la biometría (biometricuodate.com, 2018)**:**

- 1858 – Se registra la primera captura sistemática de imágenes de manos con fines de identificación.
- 1883 – Twain escribe sobre las huellas dactilares en “La vida en el Mississippi”.
- 1870 – Bertillon desarrolla antropometrías para identificar individuos.
- 1892 – Galton desarrolla un sistema de clasificación de huellas dactilares.

- 1896 – Edward Henry desarrolla un sistema de clasificación de huellas dactilares.
- 1903 – Las prisiones estatales de Nueva York comienzan a utilizar huellas dactilares.
- 1903 – El sistema Bertillon colapsa, porque no se podían diferenciar gemelos.
- 1936 – Se propone el concepto de utilizar el patrón del iris para la identificación.
- Década de 1960: el reconocimiento facial se vuelve semiautomático.
- 1965 - Comienza la investigación sobre el reconocimiento automatizado de firmas.
- 1969 – El FBI presiona para que el reconocimiento de huellas dactilares sea un proceso automatizado.
- 1975 – El FBI financia el desarrollo de sensores y tecnología de extracción de minucias.
- 1976 – Se desarrolla el primer prototipo de sistema de reconocimiento de hablantes.
- Década de 1980: se establece el NIST *Speech Group*.
- 1986 – Se publica el estándar de intercambio de datos sobre minucias de huellas dactilares.
- 1992 – Se establece el Consorcio Biométrico dentro del gobierno de EE. UU.
- 1998- El FBI lanza COOLS (base de datos forense de ADN).
- 1999 – Los componentes principales del IAFIS del FBI entran en funcionamiento.
- 2002 – Se establece el comité de normas ISO/IEC sobre biometría.
- 2008 – El gobierno de EE. UU. comienza a coordinar el uso de bases de datos biométricas.
- 2011 – Identificación biométrica utilizada para identificar el cuerpo de Osama Bin Laden.

Con lo anterior sobre la línea de tiempo se va identificando desde inicio del siglo XX que para gobiernos como los Estados Unidos junto al FBI, la aplicación de la biometría no era solo aplicable para tramites comerciales, sino para poder ser aplicado para identificar a todos los ciudadanos y crearles un perfil, que por medio de un dato biográfico, se

tenga el histórico de vida de cada uno hasta identificarlos con solo tomar una foto y enviarlo por la Internet y validar su identidad desde lugares remotos, viendo la necesidad de creación de leyes y normativas que regulen este tipo de consulta, identificación, autenticación con seguridad hacia la identidad de la persona.

Conceptos

Identidad Digital

Como se ha mencionado anteriormente, el rápido crecimiento del internet y el uso de las aplicaciones digitales en las que los usuarios cada vez más interactúan para realizar procesos que antes se hacían únicamente de forma presencial, ha creado la necesidad de implementar bases para la construcción de las identidades digitales. Nos referimos a identidades digitales como la representación única de un sujeto en el momento de hacer una interacción digital (Paul A. Grassi, 2017).

A ese concepto de identidad digital, se le puede agregar que dicha representación incluye una cantidad considerable de datos que van más allá de simple información. He aquí donde la concepción de Metadato resulta importante para la construcción de este documento y más adelante se trabajará sobre dicha idea.

Hasta acá es claro entender la importancia de la identidad digital y lo seguro que deben ser los mecanismos que se usen para verificarla. En un mundo casi completamente digitalizado el manejo de las identidades digitales no se puede tomar con ligereza y eso está claro para las entidades privadas y públicas que las manejan.

Metadatos

Dentro nuestra investigación, la palabra metadatos se repite varias veces por lo que es importante definir el significado que más aplica. Con la evolución de la tecnología, la recopilación de datos pasó a ser un factor fundamental para las empresas, al punto de ser la venta de éstos una de las formas de obtener ganancias de muchas empresas del sector de la

tecnología ya que la información de la persona es clave para el desarrollo de productos y de cómo estos se van a publicitar. El concepto de Metadato no tiene un significado unificado, por lo que debemos guiarnos por el contexto sobre el que se está hablando. En el artículo de Mayernik, Matthew en la publicación con título *Metadatos* (Mayernik, 2023) podemos encontrar las siguientes definiciones, que como él dice, pasan de muy específicas a muy genéricas:

** Greenberg (2003, p. 1876): "datos estructurados sobre un objeto que posibilitan funciones asociadas al objeto designado".*

** Greenberg (2005, p. 20): "atributos de datos que describen, aportan contexto, indican la calidad, o documentan características de otro objeto (o dato)".*

** Smiraglia (2005, p. 2): "descripciones estructuradas de recursos de información, diseñadas para potenciar la recuperación de información".*

** Gilliland (2008, n.p.): "la suma total de lo que se puede decir de cualquier objeto informativo a cualquier nivel de agregación".*

** Pomerantz (2015, p. 26): "Los metadatos son declaraciones sobre un objeto potencialmente informativo".*

El autor también menciona definiciones utilizadas en ámbitos más específicos como en contextos ambientales y geográficos (Mayernik, 2023):

** Michener et al. (1997, p. 331): "Información de alto nivel o instrucciones que describen el contenido, contexto, calidad, estructura y accesibilidad de un conjunto de datos concreto".*

** Fegraus et al. (1005, p. 159): "aquella información que describe el quién, el qué, el dónde, el cuándo, el por qué y el cómo, sobre la recogida de un conjunto de datos ecológicos".*

** Danko (2012, p. 360): "datos que describen la información de forma que pueda ser útil y tener valor, ser entendida y permitir la colaboración".*

** Gordon y Habermann (2018, p. 38): "contenido bien definido en representaciones estructuradas que lo hacen más fácil de compartir y descubrir".*

De lo anterior confirmamos que el concepto es muy amplio y abarca diferentes significados que dependen de los temas a tratar. En este documento vamos utilizar la definición descrita en la norma NE-ISO 23081-1: 2008 y explicada por (Yopazá, 2020); los metadatos son *"información estructurada o semi estructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo*". Esta definición es la que más permite acercarse de una forma estructurada a los objetivos que este documento trata, donde la identidad digital, los aspectos legales y las metodologías de autenticación e identificación será los temas principales.

Biometría

Según Luther Martin la biometría es *"el análisis de observaciones y fenómenos biológicos"* (Martin, 2009). Otra definición se encuentra en *Handbook of statistics:* "*La biometría es la ciencia de reconocer automáticamente a las personas en función de las características físicas o de comportamiento, como la cara, la huella digital, el iris, la mano, la voz, la marcha y la firma"* (D.A. Reid, 2013). Hoy en día se utiliza la biometría para reconocer a otras personas, normalmente utilizando la forma de una cara o el sonido de una voz para hacerlo. Más específicamente en el campo de la tecnología la biometría es usada para el reconocimiento e identificación de una persona por medio de procesos automatizados. De esta forma, el manejo de los datos biométricos se debe llevar con mucha responsabilidad ya que son datos que no se pueden cambiar en caso de pérdida, por ejemplo, al perder la información de una contraseña una de las soluciones de seguridad es cambiarla por una con una con mayor cantidad de caracteres. Esto no sucede con un dato biométrico, la información de la huella por ejemplo no es posible cambiarla.

Métodos actuales

Para entender que métodos se aplican para la captura de datos biométricos y relacionarlos al metadato, es importante tener el concepto básico sobre la biometría que es un análisis de las características o del comportamiento propia de cada persona para ser autenticado, y por ello hay dos métodos para la validación de la biometría, que son las mediciones fisiológicas y las mediciones del comportamiento (*ThalesGroup*, 2023).

"Mediciones Fisiológicas: Pueden ser morfológicas o biológicas. Los análisis morfológicos, consisten, principalmente, en las huellas dactilares, la forma de la mano, del dedo, el patrón de las venas, el ojo (iris y retina) y la forma de la cara.

Los análisis biológicos, el ADN, la sangre, la saliva o la orina pueden usarse por parte de los equipos médicos y la policía forense" (*ThalesGroup*, 2023).

"Mediciones del Comportamiento: Las formas más comunes son el reconocimiento de voz, la dinámica de la firma (velocidad de movimiento del bolígrafo, aceleraciones, presión ejercida, inclinación), la dinámica de la pulsación de las teclas, la manera en que se utilizan los objetos, la marcha, el sonido de los pasos, los gestos, etc." (*ThalesGroup*, 2023).

Teniendo en referencia lo mencionado anteriormente, los métodos aplicados actualmente para la captura de las biometrías son:

1. Identificación de la Huellas Dactilares (Método huellas dactilares, 2021): Reconocimiento del usuario tomando información desde las huellas digitales.
2. Reconocimiento de Iris (Método reconocimiento de iris, 2023): Reconocimiento del usuario tomando información desde la captura de información del Iris de los ojos.
3. Reconocimiento Facial (Método reconocimiento facial, 2021): Reconocimiento del usuario tomando información desde la captura de la forma del rostro o cara.

4. Reconocimiento de patrones de venas (Método reconocimiento patrones venas, 2021): Reconocimiento de patrones de las venas, o donde termina la vena en un sitio del cuerpo humano.
5. Reconocimiento de voz (Método reconocimiento de voz, 2020): Reconocimiento del usuario tomando información desde la captura del sonido emitido por la voz.

Aunque se explicaron las dos mediciones principales, la investigación se centrara en la medición física analizando el método de identificación de la cara (Biometría Facial) y consultado con la base de datos de la Registraduría Nacional del Estado Civil (Registraduría Nacional del Estado Civil, 2023).

Estado del arte

Ejemplo del uso de la identidad digital en Estonia y Países bajos

Profundizando en mayor medida en el concepto de identidad digital podemos poner ejemplos de países que han dado un mayor significado a este concepto. Estonia, desde el 2002 (MONDRAGÓN, 2020), implementó una política de modernización que ha impulsado la identidad digital a otros niveles. El país europeo fue pionero en implementar sistemas completamente digitales para la aplicación de la mayoría de los tramites gubernamentales, de forma que fue necesaria la implementación de una identidad digital por medio de diferentes tipos de identificaciones electrónicas (e-ID). Estonia ha desarrollado dicho sistema por medio de una alianza publico privada donde el sector público se encarga de identificación personal, gestión de identidad, gestión de infraestructura de identificación electrónica y actividades de supervisión y el sector privado de ofrecer tokens de identificación electrónica (e-ID), así como servicios de personalización y confianza.(Lips, 2020).

Dicho desarrollo digital fue una importarte implementación que facilitó los trámites del gobierno y que benefició al comercio en general. Acorde a estadísticas de año 2020, más de 1.35

millones de personas utilizaban e-ID (Lips, 2020), un porcentaje considerablemente alto en comparación a la población total del país. En el informe de (Valentyna Tsap, 2020) se encontró que el 50% de las personas encuestadas utilizan los sistemas de identificación y autenticación del gobierno a diario, el 29% varias veces a la semana y el resto de los encuestados por lo menos una vez al mes. El informe también concluye que la confianza y la conciencia de los ciudadanos son factores que contribuyen a la aceptación pública de estas tecnologías.
De la misma manera, Países bajos ha sido otro estado de la unión europea que ha implementado este tipo de tecnologías y que según (Lips, 2020) ha tenido muy buenos resultados, cerca del 80% (14 millones de personas) de la población neerlandés usa el sistema y más de 650 proveedores de este tipo de servicios están conectado con el servicio del gobierno. Según el informe el servicio del gobierno procesa cerca de 300 millones de autenticaciones al año (Lips, 2020).

En el caso de e-ID de Estonia y de Países Bajos, es interesante ver los resultados en ahorro de tiempos y presupuesto de la nación. Se disminuye el tedioso papeleo causado por la burocracia de los procesos y es una excelente forma de acelerar los procesos. Por otro lado, es claro que este tipo de sistemas conllevan posibles riesgos que se deben tratar con mucho cuidado, muchos de ellos relacionados con la seguridad de los sistemas e igualmente con la dificultad que implica la implementación de los mismos. Para los sistemas de digitales (*eIDAS*) de ambos países se han evidenciado los siguientes problemas que en caso de querer desarrollar estos sistemas en Colombia se deberán tener en cuenta; falta de supervisión de los sistemas, falta de un marco para la evaluación de la conformidad a nivel de la UE, No existen reglas comunes para los órganos de control (Lips, 2020). Estos inconvenientes se presentan tanto para los ciudadanos como para los funcionarios del gobierno y las empresas implicadas. Por lo que es fundamental tenerlos presentes en su desarrollo.

En cuanto a la seguridad de los sistemas y las metodologías usadas, Estonia utiliza la tecnología de *Blockchain* para mantener los datos de los usuarios protegidos y sin riesgo a pérdidas de información; evento que sería fatal para su gobierno, usando como métodos de identificación los siguientes seis tokens de e-ID: tarjeta de identificación, tarjeta de permiso de residencia, tarjeta de identidad digital, tarjeta de identidad digital de residencia electrónica, identificación móvil y tarjeta de identidad diplomática.

En el caso de Colombia

Es claro que el manejo de esta cantidad de metadatos relacionados con la información biométrica de los ciudadanos de un país requiere de procesos supremamente seguros, ya que constantemente estarán sufriendo intentos de ataques cibernéticos para lograr el robo de la información.

Es por esto que para los Estados y grandes organizaciones como la ONU; la ciberseguridad es uno de los objetivos de desarrollo sostenible, son conscientes de los peligros asociados y han desarrollado marcos sobre los que se deben trabajar. En muchos grupos económicos de países como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), se solicita a sus participantes el cumplimiento de diferentes guías para el cumplimiento de marcos de seguridad. Según (Chenou, 2021) los gobiernos deben ser muy cuidadosos a la hora de seguir estos lineamientos, ya que cada caso es diferente y el seguir estas guías definirá cómo será el manejo de la seguridad de la información de todos los ciudadanos. Es el caso de Colombia, uno de los primeros países en cumplir con los lineamientos propuestos por la ODCE (2015), hecho que ha creado el debate de si al seguir esta guía no se perdió la oportunidad de diseñar una política de consolidación de la paz cibernética en un contexto de posconflicto (Chenou, 2021).

A pesar de que la ciberseguridad ha sido un tema en la agenda del gobierno, el país ha sufrido de múltiples ataques a entidades públicas y privadas que han resultado en la pérdida de información. Es el caso de Sanitas donde el ataque generó una profunda crisis para la entidad y más grave aún, la pérdida de información personal de sus afiliados. Más recientemente el ataque realizado a la empresa privada *IFX Networks*, caso que ha afectado más de dos millones de procesos judiciales hasta la fecha (Vásquez, 2023) y que seguramente tendrá implicaciones trascendentales en las futuras decisiones políticas; en este momento se está decidiendo en el congreso la creación de un ala del ministerio de defensa encargada de la ciberseguridad.

Marco Legal

Con el crecimiento de uso de la biometría para la identificación de usuarios, el metadato está en el centro de atención para sufrir ciberataques y con ello, la perdida de los datos y privacidad, debido a ello cada país por medio de leyes o decretos crea herramientas para guiar su aplicabilidad y seguridad para que el metadato sea protegido de intrusos y ataques.

En Colombia el marco legal, le falta aún evolucionar y con los ataques que se han presentado en el trascurso del año 2023, la atención a fortalecer estas leyes es una prioridad, aún falta terreno para hacer entender a los usuarios la importación que se debe tener en cuenta al momento de compartir su dato para validarlo con una biometría y qué tipo de protección le brindarán a esta información para que no sea usada sin permiso o para fines de fraude; es decir la ley solo informa que es legal el uso de las herramientas , pero es responsabilidad del usuario como comparte el dato.

Lay leyes o decretos que aplican en el país son:

- Ley 1581 de 2012 (Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, octubre 2012) (República de Colombia, 2012), se presenta para la protección de los datos de la persona. Donde se define como dato

sensible en el titulo III del articulo 5 a los datos biométricos que los identifica como información esencial del usuario que cobija la ley descrita.

