SAN IGNACIO DE LOYOLA – ESCUELA ISIL

TÍTULO DE LA INVESTIGACIÓN

“Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea”

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE

Bachiller en Dirección de Tecnologías de la Información

PRESENTADO POR:

Soldevilla Magallanes, Sebastian Paolo - Dirección de Tecnologías de la Información

Uribe Santa Cruz, Vanessa Carla - Dirección de Tecnologías de la Información

ASESOR

Albarracín Aparicio, Roxana Alexandra

LIMA, PERÚ

2025

ASESOR Y MIEMBROS DEL JURADO

ASESOR:

Albarracín Aparicio, Roxana Alexandra

MIEMBROS DEL JURADO

Chumpitaz Miranda, Janet

Saco Vertiz Osterloh, Sandra Elizabeth

Quijano Aranibar, Ivan Ernesto

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Vanessa Carla Uribe Santa Cruz Identificado (a) con DNI N° 43573767 perteneciente al Programa de Dirección de Tecnologías de la Información, siendo mi asesor la Sra Roxana Alexandra Albarracin Aparicio identificada con DNI N°: 41981490, y cuyo código ORCID es 0000-0002-6930-3718.

Yo, Sebastian Paolo Soldevilla Magallanes Identificado (a) con DNI N° 72692956 perteneciente al Programa Bachiller en tecnologías de la información, siendo mi asesora la Dra. Roxana Alexandra Albarracín Aparicio, identificado (a) con DNI N°: 41981490, y cuyo código ORCID es 0000-0002-6930-3718.

DECLARAMOS BAJO JURAMENTO QUE:

a) Somos los autores del documento académico titulado “Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea**”.**

b) El trabajo de investigación es original y no ha sido difundido en ningún medio académico; por lo tanto, sus resultados son veraces y no es copia de ningún otro.

c) El asesor ha revisado minuciosamente el proyecto de investigación, incluyendo las citas a otros autores y las referencias bibliográficas. Este proceso se ha llevado a cabo cumpliendo con las pautas académicas y respetando las normas internacionales.

d) El trabajo de investigación cumplió con el análisis del sistema TURNITIN, el cual tiene el 21% de similitud.

e) Declaro conocer las consecuencias legales y/o administrativas que puedan derivar si se verifica la falsedad total o parcial de la presente declaración, de acuerdo con lo previsto en el artículo 411 del código penal, el numeral 34.3 del artículo 34 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo 004-2019-JUS y los artículos 14º y 15º de la RVM 049-2022-MINEDU.

Fecha: 13, Enero, 2026

Firmas de los autores

Nombres	Apellidos	Dni	Firma	Huella
Vanessa Carla	Uribe Santa Cruz	43573767		
Sebastian Paolo	Soldevilla Magallanes	72692956		

Firma del asesor

Nombres	Apellidos	Dni	Firma	Huella
Roxana Alexandra	Albarracín Aparicio	41981490		

DEDICATORIA

Queremos dedicarle nuestro trabajo a nuestra familia y amigos por el apoyo brindado.

AGRADECIMIENTOS

Queremos expresar nuestro agradecimiento a nuestra familia por el apoyo incondicional y nuestra asesora Roxana por su paciencia y apoyo.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente trabajo está enfocado en plantear una propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea, la finalidad es mejorar la gestión de datos de los usuarios y asi lograr su satisfacción como clientes.

Se planteo como objetivo proponer la implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea. En cuanto a la metodología se optó por el tipo de investigación fue aplicado, con un diseño descriptivo, con un enfoque cuantitativo y un nivel correlacional. una metodología cuantitativa debido a que se realiza con encuestas en donde se verificó la relación entre las variables de estudios, sus dimensiones, las percepciones de los usuarios a través de un análisis entre preguntas claves.

Para la presente investigación se decidió usar como recolección de datos la técnica de encuesta y como herramienta un cuestionario estructurado ya que es el indicado para un enfoque cuantitativo seleccionado.

La muestra fue compuesta por 51 Clientes en el rango de 3- 5 pm cuya edad se encuentra entre 18-45 años, que poseen un teléfono inteligente y que utilizan este tipo de plataformas.

En los resultados obtenidos muestran que la propuesta es viable por el deseo de una mejor seguridad de los usuarios para sus datos personales y su conocimiento previo de la tecnología de verificación facial.

Palabras claves: tecnología de verificación, reconocimiento facial, mejora continua, biométrica, machine learning.

ABSTRACT

The present work is focused on outlining a proposal for the implementation of identity verification technology to improve user data management in online gambling, with the aim of enhancing user data management and thus achieving customer satisfaction.

The objective was set to propose the implementation of identity verification technology to improve user data management in online gambling.

Regarding the methodology, the research type chosen was applied, with a descriptive design, a quantitative approach, and a correlational level. A quantitative methodology was adopted because it involved conducting surveys to verify the relationship between the study variables, their dimensions, and user perceptions through an analysis of key questions

For this research, the survey technique was selected for data collection, and a structured questionnaire was used as the tool, as it is appropriate for the selected quantitative approach.

The sample consisted of 51 customers in the 3-5 pm range, aged between 18-45 years, who own a smartphone and use these types of platforms. The results obtained show that the proposal is viable due to the users' desire for better security for their personal data and their prior knowledge of facial verification technology.

Keywords: verification technology, facial recognition, continuous improvement, biometrics, machine learning.

INTRODUCCIÓN

En el contexto actual de digitación los juegos de azar no son la excepción, por ello las plataformas de apuestas digitales enfrentan diferentes dificultades a la hora de gestionar los datos de sus usuarios. Las plataformas de apuesta digitales enfrentan dificultades como el ingreso de menores de edad o de personas que mienten a la hora de crearse un usuario e ingresar a sus plataformas pudiendo cometer fraude de identidad. Los sistemas de verificación son lentos y fáciles de burlar lo cual puede afectar en la satisfacción de los usuarios.

En ayuda a estos problemas, la presenta investigación plantea como la implementación de la tecnología de verificación de identidad lograría ayudar a la gestión de datos de los usuarios. La investigación está estructurada en 6 capítulos, distribuidos de la siguiente manera:

En el capítulo 1 se detalla el proyecto escogido, el área de desarrollo, actividad económica en la que se desarrollara la investigación y el alcance de la solución. En el capítulo 2 se describe el contexto general y especifico, proporcionando datos estadísticos de la problemática en otros países y en el Perú. Tambien se presentan los objetivos, justificación, limitaciones y viabilidad de la investigación. El capítulo 3 presenta el marco referencial, con antecedentes nacionales e internacionales sobre el tema de la investigación, y el desarrollo del marco teórico para definir los conceptos clave.

En el capítulo 4, se plantea la hipótesis general y las derivadas de la investigación estableciendo asi las definiciones conceptuales y operacionales de las variables planteadas. En el capítulo 5 se plantea la parte estadística con el diseño metodológico, incluyendo tambien el diseño muestral, las técnicas de recolección y procesamiento de datos, y el análisis de los resultados. Finalmente, en el capítulo 6 se desarrolla la propuesta de innovación como una

posible solución al problema planteado detallando el alcance esperado, el diagnóstico situacional, el desarrollo del proyecto y el presupuesto necesario.

Esta investigación busca proporcionar una solución estable y con mejora continua a la problemática hallada si no tambien a la satisfacción de los usuarios de estas plataformas.

CAPÍTULO I: INFORMACIÓN GENERAL

1.1. Título del Proyecto

Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea.

1.2. Área estratégica de desarrollo prioritario

Para la presente investigación se eligió la línea de investigación de aplicaciones tecnológicas y transformación digital. En época del avance tecnológico, el acceso a la información debería ser una herramienta para la evolución. Los juegos de azar en línea se han extendido como una epidemia digital sin control, ofreciendo un mundo de supuesta diversión a unos cuantos clics.

