"Adopción de biometría como mecanismo de autenticación en las empresas costarricenses"

Adoption of biometrics as an authentication mechanism in Costa Rican companies

Pablo Quirós Víquez[1]

Andy Fabricio Gómez[2]

Julio Córdoba Retana[3]***,***

Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)

2022

Resumen

El incremento en el uso de las tecnologías de información ha hecho que crezcan el riesgo y la cantidad de ataques informáticos (Team, V.R., 2021), ante esto se hace necesario que se construyan controles de acceso que brinden medidas de seguridad informática más sofisticadas. Resulta de interés para esta investigación, estudiar la adopción de estos mecanismos en Costa Rica por medio la siguiente pregunta de investigación: ¿Cuál es el nivel de adopción de la biometría en empresas en Costa Rica y cómo se puede incrementar su uso? Por medio de un estudio cualitativo y de tipo descriptivo, con ayuda de entrevistas a representantes de empresas del país se indagó si se utiliza la biometría o no; si se considera importante en las organizaciones y cuáles son las consecuencias de su uso o falta de uso. Se encontró que más de la mitad de los entrevistados utilizan algún sistema de autenticación por biometría en su lugar de trabajo; que estos no son utilizados necesariamente por empresas con mayores recursos económicos por lo que, dados esos resultados, se recomienda

---

Estudiantes de la especialización de Ciberseguridad en la Universidad Latinoamericana de Ciencia y Tecnología.

[1] *Pablo Quirós Víquez es egresado de Ciencias de la Computación de la UCR y labora como Ingeniero de soporte técnico para una empresa transnacional.*

https://orcid.org/0000-0003-1455-8008 *pquiros00@gmail.com*

[2] *Andy Fabricio Gómez está actualmente labora para una empresa transnacional.*

https://orcid.org/0000-0002-9411-5209 *fabricio.andy@live.com*

[3] *Julio Córdoba Retana es profesor de Proyecto Final en ULACIT.*

jcordobar022@ulacit.ed.cr

la adopción de los sistemas de lectura huella dactilar como el más seguro, de menor inversión y la lectura de retina como uno de los más eficiente.

Palabras clave: biometría, controles biométricos, huella digital, lectura de retina, control de acceso.

Abstract

The increase in the use of information technologies has increased the risk and the number of computer attacks (Team, V.R., 2021), in view of this it is necessary to build access controls that provide more sophisticated computer security measures. It is of interest for this research to study the adoption of these mechanisms in Costa Rica through the following research question: What is the level of adoption of biometrics in companies in Costa Rica and how can its use be increased? Through a qualitative and descriptive study, with the help of interviews with representatives of companies in the country, it was inquired whether biometrics is used or not; if it is considered important in organizations and what are the consequences of its use or lack of use. It was found that more than half of the interviewees use some biometric authentication system in their workplace; that these are not necessarily used by companies with greater economic resources, therefore, given these results, the adoption of fingerprint reading systems is recommended as the safest, with the least investment, and retinal reading as one of the most efficient.

Keywords: biometrics, biometric controls, fingerprint, retina reading, access control.

Introducción

Tomando en cuenta, “el incremento de los riesgos y amenazas a la seguridad digital”, el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y la Universidad de Oxford (2020:38) señalan que, las empresas siempre están a la búsqueda de reforzar y mejorar sus mecanismos de autenticación, pero: ¿cuáles empresas se encuentran menos vulnerables ante estos fraudes? ¿las que emplean métodos de autenticación física o lógica? ¿cuál es más efectivo? En la actualidad, muchas empresas están optando por implementar la biometría como mecanismo de identificación y verificación de identidad, pues les brinda mayor seguridad, no solo a ellas como propietarias, sino también a las expectativas de protección y comodidad para sus clientes.

En las últimas décadas según HID Global Corporation (2020), la tecnología ha proporcionado múltiples opciones para controlar los accesos y la autentificación ha sido estratégica como medida de seguridad; desde la implementación de las tecnologías de arrastres hasta las

tarjetas inteligentes y los accesos por contraseñas que han cumplido con sus novedosos objetivos. Sin embargo, la delincuencia ha evolucionado de la mano con ellas y las ha vuelto vulnerables a falsificaciones y robos.

Ante esta problemática, la biometría ha surgido con el propósito de crear credenciales irremplazables basadas en los rasgos únicos físicos que poseen los seres humanos proporcionando así, alta fiabilidad y facilidad de uso.

En Costa Rica, el uso de identificación biométrica se ha adoptado progresivamente, especialmente en años recientes, con la implementación de tecnologías para uso cotidiano en controles de acceso y sistemas de verificación de identidad en dispositivos y plataformas de entidades públicas y privadas.

Además, ha habido iniciativas para crear marcos legales que regulen su uso y el caso de la creación de una plataforma nacional de información biométrica, administrada por el Tribunal Supremo de Elecciones (TSE), que no ha estado exenta de controversias y posiciones en contra del riesgo de que su información sea filtrada a terceros (Mora, 2020).

A pesar de que las tecnologías de identificación por biometría tienen desafíos importantes que tienen que abordarse y no están exentas de ser vulneradas, su adopción ha proporcionado una capa de seguridad más robusta, en comparación con los sistemas de autenticación por nombre de usuario y contraseña, que han sido utilizados históricamente y que sufren de múltiples vulnerabilidades, tanto en su implementación y mecanismo de funcionamiento, como por malas prácticas de los usuarios que no siguen buenas prácticas para crear contraseñas robustas.

La seguridad es un área que ha sido estratégica en la historia de las transacciones. A través del tiempo se han desarrollado mecanismos de distintos tipos para salvaguardar bienes, materiales e información y el desarrollo de tecnologías de la información y la informática han cambiado la forma en que funcionan los sistemas de seguridad.

Ante la incorporación de las tecnologías de la información en una cantidad mayor de áreas de la vida cotidiana, en las que el acceso no autorizado de terceros tiene consecuencias cada vez más serias y que resulta en pérdidas económicas, violaciones a la privacidad y afectación a la reputación de las organizaciones y personas, es crítico salvaguardar con las mejores herramientas existentes los datos contenidos en estos sistemas, de manera eficiente y buscando minimizar el error humano cuando los usuarios las configuren y utilicen.

El estado de la adopción del uso de biometría en Costa Rica es de especial interés, pues su uso es de reciente adopción en el país y no se ha generalizado con la rapidez suficiente, poniendo en riesgo a usuarios y organizaciones que manejan datos informáticos.

Pregunta de investigación

¿Cuál es el nivel de adopción de la biometría en las empresas en Costa Rica y cómo se puede incrementar su uso?

Objetivo general

Evaluar el estado actual de adopción de biometría de empresas en Costa Rica, así como los riesgos y consecuencias de no incrementar su uso, a fin de persuadirlas a incrementarlo.

Objetivos específicos

- Evaluar los tipos de mecanismos de seguridad utilizados por las empresas en Costa Rica.
- Valorar las características de seguridad que ofrecen distintos mecanismos biométricos.
- Comparar el uso de biometría en Costa Rica, con respecto a casos en otros países de América Latina para valorar las ventajas y desventajas de incrementar la seguridad biométrica en el país.
- Proponer mecanismos de biometría que pueden ser adoptados por empresas en Costa Rica, para mejorar su seguridad.

Forma de alcanzar los objetivos

Para alcanzar los objetivos de esta investigación se realizó una revisión bibliográfica en distintas bases de datos como EBSCOhost y Google Scholar, también en sitios web oficiales de universidades, organizaciones y artículos que demuestran información auténtica y que aporta al análisis requerido.

Se tomaron en consideración, artículos provenientes de organizaciones internacionales como la Organización de las Naciones Unidas (ONU); la Organización para la Seguridad y la Cooperación en Europa (OSCE); el Instituto Nacional de Ciberseguridad de España (INCIBE) y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT) que abordan temas relacionados a la seguridad biométrica.