- Ley 527 de 1999 (Ley 527 de 1999, agosto 1999) (República de Colombia, 1999), y el Decreto 2364 de 2012 (Decreto 2364 de 2012, noviembre 2012), es la reglamentación para uso de identificación electrónica (validación de identidad) y firma electrónica. La información capturada por métodos biométricos es aplicada para validar la identidad digital de una persona como también firmar un documento, es estas leyes la biometría es considerada, desde el punto de vista legal, como una firma electrónica. En el decreto 2364 de 2012 en el artículo 1, define: “3. Firma electrónica. Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.” (Decreto 2364 de 2012, noviembre 2012), donde expresa que una firma electrónica es un dato biométrico, por ello también esta ley hace parte de la investigación.
- Decreto 1377 de 2013 (República de Colombia, 2013) tiene por objeto “(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma” (República de Colombia, 2013).
- Donde en el capítulo 1, articulo 3 definición número 3, la huella biométrica la define como un dato sensible como se muestra en la siguiente cita del decreto, “Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el

origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.” (República de Colombia, 2013)

- Para el uso de bases de datos públicas en la RNEC, aplica la siguiente reglamentación especial, el Decreto Ley 019 de 2012 (Decreto Ley 019 de 2012) (Republica de Colombia, 2012) A partir de esta norma, la Registraduría emite la Resolución 5633 de 2016 (Registraduría Nacional del estado Civil, 2016), que regula el acceso a bases de datos por medio de operadores biométricos autorizados como es el caso de GSE.
- Y como normativa internacional que se usa la RNEC y otras entidades tanto públicas como privadas para la aplicabilidad de la seguridad de la información es la norma ISO 27001:2013 (Dominios ISO27001:2013, 2023).

Marco institucional

GSE (Gestion de Seguridad Electrónica)

Razón social: Gestion de Seguridad Electrónica S.A.

Nit: 900204272-8

Ubicación: CALLE 77 7 44 OFICINA 701, Bogotá, Colombia.

Sector del Mercado: GSE Una entidad de Certificación Abierta que transforma a las empresas y las integra a la era digital de manera segura, fácil y sencilla. Donde brinda a los clientes productos de certificación digital, autenticación y validación de identidad digital, con la más alta tecnología en seguridad de la información y cumplimos con la normativa establecida para cada proceso de negocio; garantizando la entrega de los servicios más confiables y seguros.

Experiencia en el mercado: GSE cuenta con más de 15 años de experiencia creando las soluciones tecnológicas más intuitivas y de rápida implementación que conectan los

requerimientos en seguridad, cumplimiento, verificación y calidad de servicio con las necesidades de transformación digital real de los diferentes sectores empresariales colombianos.

Objetivo de la Organización: Construir un ecosistema digital que haga accesibles, rápidos y seguros los procesos electrónicos para cualquier persona u organización.

Cliente objetivo: Sector Público y Privado.

Acreditaciones que garantizas las soluciones a prestar:

- Acreditación como Entidad de Certificación Digital ante el ONAC.
- Sello Web Trust calificación Clase Mundial.
- Miembro de Cloud *Signature Consortium*.
- ISO 9001:2015 y ISO 27001:2013.
- Approved Trust List member Adobe.
- Operador Biométrico ante la Registraduría Nacional del Estado Civil.

Estructura Organizacional

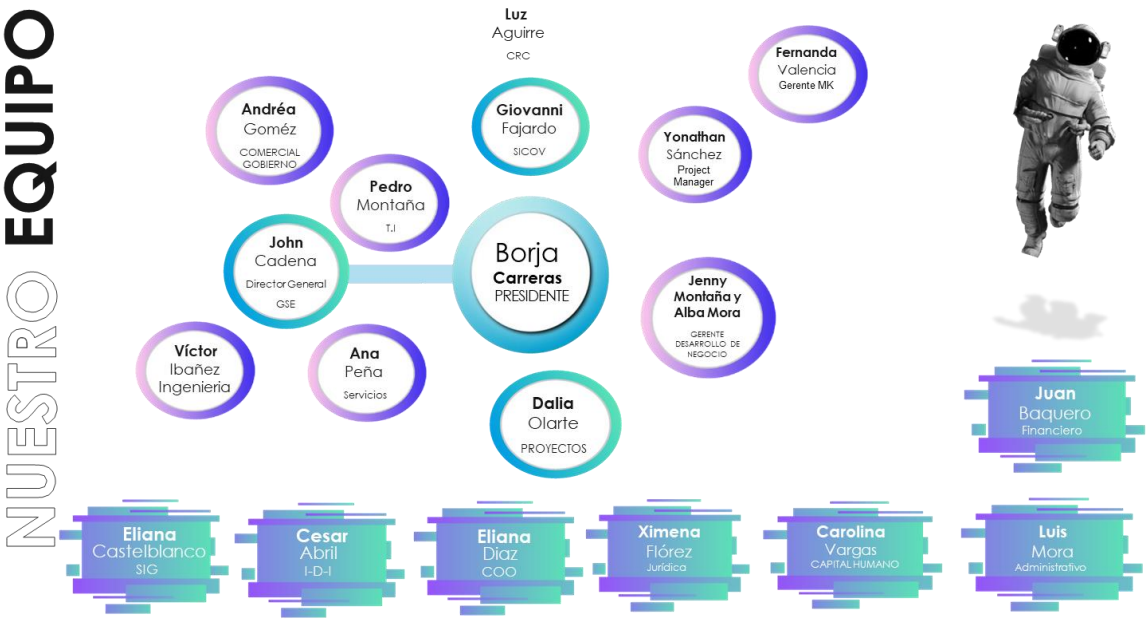


Ilustración 1. Estructura organizacional GSE. Autor: GSE, 2023.

En esta estructura, GSE no tiene un organigrama horizontal o vertical, maneja la definición de células, que en resumidas cuenta es que todas las áreas están relacionadas entre sí y es necesario el apoyo de manera no burocratizada, para la eficiencia y conocimiento de los procesos de la compañía.

M*isión*

*Provee*mos soluciones tecnológicas innovadoras que permite a nuestros clientes afrontar los retos y generar nuevas oportunidades de negocio garantizando la seguridad electrónica y jurídica.

Visión

Para el 2024 ser la compañía referente en servicios y soluciones de autenticación digital a nivel nacional, permitiendo a los ciudadanos y empresas adoptar una cultura digital.

Valores

- Foco al Cliente.
- Integridad.
- Innovación
- Imparcialidad.
- Trabajo en Equipo.

Soluciones de la organización

- **Transformación Digital**
    - Somos proveedores de tecnología que ayudan con soluciones disruptivas a organizaciones que buscan mantenerse vigentes y competitivas en el mercado.
- **Servicios Gestionados**

- Realizamos productos a medida que benefician los costos y apalancan la productividad y rendimiento.

- **Pilares**
  - **Talento digital y flexibilidad**
    - Capacitación y desarrollo del talento humano
  - **Tecnología**
    - Big data
    - Ciberseguridad
  - **Foco en el cliente**
    - Diseño de experiencia de usuario
    - Creación de activos digitales: Webs, e- commerces

Portafolio de los servicio y productos de la organización

- **Certificados Digitales**
  - **Certificados Digitales para Firmado Electrónico**

    Legalidad, Compromiso Y Respaldo: La integridad de las soluciones en GSE de firmado, cumplen con todos los requerimientos, estándares de calidad y seguridad exigidos por la ley. Garantizando que el contenido no ha cambiado ni se ha manipulado después del firmado, manteniendo la trazabilidad de todas las operaciones.

    Certificado Digital: Para poder hacer uso de tu firma digital debes tramitar primero un certificado digital expedido por un ECD, el cual contiene tus datos identificativos, opcionalmente unos atributos sobre lo que has hecho y se encuentra Cifrado de manera criptográfica con ECDSA.

    Soluciones de Firmado:

- **FirmaYA WEB**: En la Web puedes usar tanto firma electrónica, como firma digital con su estampado y cifrado bajo un modelo SaaS (*Software as a service*) con SSDF (software seguro) y OWASP (*Open Web Application Security Project*).

  Se puede usar en cualquier Sistema Operativo SO, y navegador.

  Permite incluir la imagen manuscrita de la firma y ubicarla en cualquier lado del documento, marca de agua, firmado *long term validation LTV*, y puedes obtener tres tipos de certificados Centralizado, token, firma electrónica
- **FirmaYA Driver**: Es una app que se usa luego de tener un certificado digital, almacenas llaves privadas en HSM, para firmar digitalmente documentos PDF rápidamente.

- **Certificados SSL**:

  La sigla SSL significa “capa de socket seguro” Se trata de una tecnología que establece un vínculo de sesión segura entre el navegador web del visitante y su sitio web, de modo que todas las comunicaciones que se transmiten mediante este vínculo se cifran y, por lo tanto, son seguras.

  Un certificado SSL es un archivo informático digital (o un código de tamaño pequeño) que tiene dos funciones específicas:

  a. Autenticación y verificación el certificado SSL tiene información acerca de la autenticidad de ciertos datos referentes a la identidad de una persona, empresa o sitio web.

b. Cifrado de datos el certificado SSL también posibilita el cifrado Esto significa que absolutamente nadie, excepto el destinatario deseado, puede interceptar y leer la información confidencial que se intercambia por la Web.

Se ofrecen tres tipos de certificados SSL:

- Certificado SSL DV (*Domain Validation*)
- Certificado SSL OV (*Organization Validation*)
- Certificado SSL EV (*Extended Validation*)

- **Correo Electrónico Certificado**

El servicio de correo electrónico certificado prestado por GSE, se encuentra debidamente acreditado por el ONAC. Para su funcionamiento cuenta con el estampado cronológico de tiempo, el cual está acreditado, este servicio tiene como función específica garantizar el momento exacto en que ocurren los eventos en el entorno electrónico.

El servicio de correo electrónico certificado realiza la trazabilidad del envío de un correo a cuentas de correo válidas hasta su entrega conforme a las respuestas del servidor de destino, donde observaremos los posibles eventos asociados al mismo (Apertura, Clic, Rebote).

Dicha información es certificada por GSE, por medio del documento denominado “Certificado de notificación electrónica”, en este certificado se evidencia la siguiente información:

- Remitente
- Destinatario
- Asunto del correo electrónico
- Constancia de envío (fecha y hora)

- Constancia de entrega en el servidor de correo (fecha y hora)
- Constancia de abierto (fecha y hora), siempre y cuando el correo electrónico sea abierto por el destinatario
- Contenido de la comunicación

- **Biometría**

  GSE brinda un conjunto de novedosas Soluciones Biométricas (SB) que ayudan a que las transacciones de los clientes sean escalables, autogestionadas, rápidas y seguras. Obteniendo clientes finales confiables y satisfechos con la aplicabilidad de estas soluciones**.**

  Se prima los siguientes ítems para la validación y autenticación del usuario con las SB**:**

  - **Registro**: Consulta, compara y reconoce los atributos únicos de una persona con el fin de confirmar su identidad con número de cédula de ciudadanía y datos biométricos.

    Velamos por la Confidencialidad de cada transacción, almacenándola y custodiándola en Bases de Datos (BD) cifradas, las cuales no pueden ser consultadas por terceros sin la autorización del cliente.
  - **Identificación:** Consulta, compara y reconoce los atributos únicos de una persona con el fin de confirmar su identidad con número de cédula de ciudadanía y datos biométricos.

    Aseguramos la Integridad del trámite usando Identificadores únicos de transacción (para identificar ¿Quién? ¿Dónde? ¿Cuándo? y ¿Cómo? se realizó la transacción.

- **Autenticación:** Desde un *On boarding* digital y/o con la registraduría (sin hacer registro), también podemos consultar BD de la RNEC y/o BD de terceros confiables como ANI, con los cuales podemos confirmar la autenticidad del cliente.

  El trámite es Auténtico cuando coinciden la huella dactilar (1 N) y/o registro facial contra la BD confiables o ante RNEC. La transacción es soportada por la Autorización de tratamiento de datos personales (ATDP), logs de peticiones y consultas de IUT los cuales vinculan la operación a lo largo del proceso obteniendo la Trazabilidad y el soporte que necesitamos en caso de un repudio futuro sobre el resultado de la validación.

  GSE este certificado como operador biométrico ante la Registraduría Nacional del Estado Civil (RNEC), donde brinda la posibilidad a GSE de realizar consultas de los ciudadanos nacionales o extranjeros en las bases de datos del estado, aumentando la confiabilidad de confirmación de autenticación de la persona.

  Entre la SB que ofrece GSE son:

  a. **biometría Dactilar**

     i. **biometría Dactilar contra Base de datos del Estado:** Captura de huellas dactilares de manera remota o presencial verificando la identidad con bases de datos confiables como RNEC o bases de terceros**.**

     ii. **biometría Dactilar con tecnología 4F:**

Captura huellas dactilares sin contacto, incluyendo los 10 dedos y funcionando en la mayoría de los teléfonos inteligentes disponibles en el mercado.

iii. **biometría Facial validado contra Documento**

Reconocimiento facial que permite la verificación y/o identificación de personas por medio de dispositivos móviles. Se puede acceder a bases de RNEC o Rostro contra documento.

Mapa conceptual

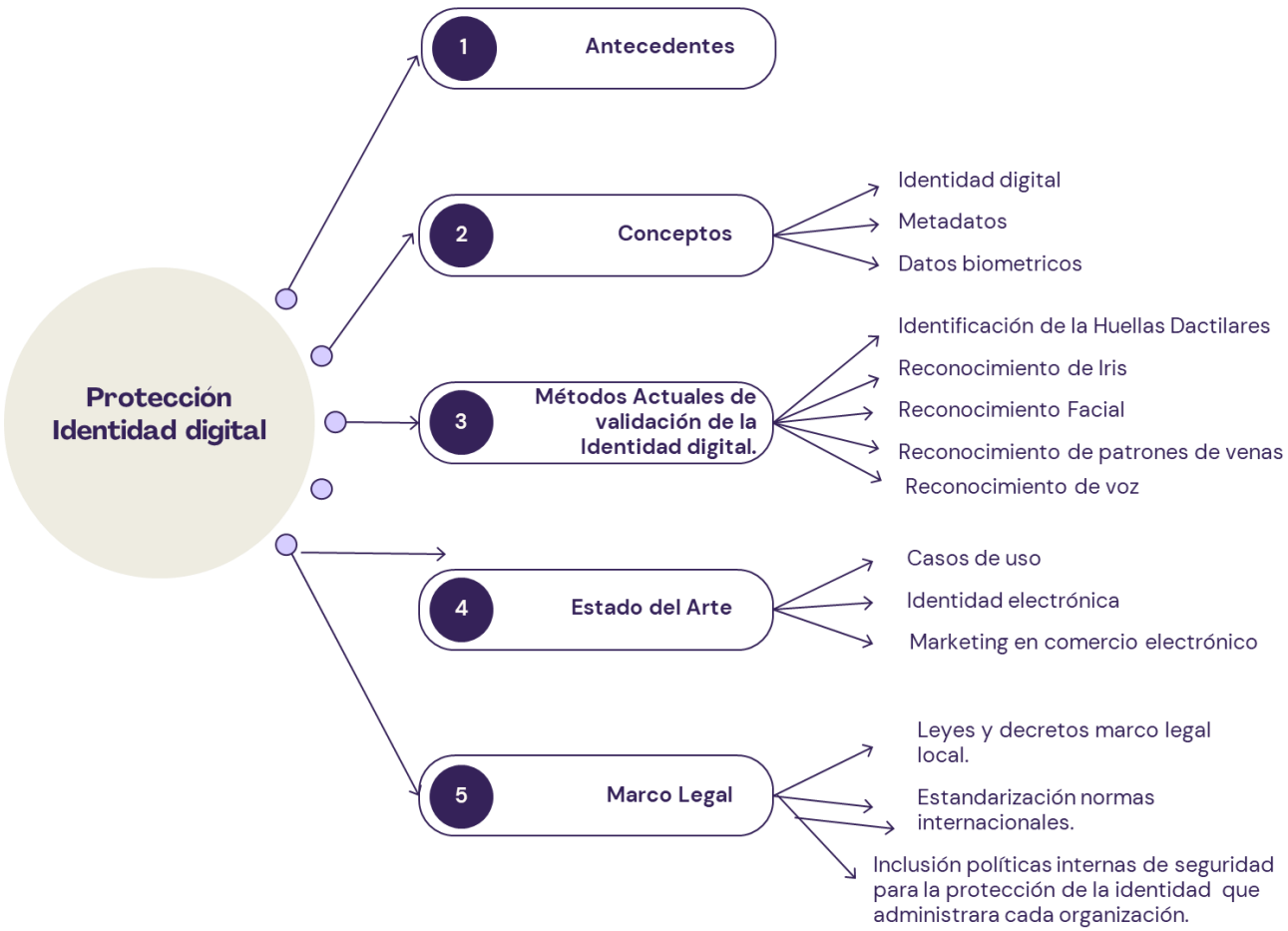


Ilustración 2. Mapa conceptual. Autor: GSE, 2023

Metodología de investigación

De acuerdo con la investigación sobre las mejores prácticas de uso de enrolamiento y autenticación por medio de métodos de autenticación en dispositivos móviles para la protección de la identidad digital, la metodología que aplica es la cualitativa, debido a las siguientes razones.