Se observa una clara diferencia, para un adulto puede ser un pasatiempo moderado, para un menor joven es un hoyo profundo. Las plataformas venden entretenimiento, pero agrupa vulnerabilidad. La libertad del internet choca de frente con la necesidad de protección, creando un campo de batalla donde la inocencia se enfrenta a algoritmos diseñados para la adicción. Proteger a los menores no es solo una obligación legal, sino el muro que separa un desarrollo saludable de la ruina psicológica y financiera.

Resulta irónico que, mientras las plataformas se revisten de un manto de responsabilidad social, su alcance ilimitado funciona como un caramelo en la puerta de un colegio para quienes carecen de madurez. Por ello, la solución debe nacer de la misma fuente del problema: la tecnología. Se debe forjar un escudo digital mediante sistemas de verificación y monitoreo, oponiendo el control al caos, la regulación a la negligencia. Implementar estas estrategias es la antítesis de la apatía; es la diferencia entre un sector legítimo y sostenible y un campo

minado para las futuras generaciones, asegurando que el progreso tecnológico sirva para construir y no para destruir.

1.3. Actividad económica en la que se aplicaría la investigación

La investigación se introduce en el entorno social, donde se libra una batalla silenciosa la del bienestar contra la quiebra individual. El objetivo es impedir que las finanzas personales y familiares sigan debilitándose a causa de una adicción que se camufla de entretenimiento.

El foco principal es erigir un escudo para la juventud. Resulta una ironía desoladora que en la era de la conexión digital, estemos perdiendo a nuestros jóvenes en el aislamiento del vicio. Las cifras no mienten y golpean con fuerza: Llanos Fajardo (2024) reporta para Perú 21 que más de 4200 menores en Perú ya han sido diagnosticados con ludopatía. Este dato alarmante demuestra que la proliferación de casinos en línea opera como una telaraña brillante y pegajosa, diseñada para atraer a los más vulnerables.

Por ello, este estudio se enfrenta a la adicción y el derecho confronta al caos. Con la ayuda de la ciberseguridad junto con el análisis del comportamiento y los estudios de las leyes disponibles, esta investigación se plantea como la clave para utilizar la tecnología como de manera más útil. La meta es clara: usar el ingenio que creó el laberinto para trazar un mapa de salida, demostrando que el progreso puede ser la cura para el mismo veneno que ayudó a esparcir.

1.4. Alcance de la solución

Este proyecto plantea una solución a uno de los grandes dilemas de nuestra era digital: cómo equilibrar la libertad ilimitada que nos ofrece internet con la protección que necesitamos. La

solución no es un simple cerrojo tecnológico; es una estrategia integral que abarca todos los puntos necesarios, solucionando el problema desde múltiples frentes que incluyen el cumplimiento de las leyes, la educación y la protección de las finanzas.

Para proteger a los más jóvenes, se necesita emplear la misma tecnología que comenzó toda esta problemática. La propuesta busca, imponer un control estricto en un entorno que suele ser controlable, utilizando la verificación de identidad como nuestro aliado principal.

A una escala global, la iniciativa busca transformar el panorama, llevando al sector a estas plataformas hacia la responsabilidad. El fin es convertir un ecosistema potencialmente vulnerable hacia una fortaleza inquebrantable, tanto para los usuarios como para la sostenibilidad de las propias empresas. De esta forma, se garantiza que la tecnología, un trabajo en conjunto para cerrar definitivamente el paso a los menores de edad.

CAPÍTULO II: DESCRIPCIÓN DE LA INVESTIGACIÓN APLICADA

2.1. Descripción de la realidad problemática

Lamentablemente el acceso de los menores de edad a los juegos de azar en línea actualmente es más simple que nunca. Las leyes, que deberían ser firmes en esta problemática no plantean soluciones suficientes. Si bien los reguladores creen que construyen diques, la realidad muestra que el agua se filtra por cada grieta. Los menores se exponen a riesgos graves, donde la adicción se comporta como una sombra que crece y las pérdidas financieras son solo el eco de una ilusión.

Según un informe estadístico de Help (2025) se evidencia que China tiene el mayor número de ludópatas del mundo. Cerca de 60 millones de chinos son ludópatas, lo que representa el 4% de la población china.

Las normativas, que en teoría debían proteger, se dispersan como hojas al viento, permitiendo que las plataformas operen en un vacío legal que es la antítesis del control. Es la paradoja perfecta: un sector que genera miles de millones de dólares, se niega a invertir en tecnología robusta para proteger a sus usuarios más vulnerables, porque la fricción en la experiencia de usuario es más temida que el daño real.

Mientras que algunos países se jactan de sus ingresos, otros, como Letonia, muestran una realidad amarga en la que el 6% de su población sufre problemas con el juego. Es la antítesis del progreso que una sociedad avance económicamente a costa de la salud mental de sus ciudadanos. La falta de homogeneidad en las soluciones tecnológicas de verificación es la prueba irónica de que la industria privilegia la ganancia sobre la protección. Por otro lado, en un artículo QuitGamble.com (2024) indico que Letonia es uno de los países con más graves dificultades relacionadas con el juego. En Letonia, el 6,0% de la población presenta problemas con las apuestas.

Los impactos en la salud mental y comportamientos adictivos por exposición temprana a los juegos de azar pueden llevar a comportamientos problemáticos y a desarrollar una adicción al juego en etapas posteriores de la vida. Según estudios, los adolescentes son más propensos a desarrollar ludopatía, y esta problemática se agrava cuando el acceso es fácil y no regulado. La falta de mecanismos de control efectivo en línea contribuye a una mayor vulnerabilidad de este grupo.

Muchas normativas dispersas y cumplimiento desigual las legislaciones varían entre países, lo que permite que los menores burlen los controles accediendo a sitios de juegos de azar alojados en jurisdicciones con menor regulación. Además, muchas plataformas internacionales operan en varios mercados sin una supervisión adecuada, lo que hace difícil asegurar el cumplimiento de las normas locales.

En Perú, la situación es alarmante, un espejo del problema global, en el que los ingresos se celebran mientras las cifras de afectados se ignoran. El mercado crece como un árbol frondoso, pero bajo sus raíces, los casos de ludopatía en adolescentes se multiplican como malas hierbas. Es la antítesis del desarrollo sostenible que un sector florezca a costa del bienestar de la juventud. El diagnóstico es simple, y a la vez, devastador: la industria se construye sobre un sistema de registro tan débil que es como una puerta sin cerradura. Un campo fértil para el fraude, la suplantación de identidad y el acceso de menores.

Además, en Perú, durante el 2024 el Ministerio de Salud atendió más de 11,000 casos relacionados con ludopatía, de los cuales un 32% correspondió a adolescentes entre 12 y 17 años. La situación resulta preocupante, ya que en los últimos dos años los casos en menores se incrementaron en un 25%, fenómeno vinculado al crecimiento de los casinos y las plataformas de apuestas en línea que captan principalmente a un público juvenil. Ministerio de Salud (2024)

Publicidad y marketing dirigidos incluyen a los menores de edad estando expuestos a publicidad agresiva en línea, lo que fomenta el interés por los juegos de azar. La segmentación de anuncios a través de redes sociales y motores de búsqueda no siempre excluye a los menores de edad, lo que aumenta la exposición al contenido relacionado con las apuestas y el juego.