Revisión bibliográfica

Los sistemas de autenticación basados en parámetros fisiológicos han crecido en popularidad y han sido adoptados ampliamente para la autenticación de usuarios en dispositivos, organizaciones y aplicaciones. Se basan en el principal aspecto de que estas características físicas de biometría son exclusivas y específicas para cada persona, lo que los convierte en controles más robustos de autenticación (Joseph *et al.*, 2022).

En comparación con sistemas como el uso de palabras de usuario y contraseñas, que presentan múltiples vulnerabilidades, entre las que se destacan la longitud del texto, el tipo de caracteres (alfa numéricos y símbolos), el período de tiempo que se lleva usando una misma contraseña, el olvido, robo o pérdida por parte de los usuarios; la autenticación basada en biometría

ofrece capas de seguridad adicionales que la hacen más segura por su asociación única a cada usuario, de mayor facilidad de uso al no tener que memorizar información que puede olvidarse fácilmente, cuando se utilizan cada vez más contraseñas para acceder a diferentes sistemas y dispositivos. Estas características hacen que estos mecanismos de autenticación sean más difíciles de vulnerar por atacantes.

La pandemia de COVID-19 que afectó la mayoría de las actividades humanas desde el año 2020, modificó la forma de interactuar con otras personas, debido a las restricciones de distanciamiento social y cantidades de personas que podían reunirse. Entre los cambios que han ocurrido de forma masiva están las reuniones virtuales y el aumento de las compras por Internet. Además, se originó la necesidad del desarrollo de controles biométricos, como es el caso de reconocimiento facial en rostros cubiertos con mascarillas para boca y nariz (Guo, 2021).

En el caso de Costa Rica, los controles de autenticación biométricos han sido adoptados e incluidos en los pasaportes nacionales, emitidos a partir del año 2022, acerca de que características tecnológicas incluye este nuevo documento y las ventajas que ofrece esta nueva tecnología, la directora general de Migración y Extranjería, Raquel Vargas (2021) explicó:

> es un documento que cuenta con un chip que tiene los datos biométricos de la persona: características de su cara, huellas, así como su información personal. “Este pasaporte nos pone a la altura de las últimas tendencias de movilidad a nivel global. Impide la falsificación y alteración, lo que lo convierte en un documento muy seguro al ser de alta tecnología”.

El Banco de Costa Rica (BCR) implemento a partir de marzo del 2021, la biometría facial en su aplicación para realizar transacciones como un mecanismo de seguridad y agilización de trámites como SINPE Móvil, pago de servicios, trámites de tarjetas, entre otros. José Ledezma Fallas, Gerente de Banca Digital (2021) expresó:

> “Esta nueva facilidad que brindamos a nuestros clientes, es parte de la Transformación Digital de la entidad. La Biometría Facial permite sustituir la contraseña que actualmente se digita para ingresar a la aplicación, por lo que ahora el ingreso es más ágil”.

El Banco Nacional de Costa Rica (BNCR), también dio el paso de la utilización de biometría en sus trámites para los clientes. Fabián Rodríguez, director de BN Digital (2021) explicó:

> “Siempre estamos pensando en cómo mejorar la experiencia digital de nuestros clientes y en esta oportunidad incorporamos la biometría aplicada a los servicios bancarios que fortalece aún más los robustos esquemas de seguridad que tienen los clientes del Banco Nacional para ingresar a sus cuentas, además de que, por la rapidez, se les facilita la interacción bancaria del servicio, a la altura de las mejores tecnologías mundiales. Esta es una iniciativa desarrollada por colaboradores de la institución”

BAC Credomatic, también ha implementado el uso de biometría y uso de inteligencia artificial para la ejecución de transacciones para sus clientes. Bac Credomatic (2022: 79) expresó a través de un Informe integrado 2021 que:

> Conforme avanzamos hacia un mundo cada vez más digital, la seguridad en un entorno de mínima fricción para el cliente toma más protagonismo dentro de las soluciones y herramientas que desarrollamos... Por esto, hemos invertido en tecnologías de seguridad que, aprovechando la inteligencia artificial y la biometría, ofrecen controles a nuestros clientes sin hacer más complejo el manejo de sus finanzas en nuestras plataformas.

Al analizar el aspecto de transacciones digitales en una comparación con países de Latinoamérica, específicamente: Argentina, Belice, Bolivia, Brasil, Chile, Colombia, República Dominicana, Ecuador, El Salvador, Guatemala, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela.

Costa Rica registra mayores números y una mejor situación de uso de banca por Internet, compras por Internet y pagos digitales, algunas de las cuales incluyen controles de autenticación biométricos para su uso. Así, el número de líneas telefónicas por cada 100 habitantes se incrementó en 20% entre 2014 y 2017 (Finnovista, 2019). Además, según el Banco Central de Costa Rica:

> 90% de la población está usando un teléfono móvil con un proveedor de servicio de Internet y la mitad de las transacciones sin efectivo son ejecutadas por tarjetas bancarias sin contacto. Miembros de la Asociación FinTech de América Central y el Caribe señalan que 82% de la biometría en Costa Rica es enviada por medio de la infraestructura digital del país (Sunel, 2020).

La innovación que ha traído la biometría para el reconocimiento de personas mediante características fisiológicas y de comportamiento ha automatizado y perfeccionado los controles de accesos, los cuales se muestran cada vez más comunes por la confidencialidad que requieren (Vega *et al.*, 2021) aun así, algunos mecanismos poseen ventajas sobre otros. No obstante, a continuación, se detallan las particularidades de múltiples opciones de seguridad biométrica.

El mecanismo de huella dactilar es muy utilizado en oficinas, teléfonos móviles, ordenadores y hasta en hogares. Se considera muy seguro, porque se apoya de los patrones dactilares que son irrepetibles e invariables; estos patrones se presentan generalmente, en forma de espirales, bucles y arcos, pero dentro de ellos mismos muestran un sinfín de variables que elevan la precisión al momento de la identificación, siendo hasta ahora el más utilizado, además de que entre todos es el más barato (Guízar *et al.*, 2021).

La técnica de reconocimiento facial es realizada mediante un algoritmo que calcula y analiza la longitud de y entre los ojos, nariz, boca, cejas, ángulos faciales y forma de la cara (Suarez y Guarda, 2019). Puede reconocer a una persona en base a una imagen o fotografía, proyectándola a una imagen digital; generalmente es utilizada como sistema de vigilancia privada y pública, a través del uso de cámaras de video. Domingo Jaramillo (2021: 25) afirmo lo siguiente:

> nos encontramos ante una técnica que, si bien es de gran utilidad, pues coadyuva a preservar la seguridad ciudadana al contribuir a identificar de forma automática a individuos delincuentes y terroristas conocidos, así como otros a los que se les ha impuesto una medida de seguridad (aun de tipo administrativo), como podría ser el alejamiento y prohibición de acceso a determinados espacios.

Por las vulnerabilidades que esta presenta, si se utilizan como sistema de control de acceso, cualquier persona podría alterar el rostro como, por ejemplo: dejándose crecer la barba, utilizando lentes o gafas solares. Es importante no olvidar que el rostro cambia a través de los años, inclusive, en casos extremos, una persona podría someterse a procesos de cirugías plásticas o usar máscaras profesionales confeccionadas a la medida para poder parecerse a otro individuo que posea acceso con este mecanismo y así, acceder a áreas restringidas que no les competen.

Sin embargo, este método podemos verlo implementado en muchos teléfonos inteligentes, donde se guardan datos muy sensibles. En palabras de Suarez y Guarda (2019: 27): “El reconocimiento facial es muy bueno, pero menos seguro que el análisis de iris y de huellas digitales teniendo la gran ventaja de no ser un método invasivo”.

Refiriéndose al mecanismo de reconocimiento del iris. Peláez y Gutiérrez (2021) destacan que la identidad o información que posee el iris es extraída mediante un escaneo con cámara de luz infrarroja para luego, proceder al debido almacenamiento en una base de datos que sirve para hacer el futuro reconocimiento del sujeto en cuestión.