1. La metodología cualitativa permite obtener una comprensión profunda de las experiencias, percepciones y opiniones de los usuarios en relación con de uso de mecanismo de autenticación de identidad como las biometrías. Esto es crucial para comprender cómo se sienten los usuarios acerca de utilizar esta tecnología en su lugar de trabajo, como en su uso diario y si están dispuestos a adoptarla.
2. Permite explorar en detalle los desafíos y barreras que podrían surgir durante la implementación de la biometría facial en una aplicación móvil. Esto incluye aspectos como la privacidad, la seguridad y la aceptación por parte de los usuarios. Estos hallazgos cualitativos pueden ayudar a identificar posibles problemas y encontrar soluciones adecuadas.
3. Permite obtener información contextualizada y rica en detalles. Esto significa que se pueden obtener *insights* (perspectivas) valiosos sobre cómo se utilizan los métodos de autenticación en el contexto laboral y personal, así como comprender las necesidades y expectativas de los usuarios en relación con esta tecnología.

En resumen, la metodología cualitativa es preferible para identificar con mayor detalle y compresión si la implementación de las biometrías en una aplicación móvil aumenta la seguridad de identidad digital, permitiendo comprender en profundidad las experiencias y percepciones de los usuarios, hallar desafíos y barreras y obtener información contextualizada y rica en detalles.

Por lo anterior y con la guía de la metodología de investigación de Sampieri, página 470 tabla 15.1 “sobre los criterios para elegir el diseño de abordaje a utilizar”, nuestra investigación no solo es cualitativa sino su diseño, marco o abordaje tiende hacia la vertiente de la “investigación-acción” (Sampieri, 2014) (pág. 496), además incluyendo la perspectiva de la “visión emancipadora: donde su objetivo trasciende la resolución de problemas o el desarrollo de mejoras en un proceso; busca que los participantes generen un cambio social profundo a través de la investigación. Este enfoque de diseño no se limita únicamente a funciones de diagnóstico y producción de conocimiento, sino que también tiene como finalidad crear conciencia entre los individuos acerca de sus circunstancias sociales y la necesidad de mejorar su calidad de vida”. (Sampieri, 2014) (Pág. 497).

Con esta guía, se genera la base de un flujo de seguimiento, donde se establecen fases para la “Investigación-acción”, donde describimos las actividades a realizar para nuestra investigación:

Tabla 1. Fases de investigación-Acción

Fase de Investigación-Acción	Descripción de la Actividad	Herramientas y Métodos Utilizados	Resultados y Observaciones
1. Planeación	Identificación del Problema de Investigación	Revisión bibliográfica, antecedentes y casos de uso.	Identificación de la necesidad de mejorar la seguridad en identidad digital para dispositivos móviles.
2. Planificación	Diseño del Estudio Piloto	Desarrollo de cuestionarios o encuestas para el usuario final.	Desarrollo de instrumentos de recolección de datos específicos para la investigación.
3. Acción	Implementación del Estudio Piloto	Promover los cuestionarios a los usuarios de dispositivos móviles.	Recopilación de datos sobre la aceptación y usabilidad de la biometría facial en dispositivos móviles.

Fase de Investigación-Acción	Descripción de la Actividad	Herramientas y Métodos Utilizados	Resultados y Observaciones
4. Observación	Análisis e Interpretación de Resultados Preliminares	Análisis cualitativo de las respuestas y observaciones	Identificación de patrones de aceptación y desafíos percibidos por los usuarios.
5. Replanificación	Ajuste del Enfoque de Investigación	Revisión de la metodología, modificación de instrumentos	Ajustes en la metodología y enfoque basados en las reflexiones y los hallazgos de la fase anterior.
7. Nueva Acción	Implementación de la Investigación Principal	Encuestas a gran escala, pruebas piloto de aplicaciones de biometría facial	Recopilación de datos a gran escala sobre la aceptación y usabilidad de la biometría facial en dispositivos móviles.
8. Consolidación	Análisis y Síntesis de Resultados	Análisis cualitativo y comparativo de datos	Identificación de patrones y tendencias a través de los datos recopilados.
9. Informe Final	Presentación de Resultados	Informe de investigación, presentaciones, artículos	Documentación de los hallazgos, implicaciones prácticas y recomendaciones para la implementación de la biometría facial en dispositivos móviles para la protección de identidad digital.

Hipótesis y temas

Luego de la búsqueda de información realizada en el marco teórico (fase de planeación), podemos empezar con la formulación de una hipótesis inicial que nos da un guía para la formulación de preguntas a resolver (fase de planificación) y que nos permitirá enfocar gradualmente la investigación.

Teniendo en cuenta los métodos de autenticación mencionados en el marco teórico, junto con el concepto de identidad digital analizado, podemos llegar a la hipótesis inicial de que uno de los factores de riesgo al momento de usar técnicas de autenticación e identificación es el desconocimiento per sé del funcionamiento y la implicación que conlleva el uso de estos métodos. Adicionalmente, pensamos que el uso correcto de una identidad digital debe ir acompañado de técnicas de autenticación que cumplan con estándares que aseguren que la información del usuario no caiga fácilmente en manos de terceros. Métodos de autenticación digital como la biometría facial acompañados de un único ente de control pueden ser una excelente estrategia para el correcto uso de la identidad digital.

Es por este motivo que se ve necesario tratar los siguientes temas para el desarrollo de la investigación. En este paso se trabajará la fase de planificación y la fase de acción, con el fin de obtener información de los siguientes temas:

- Conocimiento de las técnicas de autenticación e identificación digital: Se quiere conocer de forma general el conocimiento técnico, percepción y sentimientos generados por los conceptos de autenticación e identificación digital.
- Conocimiento sobre identidad digital: Se quiere conocer de forma general el conocimiento técnico, percepción y sentimientos generados por el concepto de identidad digital.
- Disposición de las personas entrevistadas frente a tener una identidad digital: se quiere tener una idea sobre diferentes posiciones acerca de la identidad digital.
- Disposición de las personas a las autenticaciones biométricas: se quiere tener una idea sobre diferentes posiciones acerca de las técnicas de autenticación biométricas.
- Beneficio que ofrece la identidad digital: se quiere indagar sobre qué beneficios se considera que ofrece la identidad digital en diferentes personas.

- Beneficios que ofrece un método de autenticación seguro: se quiere indagar a un experto sobre qué beneficios se considera que ofrece un método de autenticación seguro.
- Eventos que haya tenido por no tener conocimiento sobre ciberseguridad: se quiere buscar experiencias personales de ataques cibernéticos que los encuestados hayan experimentado.

Definición de Variables

Las variables que queremos analizar en esta investigación son los conceptos de Identificación digital y Autenticación con Biometría. Las definiciones conceptuales y la definición operacional de dichas variables se pueden ver en la siguiente tabla.

Tabla 2. Definición de variables

Variables	**Definición conceptual**	**Definición operacional**
Definición ID Digital	Nos referimos a identidades digitales como la representación única de un sujeto en el momento de hacer una interacción digital (Paul A. Grassi, 2017).	Se hacen preguntas para saber el conocimiento de la gente frente a esa definición. Se hará una observación directa a los entrevistados sobre los conocimientos y las disposiciones frente estos conceptos.
Autenticación con Biometría	La definición que usamos se encuentra en *Handbook of statistics:* "*La biometría es la ciencia de reconocer automáticamente a las personas en función de las características físicas o de comportamiento, como la cara, la huella digital, el iris, la mano, la voz, la marcha y la firma"* (D.A. Reid, 2013)	

Instrumento de medición

Nuestra investigación usa un enfoque cualitativo para comprender a fondo las características de los métodos de autenticación biométrica en dispositivos móviles para proteger la identidad digital. Para esto, utilizamos una herramienta de investigación conocida

como una guía de entrevista semiestructurada. A diferencia de las encuestas cerradas, esta técnica nos permite explorar las experiencias y percepciones de los usuarios en este tipo de tecnologías.

Este tipo de entrevista semiestructurada consiste en preguntas abiertas y exploratorias que se centran en aspectos clave de la implementación de soluciones biométricas. Al utilizar este enfoque, podemos obtener información cualitativa descriptiva sobre cómo los usuarios perciben la seguridad proporcionada por estas soluciones, cuál es su experiencia al utilizar la biometría para autenticarse en aplicaciones móviles y los desafíos que enfrentan en este proceso.

A continuación, se estructuran las preguntas a incluir en la encuesta para apoyar la selección de la metodología cualitativa (parte da las fases de planificación y acción).

El objetivo de analizar cada pregunta presentada en la encuesta es obtener información relevante y significativa que respalde la selección de la metodología cualitativa para la implementación de métodos de autenticación en una aplicación móvil para apoyo en la seguridad de la Identidad Digital. Cada pregunta está diseñada para explorar diferentes aspectos, como la familiaridad con la identidad digital y métodos de autenticación, las opiniones y percepciones de los participantes, los beneficios y preocupaciones percibidos, la comodidad de uso, las expectativas y la eficiencia y seguridad percibidas.

Al analizar las respuestas a estas preguntas, se busca obtener una comprensión más profunda de las actitudes, creencias y necesidades de los potenciales usuarios de la aplicación móvil con métodos de autenticación. Esto permitirá tomar decisiones informadas sobre la implementación y adaptación de la tecnología, así como identificar posibles desafíos y áreas de mejora.

En la siguiente tabla se recopilan los temas a tratar y las preguntas que se realizarán en la encuesta. Cada tema y pregunta está relacionada con una de las variables de investigación.

Tabla 3. Temas, variables y preguntas

Temas	**Variables**	**Preguntas asociadas para cada tema**
Conocimiento de los entrevistados sobre la identidad digital	ID Digital	¿Sabe usted qué es identidad digital?
Conocimiento de los entrevistados frente a los métodos de autenticación	Biometría e ID Digital	¿Qué tan familiarizado estás con el concepto de biometría para la autenticación de identidad digital? ¿Qué tipos de biometrías para la autenticación de su identidad en dispositivos móviles conoce o ha utilizado previamente?
Disposición de las personas entrevistadas frente a tener una identidad digital (percepciones y sentimientos)	ID Digital	¿Le parece seguro el uso de la identidad digital? ¿Qué percepción le genera tener una identidad digital? (miedo, angustia, inseguridad, confianza, eficacia, eficiencia) ¿Qué tipo de información le gustaría recibir antes de utilizar un método de autenticación biométrico en una aplicación móvil? En comparación con otros métodos de autenticación (por ejemplo, contraseñas, PIN), ¿crees que los métodos de autenticación biométrica son más seguras o menos seguras?
Disposición de las personas a los métodos de autenticación biométrica (percepciones, sentimientos y opiniones)	Biometría	¿Qué opinas sobre la implementación de métodos de autenticación por biometrías en una aplicación móvil? ¿Qué preocupaciones o desafíos crees que podrían surgir al implementar métodos de autenticación por biometrías en una aplicación móvil? ¿Te sentirías cómodo/a utilizando métodos de autenticación por biometrías en tu lugar de trabajo? ¿Qué factores considerarías importantes para garantizar la privacidad y seguridad de los datos biométricos?
Beneficio que ofrece la identidad digital y beneficios que ofrece un método de autenticación seguro	ID Digital	¿Cuáles crees que podrían ser los beneficios de utilizar métodos de autenticación por biometrías en el contexto laboral? ¿Qué expectativas tienes en cuanto a la facilidad de uso de una aplicación móvil que utilice métodos de autenticación biométricos? ¿Te gustaría realizar trámites documentales donde la confirmación de su identidad sea remota, evitando el traslado a sitio? ¿Consideras que la implementación de biometrías en una aplicación móvil mejoraría la eficiencia y seguridad en tu lugar de trabajo?
Eventos que haya tenido por no tener conocimiento sobre ciberseguridad	Biometría e Id digital	¿Confías en la precisión de los métodos de autenticación biométrica? ¿Has tenido alguna experiencia de error o falsa identificación?
Percepción del usuario luego de realizar la encuesta.	Biometría e Id digital	¿Tienes alguna sugerencia o comentario adicional sobre la implementación de la biometría facial en una aplicación móvil?

Las encuestas se desarrollan en la ciudad de Bogotá en el mes de noviembre del año 2023, contando con un total de dos expertos y 33 personas encuestadas.

Población y muestra

En cuanto a la población y muestra que se utilizará en esta investigación podemos empezar por recordar que al ser una investigación cualitativa de tipo investigación-acción, el tipo de muestra recomendado y que más se acomoda a nuestro estudio son: la muestra de expertos, las Muestras diversas o de máxima variación y las Muestras teóricas o conceptuales (Sampieri, 2014) (Pág. 387-388). Este tipo de muestras nos permiten tener de primera mano diversidad de información de personas con conocimientos técnicos sobre identificación digital, como también información de personas con poco conocimiento del tema; que nos den una percepción no probabilística de los temas que queremos desarrollar. Para lo cual se buscarán personas que usan dispositivos móviles para sus procesos laborales o de uso diario.

Técnicas de análisis de datos

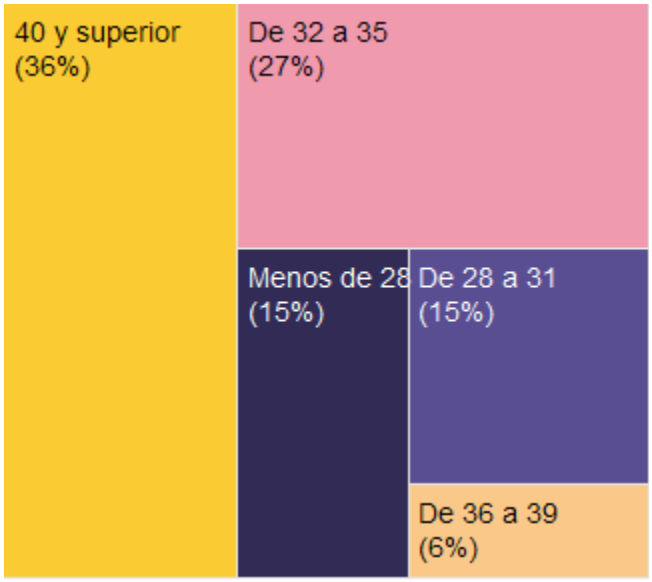
La investigación cualitativa utiliza como técnicas de análisis de datos las siguientes: Mapas conceptuales, diagramas causa-efecto, antecedentes-consecuencias, matrices (por ejemplo, de categorías, de temas de las causas cruzados con categorías o temas de los efectos), Jerarquización de temas o identificación de prioridades, Organigramas de la estructura, análisis de redes (Sampieri, 2014) (Pág. 499).