Diagnóstico

El auge del juego en línea en Perú es como una inundación que arrastra todo a su paso, con un flujo creciente de personas que apuestan desde sus dispositivos. El sistema de registro, que debería ser un el primer filtro, es irónicamente una puerta de papel que se derrumba al menor contacto. Es interesante analizar que a pesar del valor económico que se le otorga a la industria, la entrada a esta parece no tener una protección real. La debilidad de los sistemas de verificación, que no validan correctamente los datos, aumenta el peligro de que se termine convirtiendo de un campo de juego a un pantano fértil para la suplantación de identidad, el fraude y, peor aún, el acceso de los menores.

Pronóstico

Si continuamos con este sistema tan vulnerable, en el futuro veremos cómo el fraude y el lavado de dinero surgen en un lugar idóneo para su crecimiento. La promoción del juego responsable, que debería el ángulo principal, se convertirá en una tarea casi imposible de lograr.

Es interesante notar que, mientras se busca el crecimiento, la falta de seguridad se convierta en una traba que amenaza con detener el progreso de la industria. La confianza de los clientes, se desvanecerán, exponiendo a las empresas a duras sanciones. Y a la larga, esta ausencia de seguridad del contraste del desarrollo sostenible y frenará el crecimiento de una industria que podría ser próspera si sus bases fueran sólidas.

Control del problema

La propuesta principal para resolver esta problemática es el uso de la tecnología como la primera línea de seguridad, esta se basa en la implementación de sistemas de verificación que actúen como un primer filtro incorruptible.

Estas herramientas incorporan herramientas como la verificación biométrica, la validación con DNI físico y una autenticación en tiempo real, que son parte de la solución planteada para las empresas involucradas. Estas herramientas ayudaran a la reducción de fraudes y el manejo seguro de los datos personales.

Debemos analizar un punto más a analizar, que ni la mejor tecnología servirá de nada si las partes involucradas no se comprometen a usarla. Para que las soluciones planteadas puedan funcionar de manera correcta, es fundamental que el Estado, las empresas involucradas y las entidades financieras trabajen en conjunto. Es un esfuerzo conjunto para construir un entorno de apuestas más seguro y confiable para todos en Perú.

2.2. Formulación del problema

2.2.1. Problema general

¿Cómo la implementación de la tecnología de verificación de identidad puede mejorar la gestión de datos de los usuarios en juegos de azar en línea?

2.2.2. Problemas específicos

¿Cuáles son las limitaciones y fallas actuales en la verificación de identidad para la gestión de datos de los usuarios en juegos de azar en línea?

¿Qué percepción tienen los usuarios sobre la efectividad de verificación de identidad en juegos de azar en línea?

¿Qué tecnologías avanzadas pueden aplicarse para mejorar la verificación de identidad de los usuarios en juegos de azar en línea?

2.3. Objetivos de investigación

2.3.1. Objetivo general

Proponer la implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea.

2.3.2. Objetivos específicos

Determinar cómo la implementación de la tecnología de verificación de identidad puede mejorar las funciones de tecnologías implementadas en juegos de azar en línea

Determinar cómo la implementación de la tecnología de verificación de identidad puede mejorar la seguridad de información de los usuarios en juegos de azar en línea.

Determinar cómo la implementación de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea

2.4. Justificación de la investigación

2.4.1. Justificación teórica

El auge del juego en línea en Perú es como una inundación que arrastra todo a su paso, pero la ironía es que el sistema de registro, que debería ser un guardián inquebrantable, es en realidad una puerta de papel. Esto crea un contraste directo entre el crecimiento económico

de la industria y el aumento de la vulnerabilidad, un campo fértil para el fraude y el acceso de menores, que amenaza con convertirse en una tormenta que se avecina si el gobierno no actúa. Se propone un cambio hacia una seguridad robusta, usando la tecnología como un escudo de protección y la contracara de las deficiencias actuales. Es un cambio total que busca que la industria sea un entorno seguro, en vez del castillo de naipes que es ahora. La clave para que este sistema funcione es que el Estado, las empresas de juegos y las entidades financieras trabajen juntos para construir un futuro más seguro, que es el polo opuesto al descontrol que se vive hoy en día.

2.4.2. Justificación metodológica

El estudio, se desarrolla a través del análisis, diseño y evaluación de los sistemas de verificación. La ironía está en que, para corregir un proceso que se percibe como simple, se necesitan métodos rigurosos y complejos. La recolección de datos como punto principal y la satisfacción del usuario como punto clave, permite medir los resultados de las soluciones planteadas. El uso de gráficos estadísticos y estudios comparativos, nos permite identificar patrones y áreas de mejora. La aplicación de pruebas experimentales aplicadas que evalúan con objetividad la precisión, velocidad y aceptación de tecnologías como la biometría y el análisis documental nos permite planear un camino de mejora.

2.4.3. Justificación práctica

La creación de un sistema de registro es la primera solución a las problemáticas actuales. Es un cambio total que plantea un sistema seguro, eficiente y adaptable. Para las empresas, lo interesante es que, al invertir en seguridad, algo que a menudo evitan, terminan obteniendo

logros positivos, reduciendo riesgos legales y costos operativos. Para los reguladores, el sistema nos protege del fraude y el acceso de menores, permitiendo un control que es lo opuesto a lo visto actualmente. Para los usuarios, el proceso de registro, ofrecerá una experiencia ágil y segura que los hace sentir más cómodos al apostar.

2.5. Viabilidad de la investigación

Debido a que esta es una problemática a gran escala existen muchos datos a la mano para poder analizarlos, debido a que ambos hemos estudiado TI tenemos conocimiento sobre el análisis de datos, otro aspecto que nos ayudara es La tecnología para la verificación de identidad, como la biometría y la autenticación multifactorial, está en constante evolución y se ha vuelto más accesible. Esto permite desarrollar soluciones prácticas y escalables que pueden ser implementadas en plataformas de juego.

Ahora, se detallarán algunos aspectos que garantizan la viabilidad del presente estudio:

La investigación aquí planteada, se apoya en una fuente de información bastante amplia. Aunque, para combatir las problemáticas de las apuestas en línea debemos recurrir a la información que está a la vista de todos. Este proyecto no solo es técnicamente viable gracias a tecnologías avanzadas como la biometría, sino que además aborda un problema de creciente relevancia social y económica, cuya urgencia se ha hecho más clara incluso durante la pandemia. Económicamente, el proyecto representa una oportunidad única con una inversión relativamente baja, especialmente cuando se compara con los elevados costes que actualmente tienen las empresas de este rubro. Legalmente, no hay problemas, ya que no se busca reformar ninguna ley, sino optimizar las ya existentes. Todo esto sugiere que los resultados de esta investigación caerán en terreno fértil, pues tanto la industria como los

reguladores buscan activamente soluciones para un problema que, irónicamente, ellos mismos contribuyeron a crear.

2.6. Limitaciones de la investigación

Aunque esta investigación es muy viable, es importante reconocer que enfrenta ciertos desafíos que podrían dificultar tanto su desarrollo como la puesta en práctica de las soluciones que propone. Aquí, se describen las principales limitaciones encontradas:

Desde el punto de vista técnico y económico, uno de los principales desafíos de esta investigación es la compleja aplicación de tecnologías avanzadas, como la biometría o el reconocimiento facial, en las plataformas de juego de azar en línea. Si bien estas herramientas son viables en teoría, llevarlas a la práctica a gran escala supone un verdadero desafío para muchas empresas, en especial para aquellas cuyo margen de ganancia no es muy alto. El elevado desembolso inicial, lo complicado que resulta integrarlas con los sistemas que ya están operativos y la infraestructura adicional que requieren son factores que pueden hacer que las empresas se lo piensen dos veces antes de adoptar este tipo de soluciones.