Además, Peláez y Gutiérrez (2021) expresan que el iris es un músculo que presenta identidad desde el momento en que los seres humanos nacen, pero esta identidad se solidifica cuando la persona tiene un año de nacida para no alterarse más, a menos que sea por factores externos.

Un análisis realizado bajo el marco del Congreso Internacional de Investigación y la Academia Journals por parte del Ing. Rosa María Soto Mendiola, el Dr. Máximo López Sánchez, el Dr. Raúl Pinto Elías y Jesús Lorenzo Pineda Jaimes (2019) demuestra que, a través de la conexión que posee el iris con órganos importantes del cuerpo, si un órgano no estuviese estable, el iris puede presentar alteraciones en la estructura, lo que sugiere que el uso de la biometría a través del reconocimiento del iris puede no ser tan confiable y seguro.

Debido a la singularidad que la mano presenta en cada ser humano, Sánchez (2020) menciona que, el método biométrico de geometría de la mano toma sus bases en las formas y medidas que esta alberga y que la seguridad y confiabilidad que brinda le ha generado éxito como medida biométrica.

Es un hecho que la mano ha tomado tanto auge en el uso como sistema de reconocimiento que se puede ver implementado hasta en aparatos tecnológicos comunes, como lo son los teléfonos inteligentes en funciones tan simples como desbloquear la pantalla principal, acceder a aplicaciones e inclusive, hasta para tomar una fotografía.

El reconocimiento por voz es generalmente utilizado en sistemas de respuesta por voz interactiva mediante lo que se conoce como “Inteligencia Artificial” (IA) (Barrios, 2020), este

sistema fácilmente se encuentra implementado en aplicaciones como Asistente de Google; Siri en dispositivos Apple; Alexa desarrollado por Amazon y centros de atención de llamadas telefónicas.

Sánchez (2020) indica que, tiene la particularidad de que, si se utiliza como sistema de control de acceso, la precisión del reconocimiento puede influir por circunstancias del ambiente que lo rodee, como los sonidos de fondo o inclusive, mostrarse vulnerable a la falsificación mediante una grabación de voz de la persona con privilegios de acceso.

El avance de la tecnología y las ansias de ir más allá está actualmente introduciendo el sistema de reconocimiento vascular; novedoso al mercado, lo que da un paso al frente del análisis de las características físicas externas del cuerpo humano y así, examinar patrones internos del cuerpo como lo son: las venas de los dedos o manos para reducir aún más, los factores que pueden incidir negativamente en la fiabilidad y seguridad de los procesos de reconocimiento de identidad biométrica actuales; aunque existe cierto rechazo a esta tecnología por ser muy nueva, esto no le resta puntos a lo atractivo que suena para el futuro de la biometría (Cruz, 2020).

Junto con el desarrollo de las tecnologías de biometría ha habido discusiones controversiales, en cuanto al alcance que estas tienen, por cuanto recolectan y almacenan información fisiológica de las personas, que por sus características únicas de poder ser asociadas a un individuo de forma altamente precisa, las hacen muy íntimas y por lo tanto, hay mucha atención, en cuanto a quién debe y puede recolectar y mantener esta información; qué controles se deben seguir para resguardarla y con quién o quiénes se puede compartir o no. Refiriéndose a la recolección de datos biométricos para investigaciones comerciales y empresariales, Sánchez (2021) concluye que:

> implica el tratamiento de información sensible y de naturaleza privada, la cual cuenta con elementos muy marcados, ligados a la esfera de la intimidad y de los derechos individuales de la persona, para lo que, como mínimo, se requiere un consentimiento informado y razonado del sujeto de estudio en investigaciones que conlleven el uso de herramientas biométricas.

Una de las discusiones más importantes en Costa Rica se dio como consecuencia del intento de la creación de la Unidad Presidencial de Análisis de Datos (UPAD) por parte de la Presidencia de Costa Rica en el expediente N.º 21.818 de la Asamblea Legislativa de la República de Costa Rica. Dicho expediente fue criticado por múltiples sectores de la sociedad. El Congreso denunció en un informe sobre el expediente (Asamblea Legislativa de la República de Costa Rica, 2020: 65), que:

> la redacción del decreto no ponía ningún límite a la información confidencial que la UPAD podía solicitar, lo cual incluye —como lo consigna la periodista Sofía Chinchilla del periódico La Nación- “información sobre origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros”.

Casos como los anteriores contextualizan la creciente preocupación y hasta resistencia de segmentos de la sociedad costarricense sobre consentir en compartir su información biométrica con instituciones consolidadas y la preocupación es aún mayor, cuando no se sabe si se comparte con terceros.

Comparando la situación del uso de biometría en Costa Rica con el caso de otros países en América Latina; en Argentina, el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) recopila datos biométricos de las personas en ese país, incluyendo a quienes entran al territorio. En particular, recopila la información de huellas digitales y rostros en bases de datos, para que sean utilizada por las fuerzas de seguridad del país (Ríos, 2020).

Tiene un enfoque mayoritariamente dirigido a la seguridad e identificación de los habitantes de ese país en la lucha contra el crimen organizado. De manera similar al caso expuesto del intento de creación de la UPAD, Costa Rica, ha recibido cuestionamientos sobre quiénes tienen acceso a esa información, cómo y para qué se usa.

En el sector bancario de Perú, una investigación sobre implementación de sistemas de identificación por biometría en el uso de cajeros automáticos del Banco de la Nación concluyó que, la tecnología de identificación por huella dactilar es la mejor opción, en comparación con métodos tradicionales de uso de estos dispositivos, como mecanismo de seguridad en contra de los tipos de fraude de suplantación, cambiazo y clonación de tarjeta (Rojas, 2021). Se recomendó su implementación en todos los cajeros del banco.

La experiencia del uso de biometría en elecciones en Colombia ha tenido resultados positivos. Según Padrón-Pardo (2019):

> el 30 de octubre de 2011 se aplicó por primera vez la identificación biométrica en elecciones ordinarias y se realizó el mayor despliegue de biometría en la historia electoral del país: tres millones de ciudadanos, es decir alrededor del 10% del censo electoral, fueron identificados con herramientas biométricas. Con la experiencia adquirida, la Registraduría ha logrado reducir el tiempo que tarda el cotejo dactilar, que hace cuatro años tomaba tres minutos y ahora tarda de dos a tres segundos, evitando congestiones en el ingreso de los puestos de votación.

Sus primeras pruebas que comenzaron en el año 2006, no han estado exentas de críticas, entre los que se puede destacar: el temor de que se den mecanismos de fraudes más sofisticados que los tradicionales y que hagan más difícil descubrirlos.

Otro caso de uso en Colombia, desde el año 2012 se reguló en ese país con el uso de la firma electrónica. En combinación con la firma digital, se ha buscado que estos métodos aseguren la integridad y autenticidad de asegurar que el firmante que las usa es su dueño legítimo. Refiriéndose a la inclusión de biometría en la firma digital, como complemento de la firma electrónica, Martínez y Cárdenas (2021) explican que:

> Mientras que la firma digital es un procedimiento matemático que ya identifica a una persona y goza de autenticidad e integridad; la firma electrónica es un mecanismo técnico

> que, si bien identifica a la persona, únicamente permite verificar su autenticidad de integridad. De esta manera, no garantiza como tal estos atributos, sino que se requiere de mecanismos que permitan tal verificación.

La cantidad de información que se almacena para poder generar el desarrollo de la identificación mediante mecanismos biométricos es de suma preocupación y por eso, debe ser debidamente legislada. El Comité Jurídico Interamericano (2021: 199-200) como cuerpo consultivo de la Organización de los Estados Americanos (OEA) en aras de promover la protección de los datos personales sensibles y contemplando los datos biométricos como tales menciona:

> Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos... El término "Datos Personales Sensibles" abarca los Datos que se refieren a los aspectos más íntimos de las personas... Según el contexto cultural, social o político, podría incluir, por ejemplo, los Datos relacionados con su salud personal, vida sexual, orientación sexual, creencias religiosas, filosóficas o morales, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, opinión política u origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal.