Análisis de datos

A partir de los resultados generados en las encuestas realizadas a usuarios de dispositivos móviles, identificamos las siguientes informaciones frente a la investigación:

Figura 1. Grafica referente a la pregunta 1. ¿qué edad tiene?

	N	%
Menos de 28	5	15%
De 28 a 31	5	15%
De 32 a 35	9	27%
De 36 a 39	2	6%
40 y superior	12	36%
TOTAL	**33**	**100%**

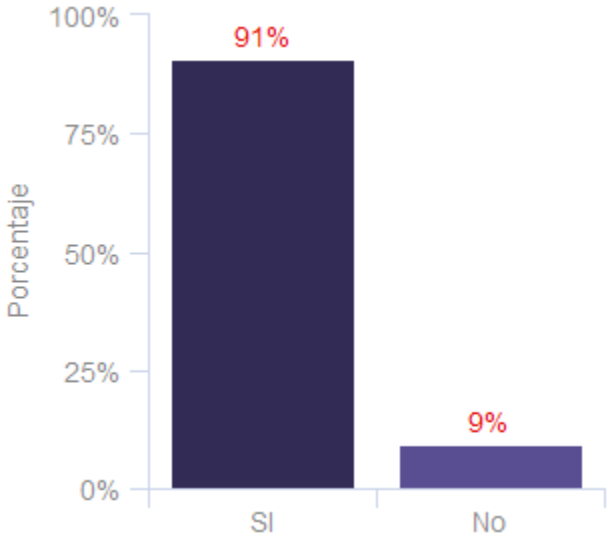


Fuente: Elaboración propia en DATAVIV

La primera gráfica presenta los resultados de la pregunta 1, la cual indaga sobre la edad de los participantes. Este análisis tiene como objetivo verificar que la muestra encuestada sea conformada exclusivamente por individuos mayores de edad. Esta condición es esencial, ya que la identificación por biometría, según la normativa legal en Colombia, solo es aplicable a este grupo demográfico. Este criterio de inclusión garantiza la idoneidad de la población encuestada para abordar de manera pertinente las cuestiones planteadas en esta investigación. Cabe destacar que la muestra está compuesta por 33 participantes.

Grafica2. Referente a la pregunta 2. ¿Sabe usted qué es identidad digital?

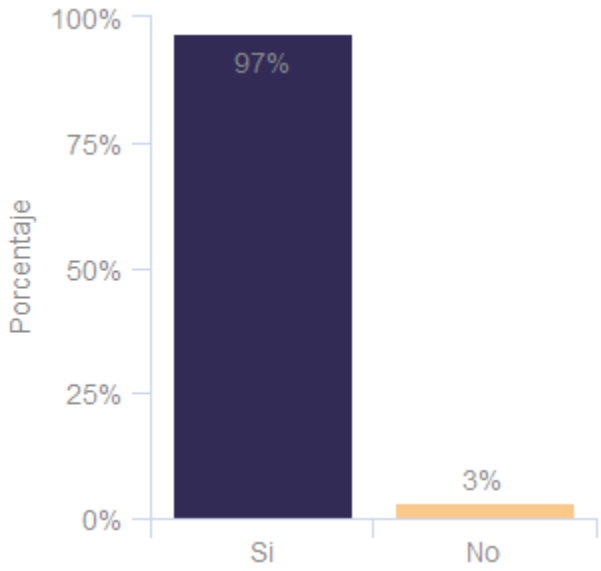
	N	%
SI	30	91%
No	3	9%
TOTAL	**33**	**100%**



Fuente: Elaboración propia en *DATAVIV*

En la Segunda gráfica, muestra el resultado de la pregunta 2, ¿Sabe usted qué es identidad digital?; la cual indaga sobre el conocimiento acerca del término 'identidad digital'. Se destaca que un 91% de los participantes demuestra familiaridad con dicho concepto. Este porcentaje de comprensión hace que la encuesta sea oportuna para la investigación. Aunque el hecho de que las personas encuestadas afirmen conocer el concepto de identidad digital, se debe verificar que tan profundo es su entendimiento.

Figura 3. Grafica referente a la pregunta 3. ¿Sabe usted qué es la identificación de una persona por una Biometría?



	N	%
Si	32	97%
No	1	3%
TOTAL	**33**	**100%**

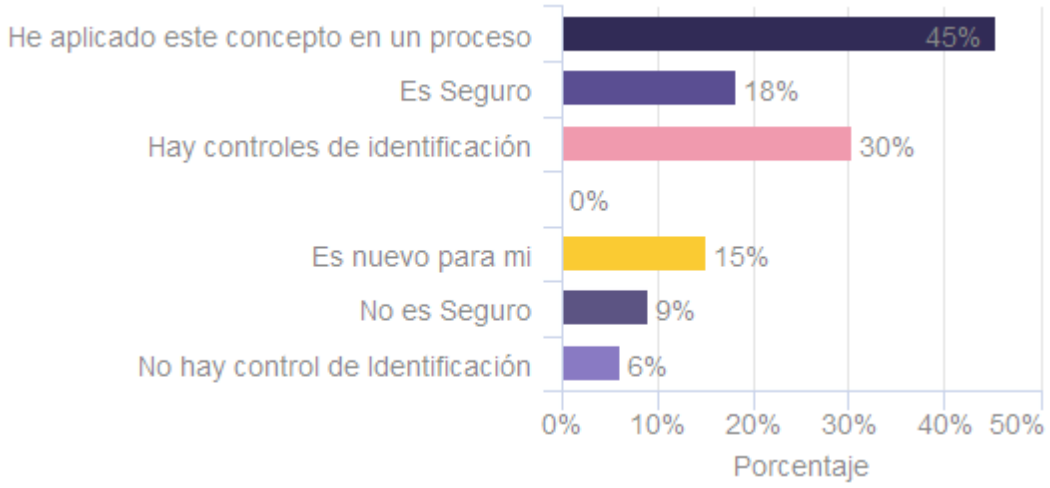
Fuente: Elaboración propia en *DATAVIV*

En la tercera gráfica, muestra el resultado de la pregunta 3, ¿Sabe usted qué es la identificación de una persona por una Biometría?; de la misma forma que la pregunta anterior. Esta respuesta nos muestra un alto porcentaje en el conocimiento del concepto de identificación por medio de biometrías, pero debemos indagar sobre el que tan profundo es dicho entendimiento. Las siguientes preguntas nos permiten acercarnos a ese fin.

Figura 4. Grafica referente a la pregunta 4. ¿Qué tan familiarizado estás con el concepto de biometría para la autenticación de identidad digital?

	N	%
He aplicado este concepto en un proceso	15	45%
Es Seguro	6	18%
Hay controles de identificación	10	30%
	0	0%

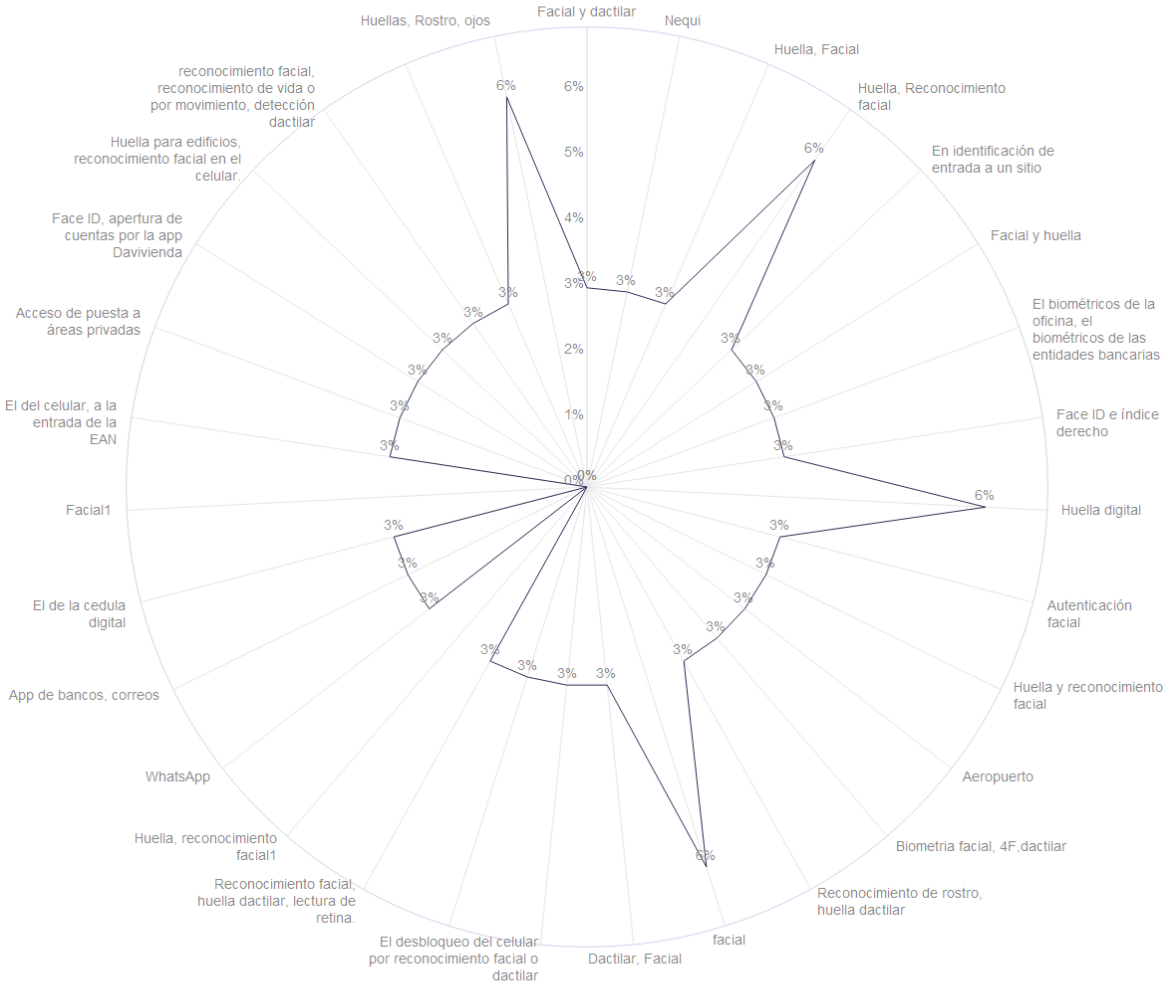
Es nuevo para mi	5	15%
No es Seguro	3	9%
No hay control de Identificación	2	6%
TOTAL	**33**	



Fuente: Elaboración propia en *DATAVIV*

En la cuarta gráfica, muestra el resultado de la pregunta 4, ¿Qué tan familiarizado estás con el concepto de biometría para la autenticación de identidad digital?; de las 33 respuestas evaluadas, el 15% de los entrevistados demuestra poco conocimiento del concepto de biometría. El 85% restante demuestra algún tipo de familiaridad. Esto puede estar relacionado con el hecho de que las biometrías están constantemente en uso en las interacciones diarias. Denotando la importancia de tener conocimiento sobre ellas.

Figura 5. Grafica referente a la pregunta. ¿Qué tipos de biometrías para la autenticación de su identidad en dispositivos móviles conoce o ha utilizado previamente?



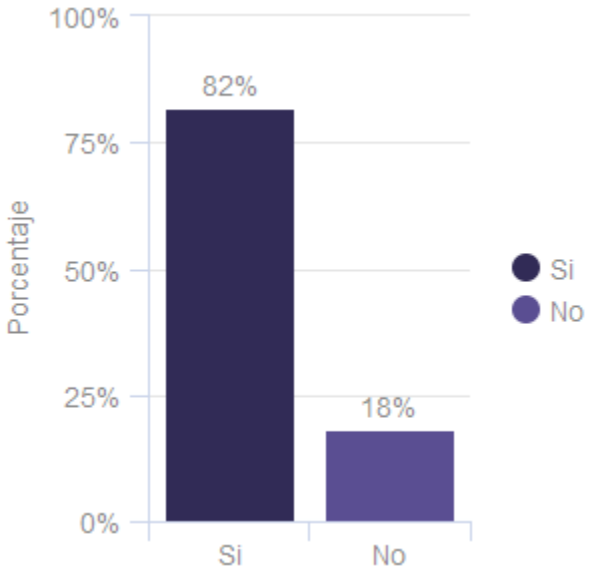
Fuente: Elaboración propia en *DATAVIV*

La quinta gráfica, muestra el resultado de la pregunta 5, ¿Qué tipos de biometrías para la autenticación de su identidad en dispositivos móviles conoce o ha utilizado previamente?; Luego de depurar los datos de esta pregunta abierta, podemos encontrar que las biometrías más conocidas por los entrevistados son la biometría facial (70%) y las huellas digitales

(61%). También se puede denotar una confusión entre el concepto de biometría y el concepto de identificación digital por medio de biometría de una aplicación específica.

Figura 6. Grafica referente a la pregunta 6. ¿Le parece seguro el uso de la identidad digital?

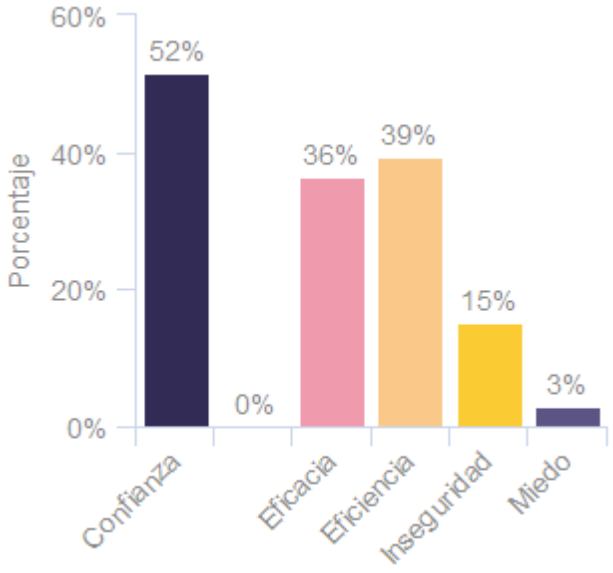
	N	%
Si	27	82%
No	6	18%
TOTAL	**33**	**100%**



Fuente: Elaboración propia en *DATAVIV*

En la sexta gráfica, muestra el resultado de la pregunta 6, ¿Le parece seguro el uso de la identidad digital?; para la cual, el 82% de los encuestados les parece seguro usar una identidad digital. De este resultado podemos ver una aceptación general de este tipo de tecnologías, lo cual es muy importante para la futura expansión de la identidad digital en distintos ámbitos del uso diario.

Figura 7. Grafica referente a la pregunta 7. ¿Qué percepción le genera tener una identidad digital?



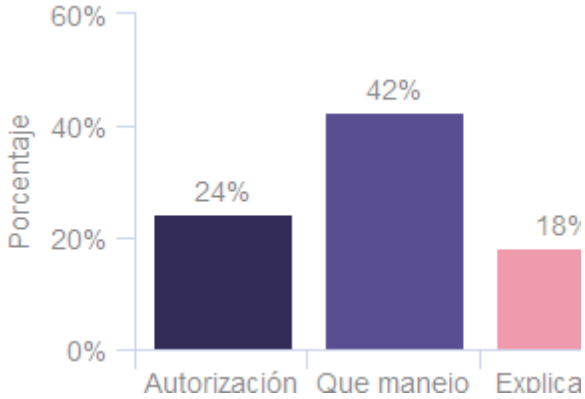
	N	%
Confianza	17	52%
Angustia	0	0%
Eficacia	12	36%
Eficiencia	13	39%
Inseguridad	5	15%
Miedo	1	3%
TOTAL	**33**	

Fuente: Elaboración propia en *DATAVIV*

En la séptima gráfica, muestra el resultado de la pregunta 7, ¿Qué percepción le genera tener una identidad digital?; en la pregunta el 82% muestra emociones positivas frente al uso de una identidad digital. Por otro lado, el 15% de las personas encuestadas respondieron que les genera inseguridad y otro 3% respondió que les genera miedo. Lo que concuerda con los resultados de la pregunta 6, donde el 18% de las personas no sienten seguridad con una identidad digital. Es por este motivo que será importante crear conocimiento acerca de la identidad digital para que las sensaciones de miedo e inseguridad se disminuyan.