Una de las mayores dificultades encontradas es la falta de un criterio uniforme a nivel internacional. Las normativas sobre juegos de azar en línea cambian radicalmente de un país a otro, lo que complica enormemente el desarrollo de soluciones aplicables de manera global. En algunos países tienen regulaciones estrictas, otros son más permisivos, lo que facilita que los menores puedan eludir los controles accediendo a sitios de juegos de azar en jurisdicciones menos reguladas. La falta de una regulación global coherente y la dificultad de coordinar esfuerzos internacionales hacen que sea complejo asegurar un cumplimiento uniforme de las propuestas de control.

Resistencia de las plataformas de apuestas las plataformas de juegos de azar en línea podrían mostrar resistencia a la adopción de nuevas tecnologías y regulaciones más estrictas esto

podría generar fricción en la experiencia del usuario y afectar la rentabilidad. Algunas plataformas podrían priorizar la retención de usuarios y la minimización de costos por encima de la implementación de controles más robustos, lo que podría dificultar la adopción de las soluciones propuestas. Además, el equilibrio entre la protección de los menores y la experiencia del usuario es un desafío que podría generar resistencia por parte de los operadores.

Limitaciones de los sistemas de verificación es posible que estos sistemas no sean infalibles, la investigación propone la implementación de tecnologías avanzadas de verificación de identidad. A pesar de los controles, los menores podrían seguir colándose utilizando documentos falsos, cuentas prestadas de familiares o amigos, o aprovechando nuevas formas de ocultar su identidad en internet. Esto demuestra lo difícil que resulta crear un sistema de verificación que sea realmente infalible.

La privacidad y la protección de datos personales surgen como una preocupación fundamental al implementar tecnologías como la biometría o el reconocimiento facial. Es comprensible que muchos usuarios muestren recelo a compartir información biométrica por cuestiones de seguridad, lo que sin duda podría dificultar la adopción de estas soluciones. Además, normativas como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea establecen límites muy estrictos sobre el uso de este tipo de datos, añadiendo otra capa de complejidad al panorama.

La investigación busca proteger a los jóvenes de los peligros del juego online, pero tenemos que ser conscientes de que aplicar restricciones demasiado estrictas podría terminar generando reacciones contrarias a las esperadas en su comportamiento. Por ejemplo, los jóvenes podrían reaccionar buscando alternativas aún más peligrosas, como plataformas no reguladas o mercados clandestinos de apuestas, donde estarían aún más expuestos. Esta

posibilidad nos revela una limitación importante en la efectividad de cualquier propuesta de control.

Uno de los mayores retos de esta investigación es la escasez de datos reales sobre el comportamiento de los menores en plataformas de apuestas online. Como el acceso de los menores de edad a estos sitios en línea no es legal, resulta complicado obtener información precisa. Además, las propias plataformas no comparten datos sobre usuarios menores de edad, lo que nos obliga a basar gran parte del análisis en estudios indirectos o en información extraída de investigaciones sobre adicción al juego en jóvenes.

Representa un desafío constante el ritmo al que avanza la tecnología para cualquier propuesta de control. Herramientas como la IA o la biometría evolucionan tan rápido algo planteado hoy puede ya no servir en unos años. Además, los jóvenes, suelen adaptarse con mayor rapidez que los sistemas de control, encontrando muchas formas de saltárselas. Estos desafíos hacen muy difícil implementar soluciones que sean efectivas a largo plazo.

Un desafío adicional es la poca transparencia de las plataformas. Estas suelen negarse a compartir datos de usuarios o información sobre sus operaciones internas, lo que nos impide analizar la situación real y, por tanto, evaluar con precisión si las soluciones propuestas serían efectivas.

Variabilidad en la regulación en este caso la ley para estas páginas es la Ley N° 31557, así que debemos alinear nuestras propuestas con el marco legal dispuesto aquí.

La investigación sigue siendo relevante y viable. Sin embargo, es fundamental reconocer estos desafíos para ajustar las expectativas sobre los resultados y para diseñar soluciones que tengan en cuenta las barreras técnicas, regulatorias y operativas. Además, será necesario considerar enfoques complementarios, como la educación y la concientización, para maximizar el impacto de las soluciones propuestas.

CAPÍTULO III: MARCO REFERENCIAL

3.1. Antecedentes de la investigación

3.1.1 Antecedentes nacionales

Velásquez Santos (2021) desarrolló la investigación titulada “¿Es viable la regulación a los juegos de azar virtuales incluidos en los videojuegos multijugador en línea para prevenir a niños y adolescentes de la ludopatía?: una aproximación desde el Derecho”, presentada en la Pontificia Universidad Católica del Perú, analiza el vacío legal existente en el país respecto a los juegos de azar virtuales integrados en videojuegos accesibles a menores de edad. El autor evidencia que, aunque la normativa peruana regula los juegos de azar físicos como los casinos y tragamonedas, no contempla los mecanismos de azar digital como las “loot boxes” o microtransacciones presentes en los videojuegos. A de un enfoque jurídico comparado, propone la creación de un sistema nacional de clasificación de videojuegos por edades, liderado por el Ministerio de Cultura y una comisión multisectorial, con el objetivo de prevenir la ludopatía en niños y adolescentes y garantizar su protección frente a los riesgos del entorno virtual, constituyéndose en un importante antecedente para futuras investigaciones sobre derecho digital, políticas públicas y protección de menores en entornos tecnológicos.

Risco (2020), desarrollo la investigación titulada "Riesgo al Trastorno de Juego por Internet (IGD) y su relación con la Función Parental", tuvo como objetivo fundamental establecer la naturaleza de la relación entre el riesgo de desarrollar el Trastorno de Juego por Internet, y la percepción que los jóvenes tenían sobre la función parental (basada en el modelo de Vazsonyi). El estudio cuantitativo correlacional se llevó a cabo con una muestra de 94 estudiantes universitarios de Lima Metropolitana, a quienes se les administraron los instrumentos IGD-20 y la Prueba de Función Parental Adolescente (AFP). Los resultados revelaron que la función parental del padre no mostró ninguna asociación significativa con el

riesgo de IGD. No obstante, en la relación con la figura materna, se encontró que una mayor percepción de soporte de la madre se relacionaba directamente con un mayor riesgo de IGD, mientras que una baja percepción de comunicación y monitoreo materno se relacionaba inversamente con el trastorno. Estos hallazgos sugieren que el riesgo a la adicción a los juegos por internet en este grupo es complejo y está influenciado por aspectos específicos de la dinámica con la madre, y se agrava con el aumento de las horas de juego.

La Madrid Coz y Ruiz Toledo (2023), desarrollaron la investigación titulada "Implementación de un sistema de autenticación mediante validación biométrica para procesos bancarios" con el objetivo de desarrollar una solución robusta de validación biométrica facial que garantizara mayor seguridad en las transacciones. El fundamento teórico se centró en técnicas de procesamiento de imágenes y reconocimiento facial, específicamente el método Haarcascade y algoritmos de Deep Learning, respaldados por normativas legales de la SBS. Para el desarrollo, se utilizaron como instrumentos el lenguaje Python, la librería OpenCv 2 y la integración de una API de RENIEC para el cotejo de identidades. Las pruebas, que emplearon una muestra de una base de datos interna y la data de RENIEC, arrojaron como resultado principal una precisión del 95.5% en la identificación y autenticación. Este alto porcentaje validó el sistema como una herramienta efectiva para optimizar la seguridad en los procesos bancarios, superando la tasa de precisión mínima requerida para imágenes de baja calidad.