Metodología

La presente investigación es de tipo cualitativa. Según Hernández-Sampieri y Mendoza Torres (2018: 256-257, 606): "En particular, las investigaciones cualitativas analizan la calidad o cualidad de las relaciones, actividades, situaciones o materiales de una forma holística y generalmente, a través de un tratamiento no numérico de los datos".

Se busca, por medio de una revisión de datos en documentación existente, comparar el uso de mecanismos de biometría como método de autentificación en las empresas de Costa Rica, con respecto al de otros países de América Latina.

En una investigación cualitativa es esencial tener claro, un eje de "exploración" por la variabilidad de circunstancias que se puedan presentar en el camino, un estudio de Guerrero (2016: 9) define que:

> la Investigación Cualitativa tiene ilimitadas posibilidades para poder analizar los diferentes sucesos que se puedan presentar de acuerdo a cada caso o tipo de estudio. Nos permite investigar aspectos sociales del comportamiento humano que no se pueden valorar de

> forma sencilla e intentar comprenderlos... en el método cualitativo existe una mayor libertad y flexibilidad de adaptación por los resultados que se puedan ir obteniendo.

Hernández-Sampieri y Mendoza Torres (2018: 7) expresan que:

> también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos".

Esta información, por lo tanto, no es de recolección de datos propios, sino que recopila información nacional e internacional de distintos documentos, a fin de conocer la situación de Costa Rica, en cuanto al uso de estos mecanismos. Resulta particularmente útil para esta investigación, el uso del enfoque cualitativo cuando hay pocos antecedentes, en cuanto al abordaje del problema es difícil medirlo (Hernández-Sampieri y Mendoza Torres, 2018).

Además, las necesidades de este estudio se ajustan a este enfoque, pues se busca recoger y documentar las experiencias de las empresas analizadas en los procesos de adopción y utilización de biometría; la información que detalle estos procesos y las características de cada una, las cuales ayuden a comprender su toma de decisiones, en cuanto al uso de estas tecnologías.

El uso del enfoque cualitativo implica que no necesariamente se tiene una hipótesis de la que se intente averiguar si es cierta, sino que se plantea inicialmente, con base en la información del marco teórico y durante el estudio, la misma puede cambiar conforme se obtengan nuevos datos (Hernández-Sampieri y Mendoza Torres, 2018).

Ruiz (2012: 56) también indica que: "No se parte de una teoría, ni se cuenta con hipótesis relacionales previas, pero sí se puede, y se debe, iniciar con pistas o claves de interpretación que guiarán los primeros pasos de la recogida de datos".

La hipótesis que se plantea es que, en las empresas y la sociedad costarricense, el uso de sistemas de autenticación por biometría no tiene un uso más amplio, debido al costo de inversión de implementación, las dudas sobre el uso de esta información sensible asociada íntimamente a cada persona denotan la falta de valor que se da a la seguridad informática en Costa Rica.

Para la recolección de información de esta investigación y la comprensión del problema actual se hace uso de la entrevista. Ruiz (2012) señala que la entrevista es una técnica para obtener información, mediante una conversación profesional con una o varias personas para un estudio analítico de investigación o para contribuir en los diagnósticos o tratamientos sociales.

El alcance de la investigación es de tipo descriptivo, pues se utiliza para comprender situaciones, contextos y fenómenos, además de describir tendencias. En este caso, las razones que explican el uso de la biometría en empresas de Costa Rica y por qué su uso es mayor o menor, en comparación con otros países. De acuerdo con Hernández-Sampieri y Mendoza Torres (2018: 92):

> en este tipo de investigación se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refiere, esto es, su objetivo no es indicar cómo se relacionan estas.

El material de referencia para la consulta de fuentes de este estudio es tomado de datos aportados por otras investigaciones relacionadas con el tema. Se consulta información de bases de datos como EBSCOhost; Google Scholar; sitios web oficiales de universidades; organizaciones y artículos para después, clasificar y analizar esta información. Lo anterior, permite poder tener un estado de la situación; identificar razones y causas, así como también, poder aportar oportunidades de mejora.

Análisis de resultados

De los representantes de empresas entrevistados se encuentran el administrador de gestión y logística de funcionamiento general de servicios brindados y recibidos en una empresa transnacional; un médico especialista en medicina legal; un asistente coordinador de liberación; un docente; un ingeniero en sistemas con jefatura en departamento de Tecnologías de Información (TI); un dentista,; un gerente comercial farmacéutico; un jefe de recursos humanos; un gerente analista de datos; un administrador en educación y director; un jefe de departamento de control y cumplimiento; un consultor de seguridad informática en sitios web; un informático, un informático administrador de ciberseguridad; un informático en infraestructura e ingeniero en sistemas en empresas que se dedican a la tecnología; la resolución de conflictos legales en una institución estatal; la manufactura de dispositivos médicos; la escuela primaria pública; una entidad financiera; un dentista en ejercicio liberal; una empresa de venta y despacho de productos de farmacia; una empresa de alimentos; un contact center; un profesor de colegio técnico profesional; una guardería infantil y un centro de idiomas; una escuela primaria pública; una empresa proveedora de servicios web; una empresa transnacional del sector producción; una empresa no especificada; una empresa de servicios informáticos en infraestructura y consultoría, respectivamente.

De las diecisiete personas a las que se entrevistó, ocho utilizan mecanismos de autenticación biométricos en sus organizaciones para identificar a sus colaboradores como empleados de la institución, aunque no necesariamente se hace con todos los colaboradores y en dos de los casos, no es de uso obligatorio; seis reportaron no utilizarlos, pero sí utilizar algún otro sistema y tres reportaron no utilizar ningún tipo.

Entre el grupo de personas entrevistadas que laboran en empresas que no utilizan sistemas de autenticación de ningún tipo, las razones que se mencionan de por qué no lo hacen es por lo costoso de su implementación para la empresa; la percepción de los altos costos; la sofisticación de implementar biometría y en la tercera respuesta, se destaca que no se usan, al tener un puesto

de trabajo de consultor. Se mencionan, además, como consecuencias de no utilizar estos métodos, el no poder validar si quienes utilizan los dispositivos de acceso son realmente quienes deben tener ese acceso.

El segundo entrevistado resalta que su organización solo cuenta con 3 personas trabajando de forma presencial. Al referirse a potenciales consecuencias negativas de no utilizar mecanismos de autenticación, las reacciones descritas son la sanción de quienes ingresen con contraseñas de otros colaboradores, aunque se admite que esto no evitaría potenciales pérdidas de información. La tercera respuesta explica que, si bien los controles de autenticación son necesarios, estos deben adaptarse a la cultura de seguridad de la empresa.

Ante la pregunta de si consideran que la empresa para la que trabajan podría beneficiarse con la utilización de mecanismos de autenticación por biometría; la primera persona entrevistada contestó que sí, explicando como razones: la robustez que se añadiría a la seguridad del lugar de trabajo. La segunda entrevista valora también como potencialmente beneficioso su uso, pero lo implementaría una vez que haya más empleados en la organización, con el objetivo de controlar quién entra y sale de las instalaciones y llevar un control de tiempos de entrada y salida. La tercera persona entrevistada considera que, además de la empresa, debe tenerse en cuenta, implementar estos controles para los clientes, también a fin de aumentar su propio nivel de seguridad.

Dos de las respuestas en esta categoría de entrevistados, adoptaría la autenticación por huella dactilar como mecanismo de seguridad y una añadiría reconocimiento facial, de retina y prueba de vida.