Figura 8. Grafica referente a la pregunta 8. ¿Qué tipo de información le gustaría recibir antes de utilizar un método de autenticación biométrico en una aplicación móvil?

	N	%
Autorización de uso de sus datos	8	24%
Que manejo hará la organización con la toma de esta información	14	42%
Explicación de porque se solicita este tipo de huella biométrica.	6	18%
Instructivo de Uso	5	15%
TOTAL	**33**	**100%**



Fuente: Elaboración propia en *DATAVIV*

En la octava gráfica, muestra el resultado de la pregunta 8, ¿Qué tipo de información le gustaría recibir antes de utilizar un método de autenticación biométrico en una aplicación móvil?; Aunque para la toma de datos biométricos, se debe solicitar previa autorización y mencionar las políticas de manejos de datos, el 75% de los encuestados solicita más información sobre cómo (15%), qué (42%) y por qué (18%) son solicitados y manejados estos datos.

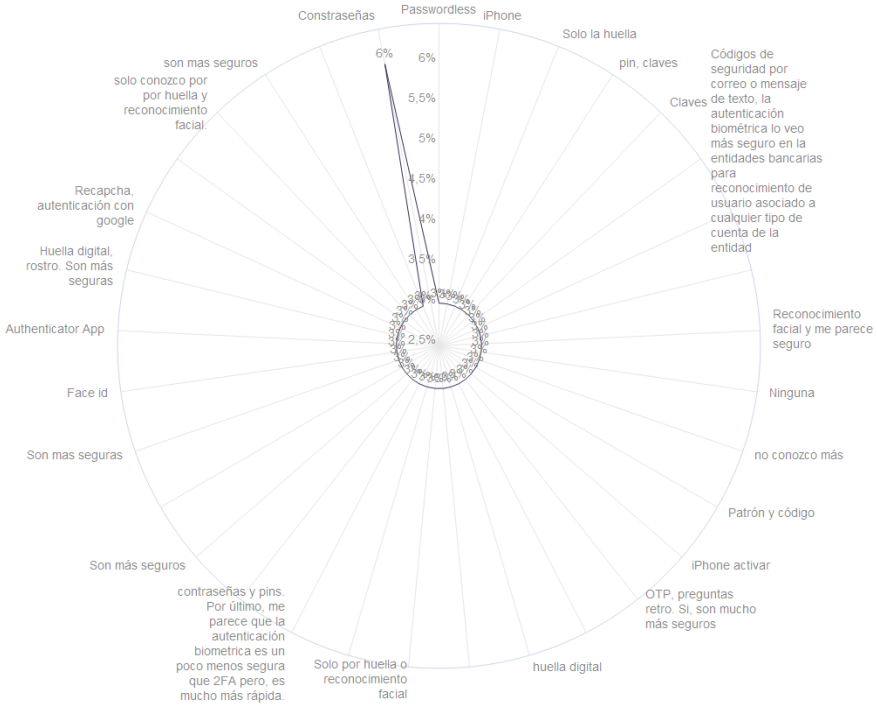
Figura 9. Grafica referente a la pregunta 9. ¿conoce que existen leyes para la protección de la identidad digital en Colombia?

	N	%
Si	12	36%
No	21	64%
TOTAL	**33**	**100%**

Fuente: Elaboración propia en *DATAVIV*

En la novena gráfica, se muestra el resultado de la pregunta 9, ¿conoce que existen leyes para la protección de la identidad digital en Colombia? Donde el 64% de los encuestados no manifiestan conocimiento sobre las leyes para protección de la identidad digital en Colombia. Nuevamente es necesario, mencionar la importancia de crear una cultura de conocimiento frente a los temas de identidad digital, que cada vez serán más usados en Colombia.

Figura 10. Grafica referente a la pregunta 10. ¿Qué otros métodos de autenticación usa en aplicaciones móviles, podría mencionar los que conoce?

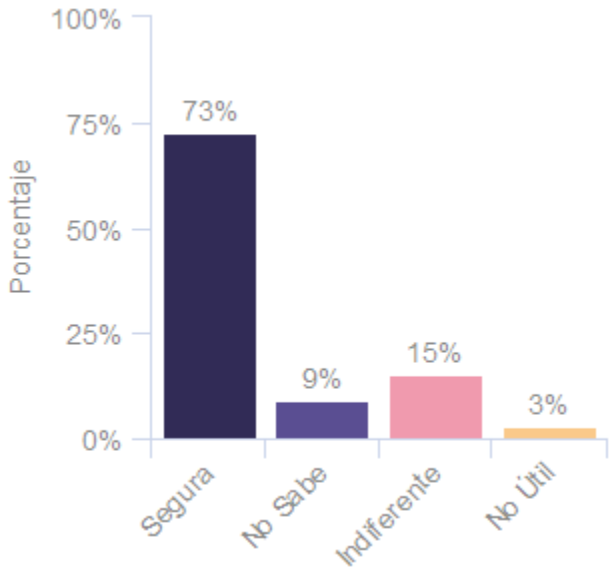


Fuente: Elaboración propia en *DATAVIV*

En la décima gráfica, muestra el resultado de la pregunta 10, ¿Que otros métodos de autenticación usa en aplicaciones móviles, podría mencionar los que conoce?, ¿además crees que los métodos de autenticación biométrica son más seguras o menos seguras? La finalidad de esta pregunta abierta es la de conocer si los encuestados tienen un conocimiento profundo sobre las biometrías. Es claro que los encuestados conocen diferentes métodos de autenticación, pero no se tiene un consenso sobre cuál es el método más seguro.

Figura 11. Grafica referente a la pregunta 11. ¿Qué opinas sobre la implementación de métodos de autenticación por biometrías en una aplicación móvil?

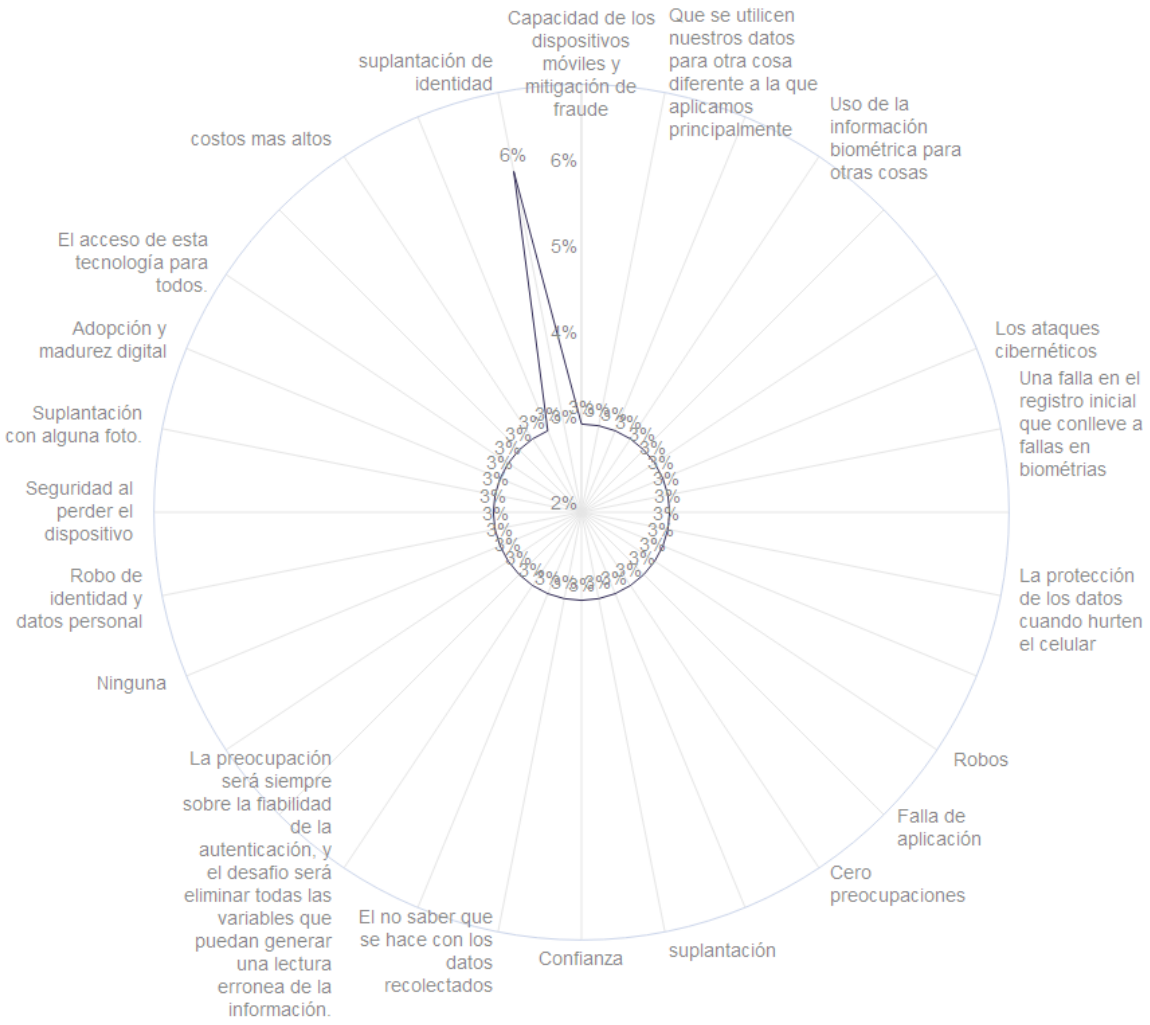
	N	%
Segura	24	73%
No Sabe	3	9%
Indiferente	5	15%
No Útil	1	3%
TOTAL	**33**	**100%**



Fuente: Elaboración propia en *DATAVIV*

En la onceava gráfica, muestra el resultado de la pregunta 11, ¿Qué opinas sobre la implementación de métodos de autenticación por biometrías en una aplicación móvil? El 75% de los encuestados les pareció seguro el uso de biometrías en aplicaciones móviles, sumado al 12% que les es indiferente el uso de estas tecnologías. Aunque el uso de estas biometrías está ampliamente expandido en aplicaciones móviles, resulta clave preguntarse si para aplicaciones triviales es necesario compartir esta información con terceros. Aunque el uso de las biometrías puede facilitar el ingreso y autenticación en aplicaciones móviles, puede ser una puerta para la pérdida de datos sensibles.

Figura 12. Grafica referente a la pregunta 12. ¿Qué preocupaciones o desafíos crees que podrían surgir al implementar métodos de autenticación por biometrías en una aplicación móvil?

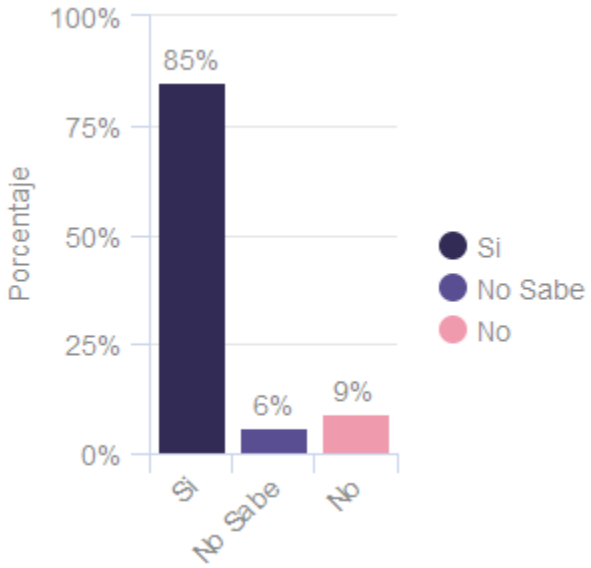


Fuente: Elaboración propia en *DATAVIV*

En la doceava gráfica, muestra el resultado de la pregunta 12, ¿Qué preocupaciones o desafíos crees que podrían surgir al implementar métodos de autenticación por biometrías en una aplicación móvil?; Al preguntar sobre las posibles preocupaciones o desafíos que puede tener la autenticación por medio de biometrías, las personas encuestadas mencionan en su gran mayoría la preocupación por el robo o suplantación de identidad. Situación para la cual se debe trabajar en enseñar cuales son los principales factores que se deben revisar para

que este robo no suceda. Por otro lado también, una menor parte de los encuestados muestra una gran confianza en este tipo de tecnología.

Figura 13. Grafica referente a la pregunta 13. ¿Te sentirías cómodo/a utilizando métodos de autenticación por biometrías en tu lugar de trabajo?

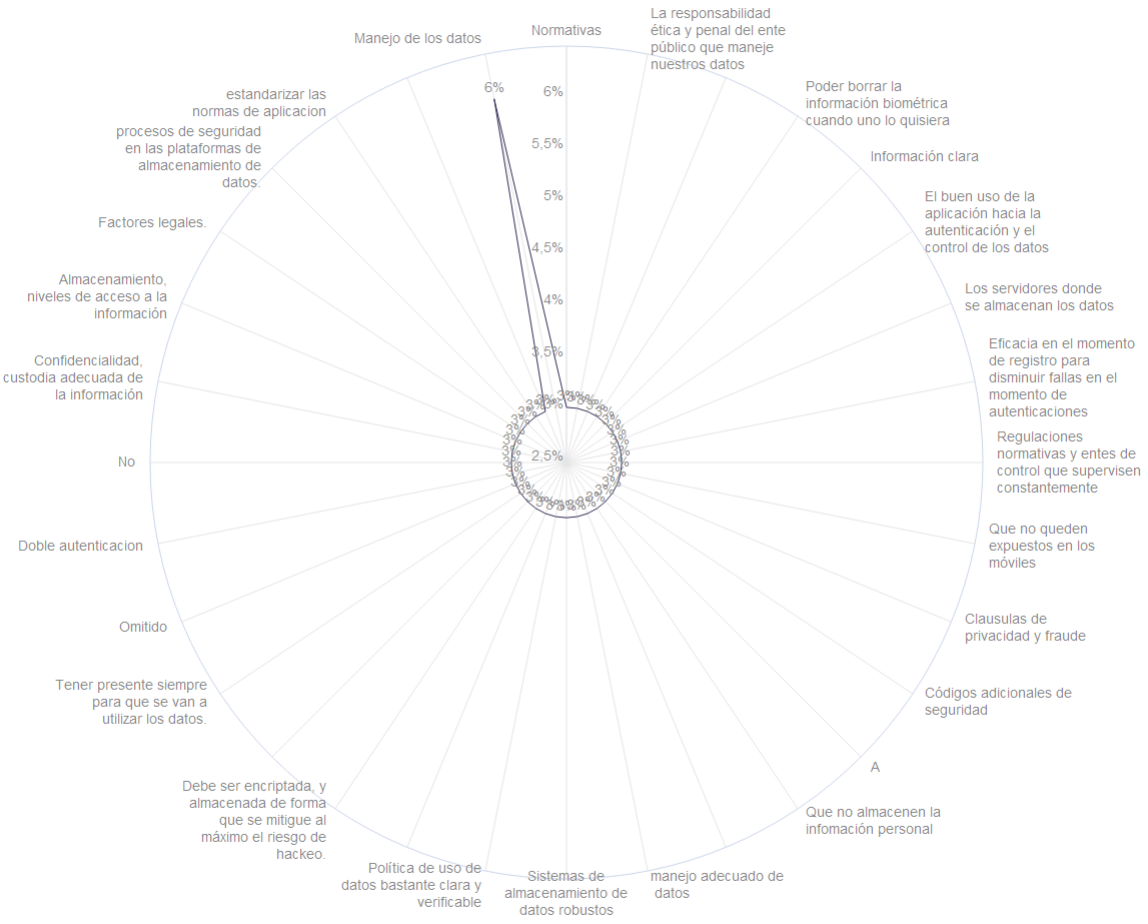


	N	%
Si	28	85%
No Sabe	2	6%
No	3	9%
TOTAL	**33**	**100%**

Fuente: Elaboración propia en *DATAVIV*

En la treceava gráfica, muestra el resultado de la pregunta 13, ¿Te sentirías cómodo/a utilizando métodos de autenticación por biometrías en tu lugar de trabajo?; esta pregunta tiene como objetivo explorar la variable de percepción hacia esta tecnología emergente. Los datos revelan que el 85% de la muestra manifiesta sentirse cómodo con el uso de métodos de autenticación por biometría en el lugar de trabajo. Sin embargo, es relevante destacar que el 15% restante muestra un grado de desconocimiento o incomodidad ante este tipo de autenticación. Esta proporción sugiere que la adaptación de esta tecnología podría no ser rápida o ampliamente aceptada en dispositivos móviles, subrayando la necesidad de considerar las actitudes individuales y las posibles barreras percibidas en la implementación de sistemas de identificación digital basados en biometría.