3.1.2 Antecedentes internacionales

Ortiz Salazar y Morales Torres (2021) desarrollaron la investigación titulada “Modelo para sistema de fidelización con reconocimiento facial para terminales de juego en casinos, orientado a facilitar el acceso a clientes sin medios externos de identificación”, cuyo objetivo fue diseñar un modelo de sistema de fidelización para clientes frecuentes en casinos, con el

fin de generar confianza, anonimato, comodidad y aumentar los ingresos de las salas. La base teórica se sustentó en el uso del Internet de las Cosas, el hardware Raspberry Pi, cámaras de alta definición con sensores infrarrojos y la biblioteca OpenCV para la detección facial, además de fundamentos sobre fidelización de clientes, marketing relacional y biometría aplicada a la seguridad. La metodología fue de tipo descriptiva, empleando métodos inductivo y deductivo, apoyados en observación directa y encuestas para recopilar información sobre la experiencia de los usuarios. Los instrumentos utilizados fueron cuestionarios y diagramas de casos de uso, requerimientos funcionales y no funcionales. La población estuvo compuesta por clientes y administradores de casinos, específicamente de la empresa CODERE Colombia. Los resultados mostraron la creación de un prototipo funcional que integró software y hardware en las terminales de juego, eliminando las tarjetas físicas y mejorando la experiencia de usuario, garantizando el anonimato, incrementando la cantidad de clientes afiliados y optimizando los ingresos de las salas.

Peña Román (2022) desarrolló la investigación titulada “Herramienta de reconocimiento facial de emociones para videojuegos”, cuyo objetivo fue crear una herramienta de reconocimiento facial de emociones que permitiera determinar la respuesta y satisfacción de los usuarios, contribuyendo a mejorar el proceso de pruebas de los videojuegos desarrollados en el Centro de Tecnologías Interactivas de la Universidad de Ciencias Informáticas. La base teórica se sustentó en conceptos de reconocimiento facial, emociones, computación afectiva, inteligencia artificial y aprendizaje automático, tomando como referencia las teorías de Paul Ekman sobre las emociones básicas y aplicando la técnica geométrica 2D como método principal para el análisis facial. Se emplearon métodos teóricos como el histórico-lógico, el análisis y síntesis, la modelación e hipotético-deductivo, así como métodos empíricos de observación y pruebas de aceptación. Los instrumentos utilizados incluyeron lenguajes UML y Python, el framework Django, el entorno PyCharm, herramientas de modelado como Visual Paradigm y bibliotecas

tecnológicas como OpenCV, NumPy, DeepFace, H5py, TensorFlow y Tkinter, junto con bases de datos MySQL. La población estuvo conformada por usuarios y desarrolladores del Centro de Tecnologías Interactivas, mientras que la muestra incluyó videojuegos desarrollados por el centro y usuarios seleccionados para las pruebas. Los resultados evidenciaron la implementación exitosa de una herramienta funcional de reconocimiento facial de emociones capaz de analizar en tiempo real las respuestas emocionales de los jugadores, mejorando la calidad, precisión y efectividad del proceso de evaluación de videojuegos.

Tapia Iñíguez (2025) desarrollaron la investigación titulada “El fenómeno de las loot boxes en adultos jóvenes chilenos”, cuyo objetivo fue analizar este fenómeno en adultos jóvenes, identificando las percepciones, comportamientos y motivaciones que impulsan su uso, así como su relación con las dinámicas del consumo digital y el juego de azar. La base teórica se sustentó en los conceptos de economía del videojuego, gamificación, psicología del consumo, recompensas variables y ludopatía, abordando teorías sobre el refuerzo intermitente y el gasto impulsivo, y destacando las similitudes entre las loot boxes y las prácticas del gambling tradicional. La metodología empleada fue de enfoque cualitativo, con un diseño interpretativo y fenomenológico, utilizando entrevistas semiestructuradas como técnica principal. Los instrumentos aplicados incluyeron guías de entrevista, grabaciones, transcripciones y matrices de codificación temática. La población estuvo conformada por adultos jóvenes chilenos usuarios de videojuegos con loot boxes, y la muestra se compuso por ocho participantes de entre 18 y 30 años. Los resultados revelaron que las loot boxes son percibidas principalmente como una extensión del entretenimiento, aunque generan conductas impulsivas y patrones de consumo problemáticos asociados a la gratificación inmediata, la expectativa de recompensa y la presión social, evidenciando un riesgo latente de comportamientos adictivos similares a los del juego de azar.

3.2. Marco teórico

3.2.1 Tecnología de verificación de identidad

Biometría facial

La tecnología de biometría facial se ha afianzado como una de las tecnologías más confiables e innovadoras para la verificación de identidad en los últimos tiempos, transformándose en algo esencial en sectores sensibles como el bancario, financiero y, de forma creciente, en la industria de los juegos de azar en línea. La tecnología opera bajo la premisa de que los rasgos faciales son únicos e irrepetibles, permitiendo la autenticación de usuarios de forma rápida y precisa a través de algoritmos avanzados que analizan múltiples puntos del rostro.

La eficacia de la biometría facial es innegable, ya que supera las vulnerabilidades de los métodos de autenticación tradicionales que ya conocemos, como las contraseñas, que son susceptibles a ataques de phishing y robo de credenciales. La integración de esta tecnología demuestra ser una herramienta robusta que combina precisión, accesibilidad y un elevado nivel de protección frente al fraude, pues utiliza sistemas de Inteligencia Artificial (IA) y Deep Learning para analizar patrones faciales únicos; de hecho, como lo afirma el reconocido investigador en ciberseguridad Schneier (2015), la seguridad está evolucionando rápidamente, y la biometría representa un avance crucial para la autenticación en el entorno digital, ofreciendo una capa de protección intrínseca que no es transferible ni adivinable, consolidando a la biometría facial como una de las aplicaciones más críticas de la Inteligencia Artificial en la seguridad digital actual.

La adopción de la biometría facial en el sector de los juegos de azar en línea corresponde a la necesidad que tienen las plataformas en línea de reforzar los entornos digitales seguros y confiables, debido al notable aumento de casos de fraude, lavado de dinero y suplantación de identidad asociados al crecimiento de las apuestas virtuales. Gracias al reconocimiento facial,

es posible verificar en tiempo real la identidad de los usuarios antes de que accedan a sus cuentas o efectúen transacciones financieras, lo que acelera los procesos de autenticación y eleva la percepción de confiabilidad y eficiencia.

La eficacia de la biometría facial es innegable, ya que supera las vulnerabilidades de los métodos de autenticación tradicionales que ya conocemos, como las contraseñas, que son susceptibles a ataques de phishing y robo de credenciales. La integración de esta tecnología demuestra ser una herramienta robusta que combina precisión, accesibilidad y un elevado nivel de protección frente al fraude, pues utiliza sistemas de Inteligencia Artificial (IA) y Deep Learning para analizar patrones faciales únicos. Como lo afirma el tecnólogo e investigador en biometría Jain, Ross, y Nandakumar (2011), El reconocimiento facial es notablemente superior a la autenticación tradicional por contraseña, principalmente porque es imposible de suplantar al usuario. Esto confirma que la Inteligencia Artificial no solo se perfila como la tecnología más transformadora de nuestro siglo, sino que su aplicación en el campo de la biometría constituye una de sus herramientas más críticas para la seguridad digital.

Es fundamental destacar que la biometría facial no solo transforma los niveles de seguridad en las plataformas de juego en línea, sino que también redefine de manera significativa la experiencia del usuario. Los métodos de siempre para entrar, como las contraseñas o esas preguntas de seguridad que te piden, se sienten lentos, aburridos y hasta un poco inseguros. En cambio, la autenticación biométrica te da acceso casi al momento y sin problemas, encajando de forma totalmente natural en la rutina del jugador.