Al emitir su opinión sobre si el uso de biometría como método de autenticación es alto o bajo en Costa Rica, un entrevistado contestó que es alto, mientras que otro afirmó no saber suficiente para poder dar una opinión; sin embargo, mencionó que en tres empleos anteriores ha usado sistemas de este tipo. Al elaborar esta pregunta, las respuestas dadas mencionan que la mayoría de las empresas del país utilizan métodos convencionales para autenticación. El tercer entrevistado consideró que, en su opinión, el uso de biometría es bajo y además es una moda, dada su reciente adopción y que las medidas de seguridad se deben brindar, según las necesidades de las organizaciones.

Del grupo de personas entrevistados que pertenecen a organizaciones en la categoría que no utilizan mecanismos de autenticación biométricos, pero sí autenticación por algún otro método, en uno de los casos se menciona desconocer porqué en la empresa para la que trabaja no los utiliza y añade que la misma es “gigante” en tamaño y funciona en general con base en estándares; por lo que opina que cambiar a un sistema de biometría sería un proceso largo y desconoce si las necesidades de seguridad de la misma han llegado al punto de necesitarlas o si ha habido incidentes que creen esta necesidad.

La segunda respuesta menciona los altos costos para la implementación de los mecanismos al ser una empresa de tipo unipersonal. En la tercera respuesta, la razón por la que la empresa no los utiliza, se explica como razón del desconocimiento de esta tecnología; la sofisticación de los mecanismos de uso y la percepción de que tiene un alto costo de implementación. El cuarto entrevistado indicó que algunos de los dispositivos de la empresa cuentan con controles por

biometría; sin embargo, estos no son un requerimiento de la organización y son de uso opcional, siendo los métodos que utilizan, segundo factor de autenticación con token, tarjetas de proximidad magnéticas de acceso para el acceso físico a las instalaciones, usuario y contraseña y certificados de inscripción instalados en los dispositivos de los colaboradores. En este caso se indica que la empresa no se ha visto en la necesidad de utilizar controles adicionales, pues los existentes se consideran seguros y se destaca el costo de la inversión en herramientas de seguridad adicionales.

La quinta persona entrevistada respondió que los costos de implementación han sido un impedimento para utilizar autenticación biométrica en su lugar de trabajo y añade que, aun así, se utilizan otros mecanismos de autenticación.

La última persona entrevistada en este grupo explicó que, en el caso de la empresa para la que trabaja, la mayoría de las personas trabajan desde sus casas como razón para no usarlos y no ha habido consecuencias negativas por no utilizarlos como control adicional a los ya utilizados para resguardar los datos y accesos generales.

Las consecuencias que se perciben pueden experimentarse por no utilizar estos sistemas; desconocer si ha habido o si hay potenciales consecuencias, dada la naturaleza de su puesto y el no acceso a reportes sobre este tipo de incidentes y su frecuencia. Sin embargo, sí se destaca el poco tiempo de respuesta por el que se caracteriza la organización para hacer frente a incidentes, por lo que se concluye que, de haber ya una necesidad de utilizar biometría, esto respondería a una necesidad global de la empresa y que se implementaría de forma estandarizada y planeada, en el caso de la empresa transnacional tecnológica.

Otra de las respuestas menciona no haber tenido inconvenientes por la falta de uso de estos sistemas hasta el momento y ser la única persona que conoce las credenciales para la base de datos que se utiliza en el trabajo. Además, se enumera la vulnerabilidad ante robos de usuarios y contraseñas, pues si las consecuencias son negativas, sus organizaciones reaccionarían ante estas contactando al Organismo de Investigación Judicial (OIJ) de Costa Rica y organizaciones gremiales, dado el carácter confidencial de la información.

En el caso de otra de las organizaciones, admitieron no tener un plan de reacción ante una consecuencia negativa, aunque no han registrado incidentes de ese tipo. El cuarto entrevistado menciona como riesgo de los controles de seguridad existentes: compartir claves y tarjetas de ingreso, además del robo de estas.

En la quinta entrevista se menciona como consecuencias de no tenerlos implementados, el hecho de que el no hacerlo hace que los mecanismos de seguridad con los que cuenta la empresa se vean menos fortalecidos a causa de esto. El último entrevistado comentó que, en caso de tener alguna consecuencia negativa por no usar estas medidas de seguridad, eso haría que en su lugar de trabajo se valore la importancia y la inversión adicional en estas herramientas

Uno de los entrevistados indicó que la reacción de la empresa para la que trabaja ante una consecuencia negativa de no usar mecanismos de autenticación biométricos, el plan que esta organización tiene actualmente para recuperación ante ataques informáticos, es la aplicación de planes de contingencia y otros mecanismos de seguridad no especificados. En otro caso, la

respuesta fue que se redirigirían los canales hacia el usuario final por medio de herramientas como la nube, para poder continuar con sus operaciones.

Al cuestionar si la empresa para la que trabajan se podía beneficiar de utilizar biometría como autenticación, todas las respuestas dadas, excepto una, mencionan que sí resaltando que, se brinda una mayor seguridad en los accesos a los sistemas y el mayor grado de fiabilidad de que quien accede a estos, es realmente la persona autorizada.

Además, se añade la mayor velocidad para tener acceso a la información y la reducción de la vulnerabilidad de las credenciales de seguridad. En el caso de la respuesta donde no se considera como un beneficio adicional en su caso particular, el hecho de que el personal no trabaje desde una oficina en las instalaciones de la empresa se considera como un factor para no implementarla.

Como respuesta a la pregunta de qué mecanismo de biometría adoptaría en este grupo de entrevistados, las respuestas obtenidas fueron huella dactilar por su costo menor en todos los casos, excepto en uno, que no contestó. En un caso adicional se mencionan identificación de retinas y reconocimiento facial. Además, se menciona la autenticación multifactor (MFA) con los dos sistemas antes mencionados como opción a utilizar.

El grupo de entrevistados en esta categoría considera en su totalidad que el uso de biometría en Costa Rica es bajo. Entre las razones citadas, están una parte amplia de la población sin acceso al tipo de hardware y software que se necesita para utilizar estas tecnologías. Además, se menciona que, las instituciones nacionales del sector público y académicas están retrasadas en la actualización de sus equipos tecnológicos, utilizando frecuentemente procesos en papel y provocando con esto, que los usuarios no tengan contacto con dichas tecnologías y como consecuencia, las utilicen poco.

También, se agrega desconocimiento del tema; el exceso de confianza en relación con la importancia que se da a la información que se guarda y la cultura de las empresas nacionales que no consideran estas medidas en sus políticas, a diferencia de empresas transnacionales. Adicionalmente, se explica en otra respuesta que, el uso es bajo en el país por el costo de implementación y mantenimiento de estos sistemas.

En el tercer grupo de personas entrevistadas, ocho mencionaron que la empresa en que trabajan sí utiliza sistemas de autenticación de identidad por biometría. Una mencionó que el sistema utilizado es Huella digital, como método de autenticación adicional al carné y placa, para el control de asistencias de entradas y salidas, controles de acceso y controles de cámaras de vigilancia.

El segundo caso menciona que, el sistema utilizado en su caso es también huella dactilar. Ante la pregunta de por qué se utiliza ese método, se registró que se utiliza para las funciones de firma y registro de documentación en tiempo real y el control de las operaciones diarias en general. Para el tercer resultado, también se utiliza la huella dactilar, además de reconocimiento facial en algunos casos, para el proceso de registro de entrada y salida de la institución por parte de los funcionarios. Se destaca su uso como una forma ágil para registrar a los funcionarios y sus accesos.

La cuarta entrevista menciona que son los empleados de posiciones operativas y de planta de producción, los que utilizan relojes biométricos como controles por biometría, mientras que los

de posiciones administrativas utilizan solamente tarjetas de acceso, mencionando que estos controles no son eficientes para esos puestos de trabajo. En este caso se utilizan dichos controles para el caso de jornadas y horarios de planta, como evidencia para pagos de nóminas y evidencia en casos de procesos disciplinarios.