Figura 14. Grafica referente a la pregunta 14. ¿Qué factores considerarías importantes para garantizar la privacidad y seguridad de los datos biométricos?

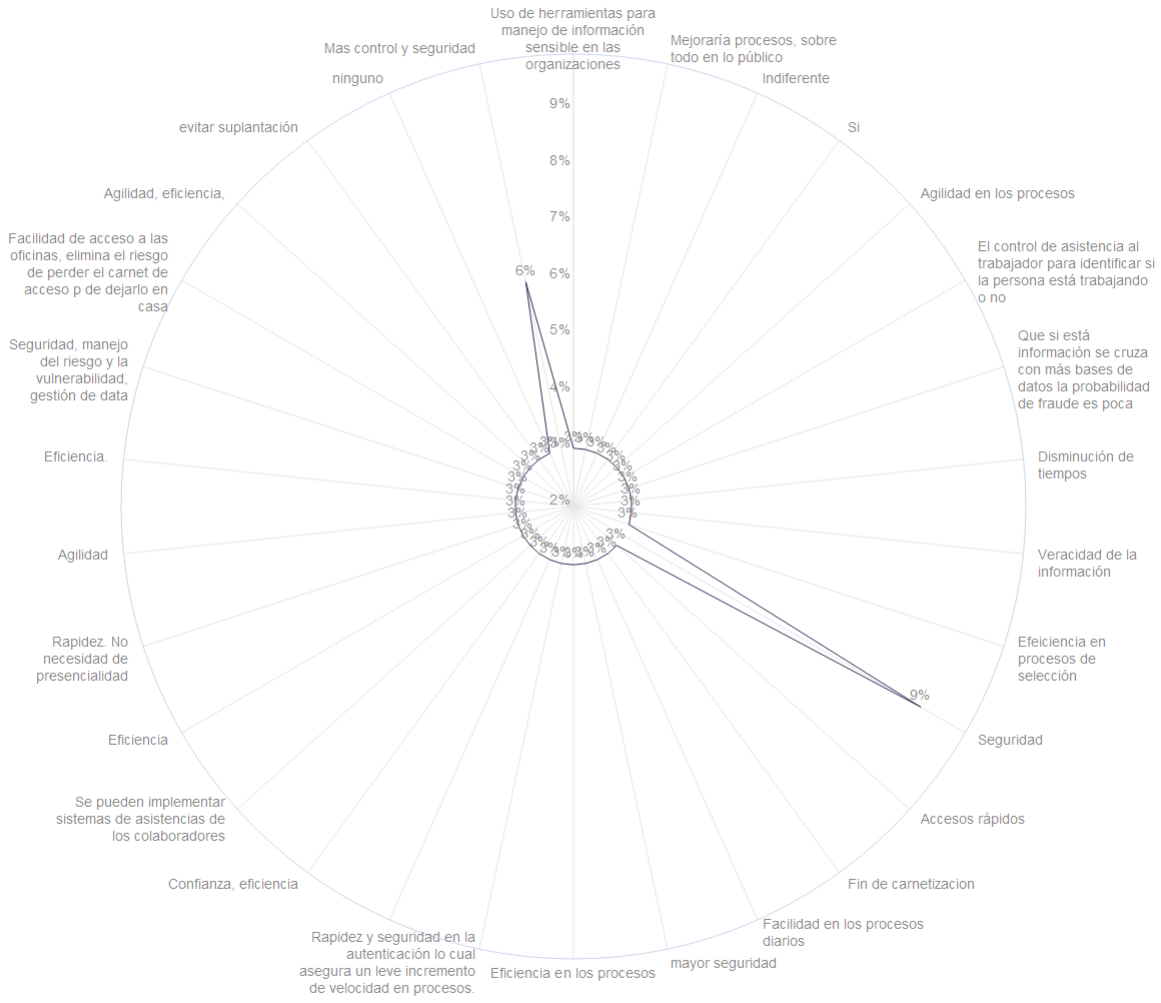


Fuente: Elaboración propia en *DATAVIV*

En la catorceava gráfica, muestra el resultado de la pregunta 14, ¿Qué factores considerarías importantes para garantizar la privacidad y seguridad de los datos biométricos?; Al examinar la diversidad de respuestas proporcionadas por los encuestados, se depura las respuestas obtenidas y se destaca que existen consideraciones cruciales vinculadas al “manejo de datos”, “el propósito de la utilización de los datos”, “los métodos de aseguramiento del dato” como también aplicación de “cláusulas o políticas de uso del dato”. Estos hallazgos evidencian la inquietud de los participantes respecto a cómo se asegura la aplicación de dispositivos móviles para un uso óptimo de los datos biométricos capturados.

Este análisis subraya la importancia de abordar aspectos específicos relacionados con la gestión y seguridad de datos en el contexto de la implementación de tecnologías biométricas en dispositivos móviles.

Figura 15. Grafica referente a la pregunta 15. ¿Cuáles crees que podrían ser los beneficios de utilizar métodos de autenticación por biometrías en el contexto laboral?

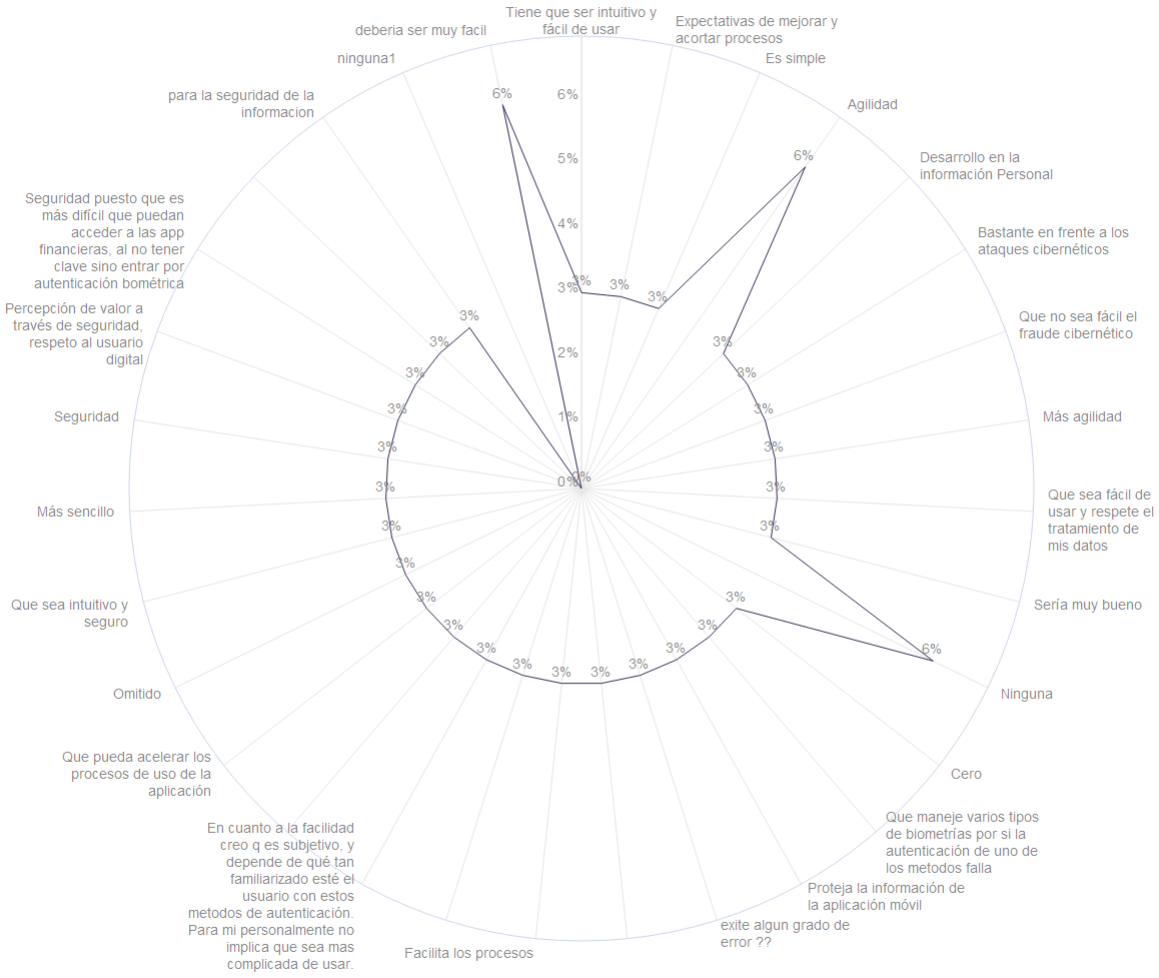


Fuente: Elaboración propia en *DATAVIV*

En la quinceava gráfica, muestra el resultado de la pregunta 15, ¿Cuáles crees que podrían ser los beneficios de utilizar métodos de autenticación por biometrías en el contexto laboral?; Al examinar la diversidad de respuestas proporcionadas por los encuestados, se

depura las respuestas obtenidas y se destaca que el beneficio comúnmente mencionado por casi el 70% de la muestra es la “eficiencia y aseguramiento de los datos”. Esta convergencia en las respuestas refleja una consistencia notable en la percepción de los encuestados. Además, se identifican otros beneficios destacados, como la “confianza”, “la veracidad del dato” y “la mejora de procesos”. Estos hallazgos revelan importantes percepciones sobre los impactos positivos potenciales que la implementación de métodos de autenticación por biometría podría tener en el entorno laboral, abarcando desde la eficiencia operativa hasta la confiabilidad y precisión de la información.

Figura 16. Grafica referente a la pregunta 16. ¿Qué expectativas tienes en cuanto a la facilidad de uso de una aplicación móvil que utilice métodos de autenticación biométricos?



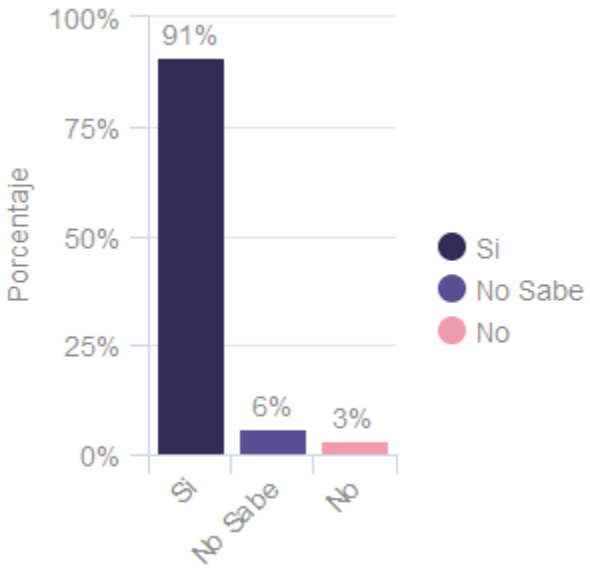
Fuente: Elaboración propia en *DATAVIV*

En la dieciseisava gráfica, muestra el resultado de la pregunta 16, ¿Qué expectativas tienes en cuanto a la facilidad de uso de una aplicación móvil que utilice métodos de autenticación biométricos?; Al examinar la diversidad de respuestas proporcionadas por los encuestados, se depura las respuestas obtenidas y se destaca un consenso en la preferencia por una interacción “fácil, amigable y eficiente”. Los participantes expresan la necesidad de que los responsables de la aplicación móvil estén atentos a garantizar una

experiencia sencilla y receptiva. Este enfoque es crucial para fomentar la aceptación y adopción de estas tecnologías, asegurando que los usuarios no sean reacios a incorporarse a este ámbito. La atención a la facilidad de uso se percibe como un factor clave para proteger la identidad digital y fomentar una transición suave hacia métodos de autenticación biométricos en los dispositivos móviles.

Figura 17. Grafica referente a la pregunta 17. ¿Te gustaría realizar trámites documentales donde la confirmación de su identidad sea remota, evitando el traslado a sitio?

	N	%
Si	30	91%
No Sabe	2	6%
No	1	3%
TOTAL	**33**	**100%**



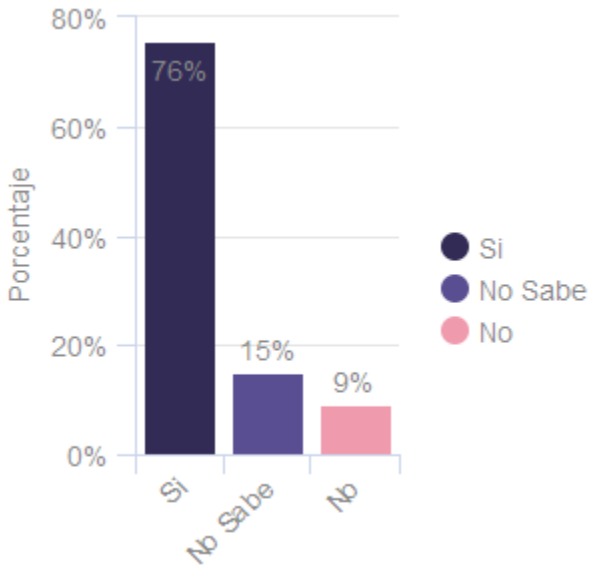
Fuente: Elaboración propia en *DATAVIV*

En la diecisieteava gráfica, muestra el resultado de la pregunta 17, ¿Te gustaría realizar trámites documentales donde la confirmación de su identidad sea remota, evitando el traslado a sitio?; La aceptación de esta propuesta por parte del 91% de la muestra sugiere un interés generalizado en la simplificación y validación de la identidad en los procesos cotidianos, los encuestados muestran su preferencia por la posibilidad de realizar trámites sin la necesidad de trasladarse a un lugar específico, respaldando la idea de validar la identidad de forma remota. No obstante, es importante destacar que el 9% restante de la muestra no

tiene una postura definida o no se siente cómodo con la idea, subrayando la necesidad de abordar consideraciones individuales y posibles desconfianza en la implementación de procesos de validación de identidad remota.

Figura 18. Grafica referente a la pregunta 18. ¿Consideras que la implementación de biometrías en una aplicación móvil mejoraría la eficiencia y seguridad en tu lugar de trabajo?