Esta tecnología logra algo genial: transforma un proceso que antes era un dolor de cabeza en algo totalmente fluido, intuitivo y a la altura de lo que esperamos hoy en día. Un buen ejemplo de esto es cuando las apps de apuestas online usan el reconocimiento facial: con solo mirar la cámara, el usuario entra rápido y seguro, igual que cuando desbloquea su móvil. Esta comodidad no solo hace que el cliente confíe más en que sus datos están protegidos, sino que

también hace que la plataforma se vea moderna y eficiente, algo clave para que los usuarios se queden.

En un sector tan competido como este, donde que el usuario se quede o se vaya depende mucho de la confianza y de lo cómodo que se sienta, estas ventajas tecnológicas son un as bajo la manga. Marcan la diferencia entre las empresas que innovan y las que se quedan atrás. Como dijo Schwab (2016), En la nueva era digital, la confianza es la moneda más importante", y esto es súper cierto en los juegos de azar online. Que la gente confíe en nuestra seguridad y que todo sea fácil de usar puede ser la clave para que una marca no solo sobreviva, sino que se posicione como líder.

Hay otro punto vital con el reconocimiento facial: nos ayuda a cumplir con todas esas normas internacionales, sobre todo con las políticas KYC (Conoce a tu Cliente) y AML (Anti-Lavado de Dinero). Estas reglas obligan a las plataformas de apuestas a saber exactamente quién es el usuario para evitar cosas ilegales como el lavado de dinero. Y el reconocimiento facial simplifica todo esto con una verificación continua y automática, asegurándose de que la identidad del usuario es correcta en cada movimiento o transacción.

Ahora bien, meter la biometría no es tan fácil, tiene sus desafíos importantes. El principal es cómo manejamos esos datos biométricos que recopilamos, ya que son súper sensibles y necesitan protocolos de seguridad y cifrado muy estrictos. Hay una preocupación ética real sobre la vigilancia a gran escala y la libertad individual, lo que nos obliga a buscar urgentemente un equilibrio entre la seguridad y nuestros derechos básicos. Sobre esto, es clave tener presente la advertencia de que, si estas tecnologías se extienden a los espacios públicos, podríamos perder el anonimato y estar bajo monitoreo constante, lo que plantea "un riesgo considerable de vulneración a los derechos humanos, especialmente el derecho a la privacidad y la no discriminación" Gamarra (2024). Por eso, tenemos que revisar el desarrollo de estos sistemas sin descanso para asegurar que las libertades civiles estén protegidas.

Para ponerlo simple: el reconocimiento facial se está volviendo la estrella para saber quién es quién en las apuestas online. Nos da un sistema rapidísimo y súper seguro que, además, hace que la experiencia del usuario sea mucho mejor. Es fundamental para cortar el fraude y para que sea más fácil cumplir con todas las normas. No obstante, para asegurar su eficacia, su implementación debe verse siempre a través del filtro del poder, ya que, como señaló Zuboff (2019). “toda tecnología es expresión de poder, y la cuestión es quién lo ejerce y con qué propósito”. Por ello, su despliegue exige medidas estrictas de protección de datos y un marco ético transparente que garantice el consentimiento y el uso responsable, siguiendo las directrices de la Agencia de Ciberseguridad de la Unión Europea. Solo de esta manera las plataformas podrán no ser solo más competitivas, sino también construir un entorno digital confiable y sostenible

Huella digital:

La huella dactilar es una de las tecnologías biométricas más populares y usadas en todo el mundo. Lo mismo te sirve para abrir una puerta cualquiera que para acceder a sistemas digitales con seguridad máxima. Su gran valor es que el patrón de crestas y valles que tenemos es totalmente único e irrepetible para cada persona. Esto la convierte en un identificador muy potente, barato y fácil de usar en muchos sitios, especialmente en las apuestas en línea, donde evita suplantaciones y asegura que solo el dueño legítimo haga las transacciones. A diferencia de las contraseñas o los PIN, que se pueden robar, la huella dactilar ofrece una certeza mucho mayor porque se basa en algo físico e intransferible. Esto tiene una razón de peso. De hecho, expertos como Maltoni, Maio, Jain, y Prabhakar (2022) lo confirman al señalar que “las huellas dactilares siguen siendo la modalidad biométrica más consolidada y fiable debido a su unicidad, permanencia y bajo costo de implementación, lo que explica su adopción masiva en sectores tan diversos como la banca, la seguridad y los servicios en línea.

En el mundo digital, las cosa con el reconocimiento de huellas ha cambiado mucho por la tecnología: dejamos atrás esos sensores ópticos viejos y fáciles de engañar con copias, y llegaron los sensores capacitivos, ultrasónicos y de alta resolución. Esto hizo que la seguridad se disparara y que el fraude se redujera muchísimo. Estas mejoras permitieron que la biometría dactilar se democratizara, llegando a los teléfonos móviles de uso masivo, lo que crea un escenario ideal para integrarla en aplicaciones como las apuestas en línea. Dado que millones de usuarios ya usan su huella para desbloquear sus smartphones o pagar, este método se adopta sin ser percibido como intrusivo o complicado. De hecho, estudios como el de Ratha, Connell, y Bolle (2001) destacan que la aceptación social de la biometría dactilar supera a la de otras tecnologías más recientes, debido precisamente a que los usuarios se sienten cómodos y confiados con su uso diario, permitiendo a las plataformas de juego aprovechar esta tecnología ya probada para optimizar la experiencia del cliente.

introducir la tecnología de huella dactilar en las plataformas de apuestas online trae muchísimas ventajas al sector, mejorando tanto la seguridad como lo fácil que resulta usar la aplicación. En primer lugar, fortalece la protección de las cuentas al impedir que terceros utilicen credenciales robadas para acceder o realizar transacciones, y a la vez facilita el cumplimiento de normativas internacionales vinculadas a la identificación de usuarios, como Know Your Customer (KYC) y Anti-Money Laundering (AML). Al igual que ocurre con la biometría facial, la verificación dactilar asegura que cada jugador es realmente quien afirma ser, reduciendo el riesgo de fraudes y operaciones ilícitas, esta tecnología puede además integrarse con sistemas de monitoreo en tiempo real, capaces de generar alertas ante intentos de acceso sospechosos o repetitivos; por ejemplo, si una misma huella se utiliza para ingresar desde múltiples ubicaciones geográficas en cortos períodos, el sistema puede bloquear automáticamente la actividad hasta confirmar la identidad del usuario.

Otro beneficio fundamental es lo fácil que resulta usarla. A diferencia de esos métodos antiguos donde hay que recordar contraseñas complicadas o hacer mil pasos extra, la verificación por huella es instantánea, muy simple y funciona en cualquier dispositivo compatible. "Esto ayuda mucho a que los clientes se queden, porque valoran enormemente las plataformas que son, a la vez, seguras y cómodas. Y si nos fijamos en los números, meter sistemas de huella dactilar sale más a cuenta que usar tecnologías punteras como el reconocimiento de iris o la autenticación por blockchain. Esto convierte a la biometría dactilar en una opción rentable y muy atractiva, sobre todo para las empresas de juegos en mercados nuevos. Sin embargo, no todo es perfecto; tiene sus peros. Por ejemplo, puede haber fallos de lectura si las huellas de un usuario están dañadas por la edad, el trabajo o temas de salud, lo que genera problemas de acceso. Y aunque clonar una huella es difícil, se han dado casos de ataques sofisticados. Esto último es crucial, porque si la huella se compromete, no puedes reemplazarla, lo que nos obliga a usar un enfoque de seguridad de muy alto nivel. Por este motivo Ross y Jain (2004) recomiendan que no usemos la huella digital sola, sino como un elemento dentro de un sistema de autenticación multifactorial (MFA). La idea es combinarla con otros métodos, como contraseñas dinámicas o el reconocimiento facial, para minimizar los riesgos y hacer que la seguridad sea globalmente mucho más robusta. Y ojo, aparte de eso, es fundamental usar protocolos de cifrado muy rigurosos y cumplir a rajatabla con todas las normativas de protección de datos. Esto es un punto clave: si, por desgracia, se llega a filtrar la información biométrica de los usuarios, el problema es muchísimo más grave y duradero que si solo se robaran unas contraseñas.