En el caso del quinto entrevistado, este enumera como sistemas de autenticación, el uso de carné de identificación, cifrado de computadores y sistema de doble verificación no especificado como información confidencial de la organización para la que trabaja. Estos se utilizan para validar el ingreso y uso de herramientas; no añadiría mecanismos adicionales biométricos y considera que el uso de biometría en Costa Rica es bajo, citando que no lo observa en muchas empresas.

La sexta entrevista menciona el uso de huella dactilar como control utilizado, aunque no es de uso obligatorio; la razón citada de su adopción es que este método es el aprobado por el Ministerio de Educación Pública y se utiliza para registrar entradas y salidas de empleados.

Las respuestas de la sétima persona entrevistada indican que el método biométrico utilizado es huella dactilar, además de claves y tarjetas de acceso; esto ha sido definido por directivas de la empresa y se utiliza para acceder en áreas restringidas. Agregó que añadiría sistemas de autenticación por biometría adicionales, sin especificar cuál o cuáles. El octavo caso explicó utilizar escáner RFID, adicional al uso de lectores de tarjetas para el control de ingreso y activos.

Al indagar sobre si el entrevistado añadiría sistemas de biometría adicionales, uno respondió que sí, mencionando que escogería el lector de retina, explicando que sería conveniente para ingresar a zonas de trabajo estériles en las que actualmente necesita quitarse guantes de trabajo para hacer uso del control de autenticación, mientras que con el uso de lectura de retina esto no sería necesario y se mantendría el nivel de seguridad del mecanismo. Otra respuesta resalta que utilizaría un sistema adicional para el manejo de la documentación en los sistemas y las verificaciones de estos.

La tercera respuesta resalta el uso de algunos usuarios de reconocimiento facial para registrar entradas y salidas laborales, pues la huella dactilar no reconoce a las personas en algunos casos. La cuarta respuesta menciona el lector de retina. La quinta respuesta no menciona ningún método adicional al que se utiliza, citando que ya se utiliza uno y no se ve la necesidad de adoptar uno adicional, al igual que la sexta respuesta. La octava persona entrevistada no añadiría métodos adicionales.

Como respuesta a la pregunta de si considera que el uso de biometría como método de autenticación es alto o bajo en Costa Rica, cuatro entrevistados contestaron que es alto, mientras que dos contestaron que es bajo. Entre las respuestas, se menciona que, en su organización, el sistema de autenticación biométrico que se usa funciona desde hace varios años, junto con controles de acceso adicionales; uno de los entrevistados menciona que su uso es alto para empresas con gran cantidad de colaboradores operativos. Se menciona, además que la cantidad de empleados en una empresa es un factor importante para adoptar este mecanismo. Por último, quienes mencionan que su uso es bajo, destacan que debería emplearse más para dar mayor facilidad y confiabilidad a los empleados en sus labores de trabajo.

Discusión de los resultados

En los últimos años, Costa Rica ha hecho esfuerzos como país por coordinar distintos sectores en el desarrollo de la ciberseguridad del país. En el año 2017, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) de Costa Rica publicó el documento "Estrategia Nacional de Ciberseguridad de Costa Rica", que pone a las personas como prioridad del plan (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017) y pretende, además invertir recursos en esta área y concienciar a la sociedad del país acerca de la responsabilidad que cada parte adquiere en la preparación que se debe tener ante los riesgos en el uso de las Tecnologías de Información y Comunicación (TIC's).

Con base en esa iniciativa estatal y al hacer una comparación con la situación de empresas y organizaciones públicas y privadas, en cuanto al nivel de uso de biometría, las entrevistas hechas muestran una situación mixta en la que se observó que ocho de dieciséis profesionales mencionan que sus lugares de trabajo utilizan autenticación biométrica, mientras que ocho utilizan algún otro control sin este mecanismo o no utilizan ninguno.

También, entre las empresas que usan estos controles, no los utilizan para todo el personal y su uso se concentra en algunas áreas o departamentos de trabajo. Al extrapolar estos resultados con los esfuerzos del país por incrementar su seguridad, se observa una concordancia entre el desarrollo de iniciativas para coordinar el establecimiento de controles de ciberseguridad a nivel país por parte del Estado Costarricense en el año 2018 y la adopción de estas iniciativas y controles en los lugares de trabajo y las herramientas que se utilizan.

Como contraparte, en el año 2022 ocurrieron múltiples incidentes de ataques informáticos masivos a múltiples instituciones estatales, entre las que se encuentran el MICITT; la Caja Costarricense del Seguro Social (CCSS); el Ministerio de Educación Pública (MEP); el Tribunal Supremo de Elecciones (TSE) y el Ministerio de Hacienda, entre otras (Blanco, 2022).

En el caso de esta última institución, un informe hecho por la Contraloría General de la República en el año 2019 evidenció en ese entonces, los deficientes controles, el rezago y la falta de preparación para estos ataques (Contraloría General de la República, 2019), a pesar de la estrategia presentada por el Micitt en el año 2017.

Estos hechos apoyan la tesis de que, si bien se ha abordado el problema de la ciberseguridad, la implementación no ha sido aplicada del todo o ha sido deficiente. En el caso de las empresas estudiadas, si bien una buena parte de los entrevistados reportó utilizar controles de autenticación biométricos en sus lugares de trabajo como medida de seguridad, en muchos casos estos se limitaron a controlar accesos de personal a instalaciones, pero no el acceso a sistemas informáticos o redes internas empresariales, por lo que existe el riesgo de que haya empresas que, si bien cuentan con estos controles, no estén protegidas de accesos lógicos no autorizados a sus datos e información.

Es de recalcar que, las personas entrevistadas que laboran en grandes empresas mencionaron la falta de recursos como razón de que no se utilizan sistemas biométricos en la mayoría de las empresas del país, mientras que los entrevistados que trabajan para empresas no

transnacionales y de menor tamaño mencionaron que son las empresas grandes o transnacionales, las que cuentan con los recursos y la cultura de trabajo para implementar o utilizar estos sistemas. Sin embargo, se dio el caso de instituciones como la escuela pública, que sí cuentan con estos mecanismos y que, en muchas ocasiones, cuentan con pocos recursos económicos disponibles, a pesar de ser mantenidas con fondos estatales.

Cabe destacar, además que se percibe falta de conocimiento técnico y de lenguaje tecnológico de los usuarios en el área de los controles de acceso por biometría. Hubo que aclarar a varios de los entrevistados, el concepto de autenticación biométrica, para que comprendieran sobre qué iban a tratar las preguntas de la entrevista. A pesar de que, el uso de estas tecnologías se ha hecho más masiva y de uso común hasta años recientes, persiste un desconocimiento de estas herramientas en una cantidad grande de usuarios.

Al analizar la opinión y el conocimiento de los entrevistados sobre los distintos métodos de autenticación por biometría que se utilizan, la respuesta más frecuentemente registrada sobre cuál de estos considerarían utilizar en caso de no tener ninguno o como adicional a los ya utilizados, el mecanismo de reconocimiento por huella dactilar fue percibido como de menor inversión económica para su implementación en los lugares en que trabajan y como el más frecuentemente mencionado. Esta afirmación coincide con lo investigado sobre los tipos de biometría (Guízar *et al.*, 2021).

El método de lectura de retina fue percibido como eficiente y ágil, además de ser el preferido en adición a los que ya se contaban en las organizaciones de los entrevistados. Entre las razones que se mencionaron para su uso está la comodidad en su uso en tareas laborales en las que es importante no utilizar las manos o evitar usarlas; se menciona también, el alto nivel de seguridad que brinda este mecanismo.

Conclusiones y recomendaciones

Las entrevistadas elaboradas mostraron opiniones y percepciones que se tienen sobre el uso de sistemas de autenticación por biometría en Costa Rica, en diferentes organizaciones, así como también realidades.

Se encontró la percepción de que, el uso de estos sistemas en el país se da principalmente entre empresas grandes, en cuanto a presupuesto, utilidades o las de tipo transnacional; además, que este tipo de empresas utilizan estas herramientas en sus procesos, adoptando las mejores prácticas de la industria.