	N	%
Si	25	76%
No Sabe	5	15%
No	3	9%
TOTAL	**33**	**100%**

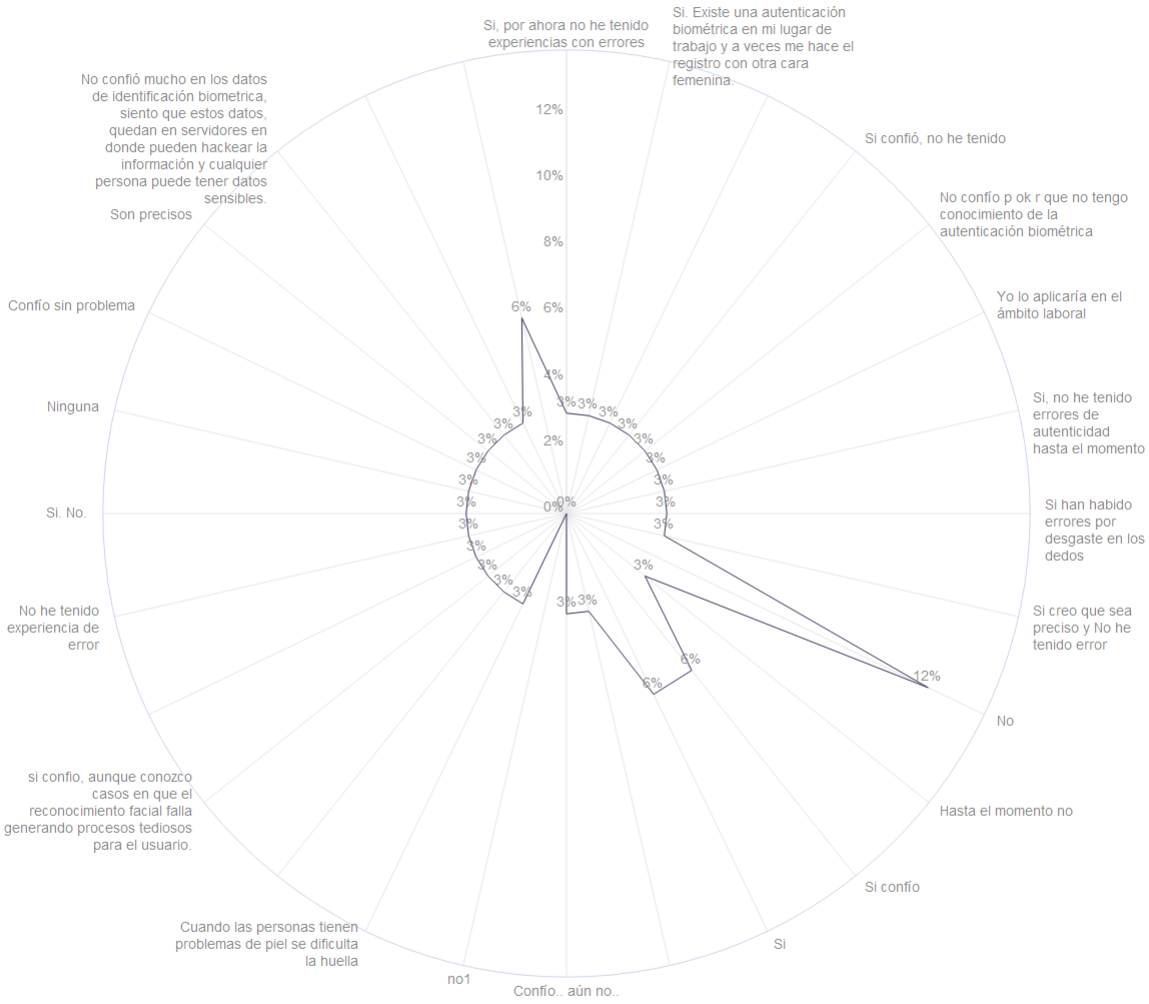


Fuente: Elaboración propia en *DATAVIV*

En la dieciochoava gráfica, muestra el resultado de la pregunta 18, ¿Consideras que la implementación de biometrías en una aplicación móvil mejoraría la eficiencia y seguridad en tu lugar de trabajo?; se observa que el 76% de la muestra considera que la biometría tiene el potencial de mejorar tanto la eficiencia como la seguridad en el entorno laboral. Sin embargo, es relevante destacar que un significativo 24% de los participantes no tiene una postura clara al respecto o no está de acuerdo con esta funcionalidad. Este hallazgo origina una preocupación, sugiriendo que una proporción considerable de empresas quizás no haya incorporado esta cultura de seguridad biométrica entre sus empleados. Esto subraya la importancia de validar no solo con los fabricantes de aplicaciones móviles, sino también de

implementar pautas y campañas informativas para sensibilizar a los usuarios sobre la relevancia y seguridad inherente a la tecnología biométrica.

Figura 19. Grafica referente a la pregunta19. ¿Confías en la precisión de los métodos de autenticación biométrica? ¿Has tenido alguna experiencia de error o falsa identificación?;

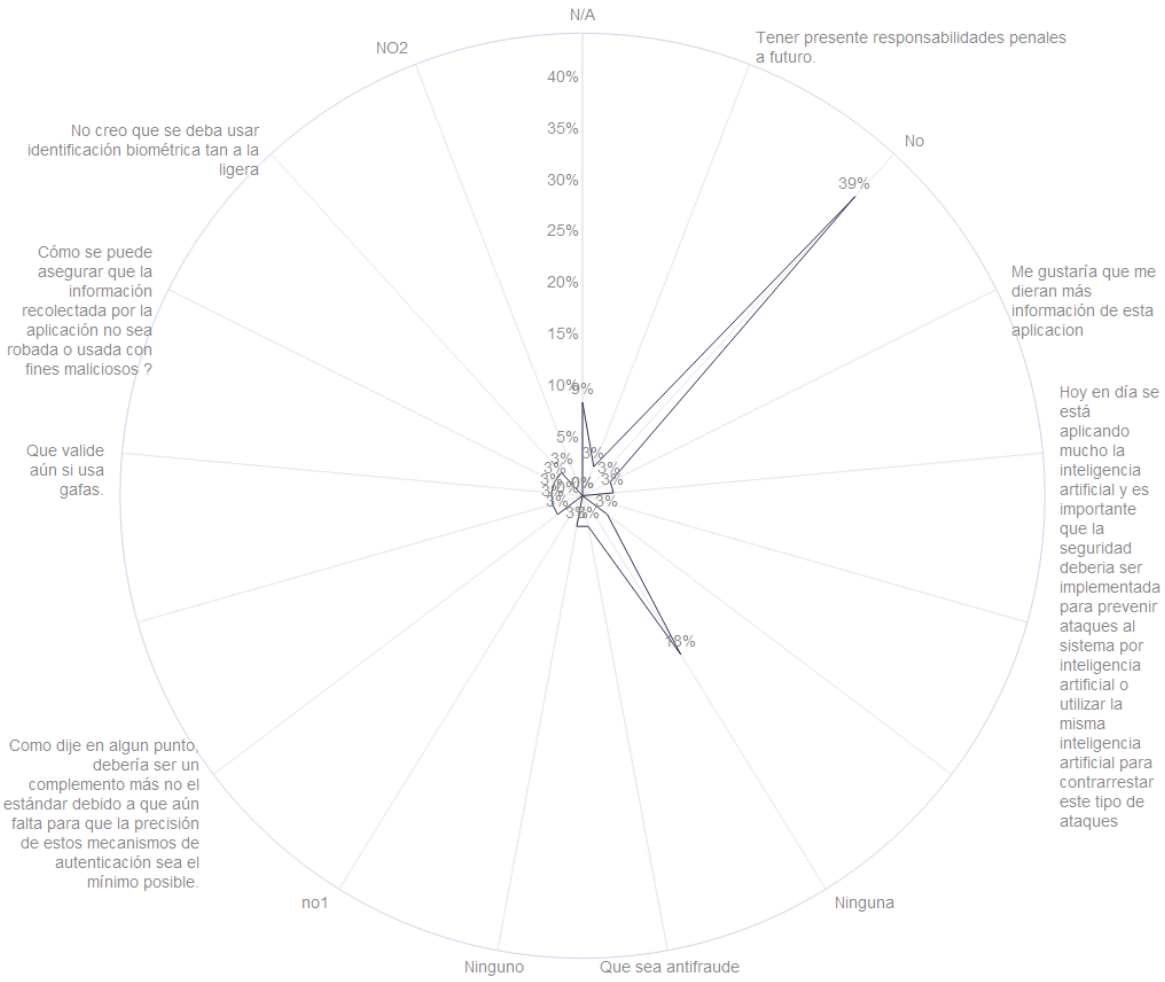


Fuente: Elaboración propia en *DATAVIV*

En la diecinueveava gráfica, muestra el resultado de la pregunta 19, ¿Confías en la precisión de los métodos de autenticación biométrica? ¿Has tenido alguna experiencia de

error o falsa identificación?; Al analizar la diversidad de respuestas proporcionadas por los encuestados, y comparándolo con las respuestas obtenidas a lo largo de esta encuesta para la investigación, donde los encuestados perciben la biometría facial como segura, eficiente y ágil. Surge una preocupación significativa, ya que más del 50% de los encuestados en esta pregunta y basándonos en la convergencia de las respuestas, aún no confían plenamente en estos métodos de autenticación. Esta tendencia sugiere la necesidad de que los fabricantes de aplicaciones móviles consideren las experiencias del usuario como un factor crítico para la adopción exitosa de estas tecnologías, y destaca la importancia de abordar las preocupaciones y mejorar la percepción de seguridad de los usuarios hacia los métodos de autenticación biométrica.

Figura 20. Grafica referente a la pregunta 20. ¿Tienes alguna sugerencia o comentario adicional sobre la implementación de la biometría facial en una aplicación móvil?



Fuente: Elaboración propia en *DATAVIV*

En la veinteava gráfica, muestra el resultado de la pregunta 20, ¿Tienes alguna sugerencia o comentario adicional sobre la implementación de la biometría facial en una aplicación móvil?; Al examinar la diversidad de respuestas proporcionadas por los encuestados, Aunque la mayoría de los encuestados indicaron que no tienen sugerencias o comentarios, se examinaron detenidamente las respuestas proporcionadas por aquellos que

ofrecieron retroalimentación más detallada. Se destaca la preocupación expresada por algunos participantes sobre el riesgo de usurpación de la identidad digital, especialmente a través del uso de inteligencia artificial. Asimismo, se señalan inquietudes relacionadas con la falta de una regulación legal local clara, la protección contra ciberataques y cómo mejorar la confianza en la seguridad de los datos faciales. Estos aspectos resaltan la percepción de preocupación e incertidumbre en la población, subrayando la necesidad de abordar estas inquietudes y garantizar las mejores prácticas de seguridad en la implementación de la tecnología biométrica facial para su adopción.

Conclusiones sobre la muestra a la población estándar.

El análisis detallado de cada pregunta de la encuesta, realizada mediante el método de entrevistas semiestructuradas con preguntas abiertas y exploratorias, ha proporcionado una visión integral de la percepción y conocimiento de la muestra en cuanto a los mecanismos de seguridad biométrica. Se ha identificado una variabilidad en el entendimiento de términos y usos de estos métodos para la protección de la identidad; aunque los participantes de la muestra tienden a utilizar estos mecanismos por necesidad para acceder a información, se evidencia una falta de comprensión clara sobre los permisos otorgados a las aplicaciones móviles al utilizar huellas biométricas y faciales.

Inicialmente, la encuesta reflejó un interés positivo en los beneficios que la seguridad biométrica puede aportar en el ámbito diario o laboral. No obstante, las últimas preguntas sobre la confianza y las expectativas revelaron un cambio de tendencia hacia una preocupación. Esta transformación puede atribuirse a diversos factores, como el desconocimiento, experiencias previas con estos servicios o la percepción de que estas tecnologías son susceptibles al aumento del fraude cibernético y a la suplantación de la identidad digital. Estos hallazgos resaltan la importancia de abordar las inquietudes de los

usuarios y la necesidad de una mayor educación sobre el uso seguro y adecuado de los mecanismos biométricos para garantizar una adopción informada y efectiva en el futuro en las aplicaciones móviles.

Entrevista a expertos

Con el propósito de fortalecer la muestra para la investigación, se llevó a cabo un proceso de entrevista con dos expertos en el campo de la identidad digital. Estas interacciones proporcionaron una valiosa perspectiva experta sobre los temas fundamentales relacionados con nuestra investigación. Con este tipo de investigación, se explora aspectos clave, desde las tendencias emergentes hasta los desafíos actuales en el panorama de la identidad digital. Las respuestas detalladas y reflexivas de los expertos a continuación:

1. **Entrevistado Experto No 1.**

   Nombre: Eduin Ordoñez
   Experiencia laboral en identidad digital: 14 años.
   Experiencia e implementación de soluciones de biometría en sector gobierno y sector bancario.

Pregunta	Respuesta
¿Qué tan familiarizado estás con el concepto de biometría para la autenticación de identidad digital?	He aplicado este concepto en procesos de Estado y sector Bancario en Colombia;
¿Qué tipos de biometrías para la autenticación de su identidad en dispositivos móviles conoce o ha utilizado previamente?	Conozco tres tipos de biometría que son: biométrica dactilar, facial y 4-4-2 (captura especial de las 10 huellas dactilares humanas)
¿Qué percepción le genera tener una identidad digital?	Eficiencia en los procesos tecnológicos hoy en día.
¿Qué tipo de información le gustaría recibir antes de utilizar un método de autenticación biométrico en una aplicación móvil?	Es importante conocer qué manejo hará la organización con la toma de esta información.
¿Qué otros métodos de autenticación usan en aplicaciones móviles, podría mencionar los que conoce?,	Conozco y he trabajado en la aplicación biometría móvil dactilar y facial, y son métodos seguros de autenticación, si se

¿además crees que los métodos de autenticación biométrica son más seguras o menos seguras?	trabajan con empresas acreditadas o homologadas con estándares de seguridad y calidad.
¿Qué opinas sobre la implementación de métodos de autenticación por biometrías en una aplicación móvil?	Son seguras, pero como lo decía anteriormente, es importante saber si estas empresas de aplicaciones móviles usan procedimiento regulados por estándares internacionales o locales, que dan mayor confianza al usuario a quien le está compartiendo la información como también estas empresas dan manejo a esta información.
¿Qué preocupaciones o desafíos crees que podrían surgir al implementar métodos de autenticación por biometrías en una aplicación móvil?	La violación a los algoritmos de prueba de vida es una realidad siempre existe la posibilidad de vulnerar la seguridad, por la seguridad evoluciona, hoy en día la biometría es la más segura, pero se sigue trabajando en mejorarla y evolucionarla.
¿Qué factores considerarías importantes para garantizar la privacidad y seguridad de los datos biométricos?	La información no debe salir del estado colombiano, y siempre debe viajar de manera cifrada en la red.
¿Cuáles crees que podrían ser los beneficios de utilizar métodos de autenticación por biometrías en el contexto laboral?	La implementación de métodos de autenticación por biometría en el entorno laboral conlleva beneficios sustanciales, destacando la identificación instantánea al acceder a las oficinas o al realizar trámites. Este enfoque no solo optimiza la eficiencia operativa, sino que también garantiza una identificación idéntica al funcionario correspondiente, asegurando un nivel superior de seguridad y mitigando riesgos asociados con prácticas de autenticación tradicionales. La biometría, al ofrecer un acceso rápido y fiable, no solo agiliza los procesos cotidianos, sino que también establece un estándar de autenticación robusto y personalizado en el ámbito laboral.
¿Qué expectativas tienes en cuanto a la facilidad de uso de una aplicación móvil que utilice métodos de autenticación biométricos?	Mi expectativa es que la aplicación móvil, al emplear métodos de autenticación biométricos, ofrezca una experiencia de manejo desatendido desde cualquier ubicación. La facilidad de uso radica en la capacidad de los usuarios para autenticarse de manera rápida y eficiente, eliminando la necesidad de intervención manual extensiva.
¿Confías en la precisión de los métodos de	Sí, confío en la precisión de los métodos de

autenticación biométrica? ¿Has tenido alguna experiencia de error o falsa identificación?	autenticación biométrica. Con la experiencia en esta área, se ha observado que la autenticación de una huella biométrica es difícil de duplicar, ya que es una parte única del cuerpo del usuario. Además, la inclusión de estándares de procesos y de seguridad de la información ha mejorado continuamente, aumentando la confianza en el uso de estas tecnologías. Actualmente, el sector bancario utiliza ampliamente esta opción para autenticar a sus usuarios, lo que subraya la fiabilidad y aceptación generalizada de la biometría como una medida segura de identificación

2. Entrevistado Experto No 2.

Nombre: Leonardo Maldonado
Experiencia laboral en identidad digital: 19 años.
Experiencia e implementación de soluciones de identidad digital, como firmas electrónicas, biometrías, factores de autenticación y correos electrónicos certificados implementados en el sector privado.