Sin embargo, se evidenció que los entrevistados que laboran en empresas de este tipo contestaron que no las tienen implementadas en sus lugares de trabajo. Por otra parte, se concluye que, en el caso de entidades estatales y escuelas públicas que, frecuentemente enfrentan problemas de falta de presupuesto y baja inversión en recursos, sí cuentan en ocasiones con estos mecanismos, al igual que otras empresas de menor tamaño, por lo que pueden adoptarse y adaptarse, según el presupuesto y necesidades de cada caso particular.

A pesar de que los ciberataques sufridos por el país en el año 2022 causaron mucha afectación en múltiples áreas de la vida del país y sus servicios públicos y evidenciaron las deficiencias presentes en la Estrategia Nacional de Ciberseguridad (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017), esta experiencia debe aprovecharse como tema de estudio y referente para las personas profesionales en ciberseguridad, autoridades gubernamentales y empresas, a fin de que puedan identificar qué vulnerabilidades podrían ser explotadas en sus sistemas y dispositivos tecnológicos y cómo pueden disminuir estas debilidades. Además, se demuestra que, en la práctica, la inversión en seguridad de forma preventiva es menos costosa que tratar de remediar y recuperarse de ciberataques.

Las entrevistas muestran mecanismos de seguridad para la autenticación utilizados en el país de naturaleza mixta: desde sistemas de ingreso por usuario y contraseña; tarjetas de proximidad; carné de identificación y placas y huella dactilar e identificación por radiofrecuencia (RFID). Se identificó que, entre las organizaciones que utilizan controles de tipo biométrico, estos se usan como control adicional a los sistemas de seguridad existentes.

Para los casos de empresas que no utilizan biometría, se recomienda que se adopte este tipo de herramientas, como control adicional a los mecanismos existentes que utilicen, junto con la creación de políticas de uso de estas herramientas, a fin de que se usen de manera apropiada. Se recomienda también que, junto con estas políticas y reglas de uso, se establezcan estrategias de recuperación ante vulnerabilidades y potenciales violaciones de estas medidas de seguridad.

De las respuestas recopiladas predominó como mecanismo de autenticación biométrico más mencionado y preferido el de huella dactilar y se destacó su facilidad de uso y costo. Aunado a este, en el caso de algunos de los lugares de trabajo en que ya se utilizó, se consideró que el lector de retina puede ser una opción más adecuada, para que su uso sea más eficiente en trabajos en los que se dificulte, utilizar las manos para manipular un lector de huella.

De acuerdo con la bibliografía consultada, en la que se destaca el mecanismo de huella dactilar como uno de los más seguros y menos costosos, aunado al conocimiento que varios de los entrevistados mostraron hacia este mecanismo, se recomienda que se considere su uso. Como herramienta para la toma de decisiones en la adopción de este mecanismo o cualquier otro que se considere apropiado, se debe hacer antes un análisis de costo-beneficio, en el que se estudien las necesidades y recursos con los que cuenta la organización.

Se encontró que existen iniciativas estatales para la protección de la seguridad informática, incluyendo la información biométrica, entre las que destacan intentos de legislación para regular la recolección de datos biométricos de las personas, como en el caso de la UPAD, similar al caso estudiado del SIBIOS, en Argentina.

Para ambos casos, se encontró también, que hubo múltiples cuestionamientos sobre el manejo que se pretende dar a esta información, dado que constituye datos ligados de manera muy intrínseca a cada persona. En el caso de Costa Rica, la iniciativa de la creación de la UPAD no prosperó.

A nivel país, Costa Rica debe continuar con los esfuerzos por fortalecer y desarrollar su estrategia nacional de ciberseguridad, que incluya legislación, además de controles lógicos y

físicos relacionados, tomando como base, las recomendaciones hechas por organismos, como la OEA (Comité Jurídico Interamericano, 2021).

Además, los recientes ataques informáticos hechos a varias instituciones estatales de Costa Rica deben concientizar a la población sobre las consecuencias de la negligencia de estos controles, en especial por el impacto en múltiples servicios brindados por estas instituciones a la población del país por los incidentes ocurridos en el año 2022 (Blanco, 2022).

La información recopilada en las entrevistas hechas mostró que, al decidir cuál o cuáles herramientas de control biométrico se adoptarían en un lugar de trabajo, se consideran relevantes aspectos tanto técnicos, en cuanto al nivel de seguridad del sistema, como también su facilidad de uso y familiarización entre los usuarios, según las labores para la que se requiera.

También, se identificó que, si bien las características anteriormente mencionadas son importantes, la inversión que se deba hacer en adoptar y mantener estos sistemas es de mucha relevancia para las organizaciones, especialmente si cuentan con recursos limitados.

Con base en los métodos de autenticación biométricos investigados, se recomienda especialmente en las organizaciones que no utilizan ninguno, adoptar el uso del mecanismo de huella dactilar.

Entre las razones de esta recomendación, se destacan importantes características técnicas que se encontraron en esta investigación, entre las cuales están: su nivel de seguridad basado en patrones dactilares difíciles de replicar, que generan múltiples variables que son inherentes a cada individuo. A nivel de costo, también se encontró que es el más barato (Guízar *et al.*, 2021), por lo que es una alternativa de mayor comodidad económica para organizaciones que destacan el factor económico como relevante al hacer esta inversión.

Se recomienda también, el uso del método de autenticación por lectura de retina, en tareas y ambientes que, por su naturaleza, dificulten el uso de la huella dactilar como, por ejemplo, zonas de trabajo estériles, que requieran el uso de guantes o impidan en algún grado, el uso de las manos.

Debe, además considerarse que, en el ámbito de la seguridad, el factor humano es de gran importancia, pues aun cuando se cuente con un alto nivel de medidas de control, estas se verán comprometidas y potencialmente vulneradas, si sus usuarios por descuido, desconocimiento, negligencia o de manera intencional, les dan un uso incorrecto.

En este sentido, si la herramienta de biometría como mecanismo de seguridad es percibida como negativa por sus usuarios, en cuanto a dificultad de uso, el que provoque alta disrupción en sus labores o genere mayor esfuerzo para validar accesos; si su costo de implementación y mantenimiento es alto o inclusive, si se percibe como desconocida, se corre el riesgo de que los usuarios eviten su uso; busquen formas de evadirlo o romper sus controles y si es posible, omitirlos o suprimirlos.

Por último, si el mecanismo biométrico es simple y fácil de usar, amigable con el usuario y si hay un grado de conocimiento de la herramienta, es más probable que su adopción sea más rápida y aumente su eficacia.

Referencias

Asamblea Legislativa de la República de Costa Rica. (2020). *Comisión especial investigadora sobre las posibles violaciones por parte del gobierno de la república al derecho a la intimidad de las personas, respecto a la obtención y manejo de sus datos personales (Unidad Presidencial de Análisis de Datos) expediente N°21.818*. http://www.asamblea.go.cr/glcp/virtuales_documentos/CE%2021818%20UPAD/Informe%20UPAD.pdf

BAC Credomatic. (2022). *INFORME INTEGRADO 2021*. https://www.baccredomatic.com/sites/default/files/2022-05/Informe_Integrado_BAC_2021_0.pdf

Barrios Tao, H., Díaz Pérez, V. & Guerra, Y. (2020). Subjetividades e inteligencia artificial: desafíos para "lo humano". *Veritas: Journal of Philosophy & Theology*, *47*: 81–107.

BCR ofrece Biometría Facial como mecanismo de seguridad en su App. (2021). https://www.mibcr.com/wps/portal/blog/blog/

Blanco, J. (2022). *Ministerio de Hacienda tiene debilidades cibernéticas desde el 2019*. Semanario Universidad. https://semanariouniversidad.com/pais/ministerio-de-hacienda-tiene-debilidades-ciberneticas-desde-el-2019/

Comité Jurídico Interamericano. (2021). *Informe del Comité Jurídico Interamericano. Principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales.* Organización de los Estados Americanos.

Contraloría General de la República. (2019). *Informe de auditoría de carácter especial sobre la seguridad de la información de los centros de datos del Ministerio de Hacienda*. https://cgrfiles.cgr.go.cr/publico/docs_cgr/2019/SIGYD_D_2019020631.pdf

Costa Rica con pasaporte biométrico en el 2022. (2021). https://www.presidencia.go.cr/comunicados/2021/09/costa-rica-contara-con-pasaporte-biometrico-en-el-2022/

Cruz, G. J. (2020). *Diseño e implementación de un Sistema Piloto de Control de Acceso basado en Patrón Vascular*. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4377/Giancarlo_Cruz_Iturrizaga_Trabajo_de_Suficiencia_Profesional_Titulo_Profesional_2020.pdf?sequence=5&isAllowed=y

Domingo, C. (2021). *Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana, El Criminalista Digital, 9*: 20-37. https://revistaseug.ugr.es/index.php/cridi/article/view/20899/20280

Finnovista. (2019). *FINTECH en Costa Rica: Hacia una evolución de los servicios financieros*, Banco Interamericano de Desarrollo.

Gacovski, Z. (2020). *Biometrics Authentication Methods*. Arcler Press.

George, C. y Grinnell. (2020). *The Social Life of Biometrics*. Rutgers University Press.

Guerrero, M. A. (2016). *La Investigación Cualitativa. INNOVA Research Journal, 1(2)*: 1-9. https://doi.org/10.33890/innova.v1.n2.2016.7

Guízar-Sahagún, G., Grijalva-Otero, I. & Madrazo-Navarro, I. (2021). Huellas dactilares: origen, usos y desafíos que genera la incapacidad para su registro. *Revista Médica Del IMSS, 59*(6): 568–573.

Guo, Y. (2021). Impact on Biometric Identification Systems of COVID-19. *Scientific Programming*: 1–7. https://doi.org/10.1155/2021/3225687

Hernández-Sampieri, R. y Mendoza Torres, C. (2018). *Metodología de la Investigación: las rutas cuantitativa, cualitativa y mixta*. Mc Graw Hill.

Ingrese a BN Móvil con huella dactilar o registro facial. (2021). https://bnmascerca.com/

Joseph, A. A., Ng Ho Lian, A., Kipli, K., Kho Lee Chin, Mat, D. A. A., Sia Chin Voon, C., Chua Sing Ngie, D. & Ngu Sze Song. (2022). Person Verification Based on Multimodal Biometric Recognition. *Pertanika Journal of Science & Technology*, *30*(1): 161–183. https://doi.org/10.47836/pjst.30.1.09

Martínez Molano, V. & Rincón Cárdenas, E. (2021). Problemas y desarrollo de la identidad en el mundo digital. *Revista chilena de derecho y tecnología*, *10*(2): 251-276. https://dx.doi.org/10.5354/0719-2584.2021.59188

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica.* https://www.micitt.go.cr/wp-content/uploads/2022/05/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-Oficial.pdf

Peláez Guevara, J. & Gutiérrez Núñez, C. (2021). El Iris Humano Como Método de Identificación Forense. *Advocatus*, *18*(36): 161–181.

Padrón-Pardo, Floralba. (2019). E-voting en Colombia: avances y desafíos en la implementación. *Revista Derecho del Estado*, (42): 211-248. https://doi.org/10.18601/01229893.n42.08

Rios, A. (2020). Seguridad y biometría en cuestión: el sistema federal de identificación biométrica (SIBIOS) en Argentina. *Aposta*: 57–72.

Rojas, J. (2021). *Diseño de un sistema de acceso biométrico mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación para mejorar la seguridad de la entidad financiera*. (Trabajo de suficiencia profesional de pregrado). Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Ruiz Olabuénaga, J. I. (2012). *Metodología de la investigación cualitativa: Vol. 5a edición*. Universidad de Deusto.

Sánchez, J. J. (2020). *Biometría y la seguridad informática en los métodos de autenticación*. (Monografía). Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/39060.

Soto Mendiola, R. M., López Sánchez, M. & Lorenzo Pineda Jaimes, R. P. E. J. (2019). Análisis de Sistemas de Cómputo basados en la Iridología para la detección de enfermedades en el iris del ojo humano. *Congreso Internacional de Investigacion Academia Journals*, *11*(9): 3445–3449.

Suarez, D. & Guarda, T. (2019). *Sistemas Biométricos aplicados en smartphones*. https://www.researchgate.net/profile/Teresa-Guarda/publication/331178385_Biometric_systems_applied_in_smartphones/links/5fabe79aa6fdcc331b947880/Biometric-systems-applied-in-smartphones.pdf

Team, V. R. (2021). *Verizon 2021 data breach investigations report.*

Vega Luna, J. I., Laguna Acosta, M. A., Salgado Guzmán, G. & Cosme Aceves, J. F. (2021). *Autenticación por patrón de movimientos de mano para acceso a un laboratorio*. *Revista Ciencia, Ingeniería y Desarrollo Tec Lerdo.* http://revistacid.itslerdo.edu.mx/coninci2021/CID012.pdf

Anexo A. Cuestionario de entrevistas

Parte I.

Se le informa al participante la finalidad de la investigación, su carácter confidencial y que la participación es voluntaria. Se le solicita el consentimiento para utilizar su opinión para este estudio. El participante puede negarse a contestar o terminar la entrevista en el momento que lo desee. La entrevista no durará más de 20 minutos.

Parte II.

Guía de preguntas para entrevista

1. Por favor indique su profesión, puesto y el tipo de actividad a la que se dedica la empresa para la que trabaja.
2. ¿Utiliza la empresa para la que trabaja algún mecanismo de autenticación biométrico para corroborar que usted y otras personas son empleados de la misma?

No utiliza ningún mecanismo de autenticación

1. ¿Por qué la empresa para la que trabaja no utiliza mecanismos de autenticación?
2. ¿Qué consecuencias se le presenta a la empresa al no utilizar mecanismos de autenticación?
3. Si las consecuencias son negativas ¿Cómo reaccionaría la empresa ante estas?
4. ¿Considera que la empresa para la que trabaja podría beneficiarse con la utilización de mecanismos de autenticación por biometría? ¿Por qué?
5. Si considera que la empresa para la que trabaja podría beneficiarse de utilizar mecanismos de autenticación por biometría ¿Cuáles propondría? ¿Por qué?
6. ¿Considera que el uso de biometría como método de autenticación en Costa Rica es alto o bajo? ¿Por qué?

No Utiliza mecanismos de autenticación biométricos

1. ¿Por qué la empresa para la que trabaja no utiliza mecanismos de autenticación biométricos?
2. ¿Qué consecuencias se le presenta a la empresa al no utilizar mecanismos de autenticación biométricos?
3. Si las consecuencias son negativas ¿Cómo reaccionaría la empresa ante estas?
4. ¿Considera que la empresa para la que trabaja podría beneficiarse con la utilización de mecanismos de autenticación por biometría? ¿Por qué?
5. Si considera que la empresa para la que trabaja podría beneficiarse de utilizar mecanismos de autenticación por biometría ¿Cuáles propondría? ¿Por qué?

6. ¿Considera que el uso de biometría como método de autenticación en Costa Rica es alto o bajo? ¿Por qué?

Utiliza mecanismos de autenticación biométricos

1. ¿Qué sistema(s) de autenticación de identidad biométricos utiliza la empresa para la que trabaja?
2. ¿Por qué se utiliza este método o métodos?
3. ¿Para qué funciones utilizan este(os) método(s)?
4. ¿Añadiría sistemas de autenticación biométricos adicionales a los que ya se utilizan en la empresa para la que trabaja? ¿Cuáles? ¿Por qué?
5. ¿Considera que el uso de biometría como método de autenticación en Costa Rica es alto o bajo? ¿Por qué?