Pregunta	Respuesta
¿qué biometría cree usted que es la más segura y eficaz?	Se debe partir del hecho de que la biometría es probabilística, y siempre tendrá un porcentaje de falsa aceptación o de falso rechazo, por lo cual mi respuesta es que deben combinarse al menos dos tipos de biometría para disminuir el margen de error. La biometría de lectura de iris, con biometría facial es la combinación que el NIST (NIST, 2023) está planteando probar para el 2024.
¿Es seguro el uso de las autenticaciones biométricas?	Las autenticaciones biométricas son razonablemente seguras, pero no infalibles, depende mucho de factores como la calidad de los sensores y la forma en que se implementan.
¿Qué futuro tienen la identificación biométrica en Colombia?	En Colombia se visualiza una tendencia de crecimiento hacia la biometría facial, especialmente con la activación de acceso

	por parte de la RNEC (RNEC, BIOMETRÍA, 2023) a sus bases de datos.
¿Qué medidas de seguridad debemos tener en cuenta a la hora de utilizar métodos de autenticación biométrica?	Se debe proteger de manera especial los datos biométricos, con cifrado avanzado en su tratamiento en tránsito y en reposo, garantizado el control exclusivo por parte del propietario del dato biométrico (privacidad y seguridad por diseño)
¿Cuál es el futuro de la identidad digital en Colombia?	La identidad digital en Colombia es de las más avanzadas de América Latina, y está a punto de ser pionera en la gestión de notificaciones y firmas digitales para los ciudadanos, lo cual será un hito en la gestión de identidad por parte de una entidad de gobierno
¿Cuáles son las grandes falencias del uso de biometrías para autenticación?	Falta incrementar el control de calidad y confiabilidad de los sensores y hardware biométrico por parte de los fabricantes de dispositivos móviles, y estrategias para aumentar la cobertura en usuarios que no tengan posibilidad de poseer dispositivos propios, para una gestión 100% digital.

Conclusiones sobre la muestra a la población experta

En esta muestra obtenida de los dos expertos entrevistados se destacan las siguientes conclusiones:

1. Las respuestas proporcionadas indican una combinación de experiencia práctica, percepciones positivas, conciencia de desafíos de seguridad, y expectativas de eficiencia en la implementación de métodos biométricos. Donde contribuyen significativamente a la comprensión integral de la biometría en el contexto de la identidad digital y la autenticación.
2. Se destaca la importancia del uso de biometrías, como necesidad de medidas de seguridad robustas, el crecimiento de la biometría facial en Colombia, y la importancia de

abordar las limitaciones técnicas y de accesibilidad para lograr una implementación exitosa de la autenticación biométrica.

3. Es muy importante no omitir que hay organizaciones que regulan los procesos de implementación y de seguridad de tecnologías de identidad digital, que aportan capas adicionales de confianza para el proveedor de las aplicaciones móviles tanto como a los usuarios para el uso de autenticación biométrica, que son regulados por instituciones internacionales o por el marco legal local.
4. Se reconoce que las autenticaciones biométricas son razonablemente seguras, pero no infalibles. La seguridad depende de factores como la calidad de los sensores, la implementación y cumplimiento de normas regulatorias para el mejor uso de estas tecnologías, subrayando la necesidad de considerar estos elementos críticos en cualquier sistema biométrico.
5. De acuerdo a la conclusión anterior, la inclusión de estándares de implementación y de seguridad, cubre en gran parte la necesidad de la protección de datos y uso de herramientas para el tratamiento de los datos en tránsito o reposo en la red.
6. Se prevé un crecimiento en el uso de la biometría facial en Colombia, especialmente en la activación de acceso por parte de la RNEC a sus bases de datos. Esta tendencia sugiere un papel cada vez más relevante de la biometría en la identificación digital en el país.
7. La percepción de la identidad digital se asocia con la eficiencia en los procesos tecnológicos, indicando una valoración positiva de cómo la biometría puede mejorar la eficacia de las operaciones cotidianas La preocupación por la privacidad y seguridad de los datos biométricos es evidente, enfatizando la importancia de mantener la información dentro del estado colombiano y transmitirla de manera cifrada para garantizar la integridad y confidencialidad.

Conclusiones finales de la investigación

Sobre la toma de la muestra entre la población estándar y la muestra de expertos, se encontraron conclusiones valiosas, ofreciendo una visión completa sobre la percepción y aplicación de la seguridad biométrica, así como sus implicaciones en el contexto de la identidad digital y la autenticación. Debido a ello se identifican las siguientes conclusiones comparando las dos muestras:

- Ambas poblaciones reconocen que las autenticaciones biométricas son razonablemente seguras, pero no infalibles, dependiendo de factores como la calidad de los sensores y la implementación.

- La percepción positiva de la identidad digital se asocia con la eficiencia en los procesos tecnológicos, pero la preocupación por la privacidad destaca la necesidad de cifrado y control estricto de los datos biométricos.

- En conjunto, estas conclusiones subrayan la importancia de la educación, la transparencia y el desarrollo continuo de estándares para garantizar la adopción segura y efectiva de la autenticación biométrica en aplicaciones móviles, satisfaciendo las necesidades y preocupaciones tanto de la población estándar como de la población experta.

Con lo anterior la investigación es exitosa en varios aspectos:

- **Contribución de Expertos:** La muestra de expertos aporta una comprensión profunda de la biometría facial, incluyendo desafíos y recomendaciones, lo que fortalece la validez de la investigación.
- **Revelación de Inquietudes:** La identificación de inquietudes y la transformación hacia la preocupación en la población estándar demuestra que la investigación

abordó temas importantes y proporciona oportunidades para futuras intervenciones educativas.

- **Perspectiva Integral:** La combinación de datos de la población estándar y expertos ofrece una perspectiva integral, permitiendo una evaluación más completa de la viabilidad de la biometría facial como identidad digital.
- **Previsión de Crecimiento**: La previsión de crecimiento en el uso de la biometría facial, especialmente respaldada por la activación de acceso por parte de la RNEC, indica una dirección positiva y relevante para la implementación futura.

Para soportar el anterior párrafo, durante la preparación de esta investigación la RNEC, el 25 de noviembre de 2023, hizo el lanzamiento de la identidad digital llamada “cedula digital 2.0” (Tiempo, 2023), junto con un nuevo decreto “resolución 27145 de 2023” (RNEC, Resolución 27145 de 2023, 2023), donde los ciudadanos que apliquen a esta solución tendrán acceso a los siguientes cuatro servicios:

- **Identificación:** los colombianos se podrán identificar fácilmente en escenarios presenciales y medios digitales (Infobae, 2023).
- **Transacciones virtuales:** se podrán hacer mediante el protocolo de identidad OIDC, con altos niveles de seguridad a través de autenticación biométrica facial y PIN (Infobae, 2023).
- **Notificaciones:** se podrán recibir y gestionar notificaciones de entidades públicas y financieras con la confirmación de lectura y documentos adjuntos (Infobae, 2023).
- **Documentación:** se podrán recibir documentos, leerlos y firmarlos con certificado digital, almacenarlos y contar con la posibilidad de compartir a terceros (Infobae, 2023).

Con lo anterior respalda también la investigación dado a que es necesario que la población en Colombia y las empresas que realizan aplicaciones móviles, deben iniciar la adaptabilidad de estos recursos para eficiencia de procesos como para la seguridad de los datos biométricos, porque se está iniciando una transición a esta tecnología con ayuda y supervisión del estado.

Además, la investigación proporciona una base sólida para la comprensión de la viabilidad de la biometría facial como identidad digital, destacando áreas de mejora y subrayando la importancia de abordar las preocupaciones de los usuarios para garantizar una adopción informada y efectiva en el contexto de las aplicaciones móviles.

Finalmente, cabe recordar que el proceso de investigación es cíclico al ser esta una investigación cualitativa. Por lo que los resultados y conclusiones mostradas en este documento son un primer acercamiento a una investigación que debe ser iterativa. Los resultados obtenidos nos permiten un acercamiento a los problemas, situaciones y posibles alternativas que la identificación digital tiene en Colombia, pero es claro que estos pueden ser analizados con mucha mayor profundidad. He acá la importancia del ciclo de investigación mencionado en el documento. Para un futuro, por ejemplo, se puede continuar con un acercamiento más específico hacia los problemas o ventajas de la identidad digital en las votaciones locales, o de la misma forma, un acercamiento a los problemas que pueden desencadenarse en el futuro por la falta de conocimiento a la hora de compartir información única como las biometrías a terceros que no cumplen con estándares de seguridad.

Listado de referencias

Chenou, J.-M. (2021). The contested meanings of cybersecurity: evidence from post-conflict Colombia. *Conflict, Security & Development* , 1-19.

D.A. Reid, S. S. (2013). Chapter 13 - Soft Biometrics for Surveillance: An Overview. En S. S. D.A. Reid, *Handbook of Statistics* (págs. 327-352).

Infobae. (24 de 11 de 2023). *Registraduría lanza Cedula digital 2.0: conozca los servicios que trae y cómo actualizar el documento*. Obtenido de https://www.infobae.com/colombia/2023/11/26/registraduria-lanza-cedula-digital-20-conozca-los-servicios-que-trae-y-como-actualizar-el-documento/

Lips, S. B. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. *Communications in Computer and Information Science book series (CCIS,volume 1349)*.

Martin, L. (2009). Biometrics. En L. Martin, *Computer and information security Handbook* (págs. 645-659).

Mayernik, M. (2023). METADATOS. *Anales de Documentación; Murcia* , 1-20.

MONDRAGÓN, N. S. (2020). *GENERACIÓN DE IDENTIDAD DIGITAL PARA EL ACCESO A LOS SERVICIOS CIUDADANOS DIGITALES EN COLOMBIA.* Bogotá: Universidad de los Andes.

NIST. (2023). *NIST Nationatl Institute of Standars and Technology*. Obtenido de https://www.nist.gov/

Paul A. Grassi, M. E. (2017). Digital Identity Guidelines. *NIST Special Publication 800-63-3*.

Registraduría Nacional del estado Civil. (2016). Resolución 5633 de 2016. Colombia.

RENEC, R. N. (s.f.). *www.registraduria.gov.co.* Obtenido de https://www.registraduria.gov.co/Que-es-un-sistema-biometrico.html

República de Colombia. (1999). Ley 527 de 1999. *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."*. Colombia.

Republica de Colombia. (2012). Decreto 19 de 2012. *"Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública."*. Colombia.

República de Colombia. (2012). Ley 1581 de 2012 Protección de Datos Personales. Colombia.

RNEC. (2023). *BIOMETRÍA*. Obtenido de https://wsp.registraduria.gov.co/biometria/

RNEC. (11 de 2023). *Resolución 27145 de 2023*. Obtenido de https://www.registraduria.gov.co/IMG/pdf/20231124_resolucion-27145.pdf

Sampieri, R. H. (2014). Metodología de la investigación. México DF: McGrawHill.

Tiempo, E. (26 de 11 de 2023). *Lanzan la cédula digital 2.0*. Obtenido de https://www.eltiempo.com/economia/finanzas-personales/cedula-digital-2-0-en-colombia-trae-novedades-asi-puede-actualizarla-o-tramitarla-829415

Valentyna Tsap, S. L. (2020). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. *Electronic Government and the Information Systems Perspective*, 159–173.

Vásquez, G. B. (13 de Septiembre de 2023). *El tiempo.* Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-que-informacion-se-pudieron-haber-robado-en-el-ciberataque-805730

Yopazá, W. R. (2020). *GUÍA DE METADATOS.* Archivo general de la nación Colombia.

Anani, W., & Ouda, A. (2017). The importance of human dynamics in the future user authentication. 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE).

Biometría de reconocimiento de las venas de los dedos. (2021, septiembre 7). Miteksystems.com. https://www.miteksystems.com/es/blog/biometria-de-reconocimiento-de-venas-de-los-dedos
Biometría para identificación y autenticación. (s/f). Thales Group. Recuperado el 16 de septiembre de 2023, de https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria
Colombia, T. (2022, abril 27). La tasa de intentos de fraude digital en Colombia aumentó un 134 % de 2019 a 2021. La tasa de intentos de fraude digital en Colombia aumentó un 134 % de 2019 a 2021; TransUnion Colombia. https://noticias.transunion.co/la-tasa-de-intentos-de-fraude-digital-en-colombia-aumento-un-134--de-2019-a-2021/
de la información se verificarán los siguientes dominios:, F. a. las P. de S. (s/f). Dominios de la ISO270001 - aplicadas a las políticas de seguridad de la información. Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.registraduria.gov.co/IMG/pdf/20210706_dominios-iso-270001.pdf
Decreto 19 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=45322
Decreto 2364 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583
Ley 527 de 1999 - Gestor Normativo. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276
Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
Mayhew, S. (2018, febrero 1). History of biometrics. Biometricupdate.com. https://www.biometricupdate.com/201802/history-of-biometrics-2
NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de http://sarlaft.fiduagraria.gov.co/meci_files/ISO%2027001%202013.pdf
Normatividad. (s/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://observatorioecommerce.mintic.gov.co/797/w3-propertyvalue-377739.html
Pablo. (2021, agosto 26). Biometría para principiantes: ¿sabes qué es? Alice Biometrics. https://alicebiometrics.com/biometria-para-principiantes/
Pablo. (2022, marzo 10). 5 técnicas biométricas comunes comparadas. Alice Biometrics. https://alicebiometrics.com/5-tecnicas-biometricas-comunes-comparadas/
Portafolio. (s/f). RappiPay implementará biometría facial con apoyo de la Registraduría. Portafolio.co. Recuperado el 16 de septiembre de 2023, de https://www.portafolio.co/innovacion/alianza-entre-rappipay-y-registraduria-para-evitar-fraude-con-biometria-facial-585261
¿Qué es el reconocimiento de voz y cómo funciona? (2021, abril 14). RecFaces. https://recfaces.com/es/articles/reconocimiento-voz
Qué es y cómo funciona el reconocimiento facial. (s/f). Org.Co. Recuperado el 16 de septiembre de 2023, de https://digitalid.karisma.org.co/2021/07/01/que-es-reconocimiento-facial/
Reconocimiento de Iris. (s/f). NEC. Recuperado el 16 de septiembre de 2023, de https://co.nec.com/es_CO/global/solutions/biometrics/iris/index.html
Registraduría Nacional del Estado Civil. (s/f). Registraduría Nacional del Estado Civil - La Registraduría del Siglo XXI. Registraduría Nacional del Estado Civil. Recuperado el 16 de septiembre de 2023, de https://www.registraduria.gov.co/Acceso-a-la-base-de-datos-biometrica-de-la-Registraduria-Nacional-del-Estado.html
Ventas de comercio electrónico en Colombia crecieron 40% y llegaron a $40 billones. (s/f). Diario La República. Recuperado el 16 de septiembre de 2023, de

https://www.larepublica.co/empresas/las-ventas-de-ecommerce-en-colombia-crecieron-40-y-llegaron-a-40-billones-3305200
(S/f). Gov.co. Recuperado el 16 de septiembre de 2023, de https://www.registraduria.gov.co/IMG/pdf/RESOLUCION_5633.pdf