Para cerrar, la verificación por huella dactilar es una tecnología que ya está madura, es muy confiable y la gente la acepta bien. Ofrece ventajas claras en seguridad, es fácil de usar y más económica comparada con otras opciones. Usarla en la industria de juegos de azar online es una oportunidad estratégica: mejora cómo se manejan los datos, ayuda a cumplir con las

normas internacionales y, lo más importante, refuerza la confianza en un sector que se enfrenta cada vez más al fraude y la suplantación de identidad. En conclusión, la tecnología de huella dactilar es esencial hoy en día en las apuestas online. Es un factor que influye directamente en que las operaciones sean más seguras y eficientes. Hay un consenso claro entre los expertos en seguridad digital. Tal como señalan Choo y Liu (2006), "la gestión de la identidad digital, que incluye la verificación y autenticación de usuarios, es esencial para mitigar riesgos y establecer una confianza operativa en los sistemas de información". Pero, para que esto funcione del todo, no basta solo con instalar la tecnología. Es clave que su uso vaya de la mano con medidas técnicas muy serias (como un cifrado de última generación) y con leyes bien sólidas. Solo así podremos asegurar que los datos biométricos están blindados y que reducimos al máximo los puntos débiles. Así, la huella dactilar consigue que el mundo digital sea más que solo seguro y rápido: también se vuelve más ético, responsable y de fiar.

Blockchain:

La tecnología blockchain ha revolucionado muchos sectores económicos y sociales al darnos un sistema descentralizado, transparente y muy seguro para registrar y validar operaciones digitales. Si bien se hizo famosa por las criptomonedas, ha crecido mucho, y hoy una de sus aplicaciones más importantes es la verificación de identidad. A diferencia de los sistemas de autenticación de siempre, que guardan todos los datos en un solo lugar y son fáciles de atacar, blockchain reparte la información en una red de nodos. Esto hace que sea casi imposible manipularla, cometer fraudes o que alguien entre sin permiso. En las apuestas online, esta tecnología es una gran opción para manejar los datos de los usuarios, ya que permite crear identidades digitales que son seguras, fáciles de comprobar y resistentes a la falsificación. Básicamente, blockchain nos da una respuesta fundamental para cualquier entorno digital que exija tener total certeza y seguridad sin tener que confiar en un solo punto de control. La

investigadora Swan (2015), que fue de las primeras en analizar la tecnología a fondo, lo deja muy claro: “la capacidad de la blockchain para crear un registro inmutable, distribuido y consensuado de la verdad es su principal valor”. O sea, que toda esta arquitectura descentralizada y criptográfica es fundamental para construir sistemas donde la confianza ya está metida en el diseño mismo. De esta forma, nos aseguramos de que los datos sean totalmente transparentes, estén blindados y que nadie pueda meterles mano.

El gran aporte de blockchain a la verificación de identidad se llama Identidad Soberana Digital (SSI). Con esto, tú eres el dueño absoluto de tu identidad y decides qué datos compartes, sin depender de nadie más, ni de bancos, ni de gobiernos, ni de ninguna empresa. Esta autonomía es muy atractiva en las apuestas online, donde la gente se preocupa mucho por el mal uso de sus datos personales y financieros. Gracias a blockchain, un jugador podría confirmar su identidad de forma segura (criptográfica) ante una plataforma de apuestas sin necesidad de enviar copias de documentos sensibles. Así se reduce drásticamente el riesgo de que la información sea robada. Estudios recientes sostienen que la Identidad Autosoberana (SSI) representa un cambio de paradigma en la gestión de datos, al pasar de sistemas centralizados y vulnerables a un modelo descentralizado que prioriza la privacidad y el control individual. Como resalta el tecnólogo Allen (2016), la SSI pone al individuo como dueño de sus propias credenciales, algo que es vital para el futuro de la confianza digital. Por ejemplo, una plataforma de juegos online podría verificar la identidad de un usuario usando credenciales que ya fueron certificadas en la cadena de bloques, con la seguridad de que esa información no se ha tocado. Este modelo de verificación que se puede reutilizar no solo hace las operaciones más eficientes y cómodas para el usuario, sino que también aumenta la transparencia y la trazabilidad de todas las transacciones, aspectos clave en un sector tan regulado y vulnerable al fraude

Hay una ventaja clave más del blockchain: la información que mete no hay quien la mueva. Una vez que el dato se registra, si alguien intenta cambiarlo, toda la red salta la alarma, lo que da una seguridad que las bases de datos comunes ni se acercan a ofrecer. Esto es importantísimo para las apuestas online, que viven luchando contra las cuentas e identidades falsas. Y como la información está distribuida por muchos sitios, no hay que confiar en un solo servidor. Esto reduce muchísimo el riesgo de que un ciberataque o un fallo técnico nos deje en la lona. Al final, la fuerza del blockchain en seguridad digital está justo en eso: en su descentralización, que elimina los puntos que podrían fallar. Como destacan Xu, Chen, Kou, y Heijden (2019) en su investigación, “la descentralización es un factor clave que permite que blockchain ofrezca una mayor resiliencia y confianza en la integridad de los datos”. Sin embargo, aplicar esta tecnología a la verificación de identidad también tiene sus retos importantes. Entre ellos está la escalabilidad, porque validar cosas en redes públicas puede ser más lento y caro que en los sistemas centralizados. También está la interoperabilidad: no hay una regla universal que haga que las distintas blockchains se entiendan entre ellas. Además, está el asunto de que las diferentes blockchains no se hablan (la famosa interoperabilidad), porque les falta un estándar común. Y luego, el gran punto: el marco legal. Muchas de nuestras leyes aún no reconocen como válidas las identidades digitales que nacen con esta tecnología. Todo esto nos lleva al último reto: hay que educar bien a la gente y a las empresas para que entiendan la tecnología y superen esa resistencia que les da su complejidad.

A pesar de los desafíos que mencionamos, es innegable el enorme potencial que tiene blockchain para cambiar por completo la forma en que se verifica la identidad en las apuestas online. Su capacidad para asegurar la privacidad, la seguridad, la transparencia y la trazabilidad lo convierte en un socio estratégico clave, especialmente en un sector donde la confianza del usuario es lo que define si un negocio se mantiene o no. En resumen, blockchain

es una innovación que rompe los esquemas, superando las limitaciones de los sistemas de autenticación de siempre. Nos da una alternativa descentralizada y a prueba de fraudes que, si se implementa bien, puede transformar la manera en que las plataformas de apuestas manejan los datos de sus clientes. De esta forma, no solo se mejoran la seguridad y el cumplimiento de las normas, sino que también impulsamos una nueva relación digital basada en la confianza, la transparencia y la autonomía total del usuario. El blockchain va más allá de solo ser la tecnología de las criptomonedas, y se está convirtiendo en la base de todos los servicios digitales que vienen. Como afirman las expertas Filippi y Swan (2017) “blockchain no es únicamente una tecnología para transacciones financieras, sino una infraestructura capaz de redefinir la confianza en entornos digitales”. Este cambio es esencial porque, en esencia, la tecnología nos da la llave para construir un mundo digital mucho más seguro. Ahora, la confianza no va para las entidades centrales (como un banco o el gobierno), sino que está garantizada por la criptografía y el acuerdo de la red. Esto, en el fondo, está reescribiendo las reglas de cómo interactuamos y verificamos todo en internet

Verificación digital de identidad mediante procesos:

El proceso de verificación digital de identidad, conocido por sus siglas en inglés como KYC (Know Your Customer), de ahora en adelante verificación digital, se ha vuelto una de las medidas más importantes para asegurar que los usuarios sean realmente quienes dicen ser en entornos regulados, como el sector financiero, las empresas fintech y, últimamente, también en los juegos de azar online. A diferencia de la biometría o el blockchain, este método se enfoca en validar la identidad del usuario a través de la revisión de documentos oficiales (como el pasaporte, el DNI o la licencia de conducir), usando tecnologías de inteligencia artificial (IA) y reconocimiento óptico de caracteres (OCR) para complementarla. Este procedimiento, que antes se hacía a mano y de forma presencial, se ha digitalizado por completo, permitiendo que

los usuarios se registren de forma remota y en pocos minutos. La verificación digital no es solo para estar más seguros, sino que es una de las mayores novedades en el mundo de la regulación tecnológica. Los especialistas Arner, Barberis, y Buckley (2017), destacan que esta tecnología consigue un balance ideal: permite cumplir con todas las leyes sin sacrificar lo rápido que operan ni lo fácil que es para el cliente. Lograr este balance es fundamental en sectores con tantas reglas, como las apuestas online. Las soluciones avanzadas permiten a las plataformas cumplir con toda la verificación digital y la Prevención de Lavado de Dinero (AML) de forma fluida. Con esto, molestamos menos al usuario y ganamos en rentabilidad. En el sector de juegos de azar online, esta tecnología es vital porque no solo valida rápido la identidad de los jugadores, sino que también asegura que cumplen con la edad y la residencia legal, requisitos cruciales para operar en cualquier mercado regulado.

El funcionamiento de la verificación digital es bastante ingenioso. Comienza cuando el usuario sube sus documentos, que son leídos y validados automáticamente por sistemas OCR que extraen todos los datos importantes (nombre, identificación, etc.). Después, entra en acción la inteligencia artificial: compara la foto del documento con una selfie que te haces al momento. Usa el reconocimiento facial para confirmar que eres tú y evitar que te suplanten. En ocasiones, te piden incluso una “prueba de vida”, haciendo que parpadees o muevas la cabeza para asegurar que no es una foto. Todos estos sistemas han logrado reducir enormemente el fraude al abrir cuentas y, de paso, mejoran la experiencia del cliente al olvidarnos de las filas y las espera. Verificar la identidad en las apuestas online es beneficioso para todos. Por un lado, las empresas cumplen fácilmente con regulaciones vitales como la Prevención de Lavado de Dinero (AML), reducen sus costos operativos al automatizar los procesos y aseguran la calidad de sus datos. Por otro lado, el usuario siente mucha más confianza y transparencia al operar en una plataforma supervisada que minimiza el riesgo de fraude. Además, como es un proceso rápido y móvil, se elimina la fricción en el registro, mejorando la experiencia y

fidelizando a los jugadores. Para cerrar la idea, la verificación digital dejó de ser un simple trámite para transformarse en una ventaja competitiva esencial en la economía actual. Tal como señala la consultora PwC (2022), las soluciones de la verificación digital se han consolidado como un componente esencial para equilibrar la seguridad regulatoria con una experiencia de cliente ágil y confiable en entornos digitales". Esto demuestra que usar procesos de verificación avanzados, rápidos y fluidos es clave para las empresas. Así, no solo cumplen con reglas estrictas (como KYC y AML), sino que logran algo crucial: retener y atraer a clientes que solo quieren interacciones seguras y sencillas.

A pesar de sus ventajas, no todo es perfecto; esta verificación trae consigo retos importantes. El principal es la protección de datos: cuando digitalizamos y guardamos documentos oficiales, si la ciberseguridad no es de hierro, sube el riesgo de filtraciones. Luego está la inclusión digital, porque no todo el mundo tiene el móvil o la conexión adecuada para hacer el proceso online, dejando fuera a ciertas personas. Y hay un tema ético: a veces, la inteligencia artificial arrastra sesgos que provocan fallos al reconocer caras de ciertas etnias o géneros. Este problema de los sesgos algorítmicos es un reto técnico y ético enorme que amenaza la promesa de que la tecnología sea justa para todos. Como destacan los investigadores Biega, Gummadi, y Weikum (2018), estos sesgos "constituyen un reto ético y técnico para garantizar la equidad en los procesos de verificación digital, especialmente en sectores donde el acceso justo y transparente resulta crucial". Esto significa que los sistemas de autenticación podrían ser menos precisos o poner más barreras a ciertos grupos de personas. Por eso, es clave revisar muy bien los datos y los modelos de IA para que, por ser rápidos, no se pierdan la justicia ni la transparencia.

En resumen, la verificación digital de identidad, impulsada por inteligencia artificial, es una solución efectiva y muy adoptada para aumentar la seguridad y la confianza en las apuestas online. Su punto fuerte es que combina la revisión de documentos con biometría en tiempo

real, volviéndola indispensable para cumplir con las regulaciones, frenar el fraude y agilizar la experiencia del cliente. Eso sí, para implementarla bien, necesitamos políticas claras de protección de datos, auditar los algoritmos para que sean justos y crear programas de inclusión digital que aseguren que todos puedan acceder a ella. De esta forma, la verificación digital no solo sirve para comprobar identidades de manera eficiente, sino que es un componente esencial para crear un sector de apuestas online más seguro, transparente y que dure en el tiempo. Como bien señala la consultora Deloitte (2021), “la automatización de procesos la verificación mediante inteligencia artificial y biometría no solo mejora la eficiencia operativa, sino que también refuerza la confianza del usuario en entornos digitales altamente regulados”. La tecnología es crucial: permite a las plataformas seguir regulaciones exigentes (KYC y AML) sin demoras ni problemas, convirtiendo el simple trámite legal en una poderosa arma competitiva.

3.2.2. Gestión de datos de los usuarios

Recolección y almacenamiento seguro de datos:

Un aspecto central en la gestión de datos es, sin duda, cómo se recolecta y se guarda la información de forma segura. Piensa que esta es la base para todo lo demás: el análisis, la segmentación y la personalización de los servicios. En el caso de las apuestas online, esto cobra mucha más relevancia, ya que estas plataformas recogen un volumen enorme de datos sensibles cada día (personales, financieros y de comportamiento de los jugadores). Por normativa internacional, como el GDPR de la Unión Europea, recolectar estos datos exige cumplir con tres pilares: transparencia, finalidad legítima y el consentimiento informado del usuario. En pocas palabras, los usuarios tienen derecho a entender fácilmente qué información se les pide, para qué la van a usar y por cuánto tiempo la van a guardar. Como recuerdan los

expertos en privacidad Tene y Polonetsky (2013), “la confianza de los usuarios depende en gran medida de la percepción que tengan sobre cómo las organizaciones recopilan, usan y protegen su información personal”. Por lo tanto, manejar los datos de manera ética y transparente no es solo una obligación legal, sino que se convierte en una ventaja competitiva brutal para las empresas que quieren destacar. En sectores como el juego online, esta transparencia es lo más importante para retener clientes y construir una marca sólida y confiable.

Las plataformas de apuestas online recogen datos a través de muchísimos puntos de interacción, como los formularios de registro, las verificaciones de identidad, las transacciones financieras, y hasta los patrones de navegación o el servicio al cliente. Toda esta información se organiza en tres categorías: los datos personales (como el nombre, edad o dirección), los datos financieros (métodos de pago e historial de transacciones) y los datos de comportamiento (cuánto tiempo juegas o la frecuencia de tus apuestas). Tras recogerla, es fundamental que esta información se guarde en entornos digitales que aseguren al máximo que es segura y que no se alterará Para lograr esto, las empresas usan infraestructuras de almacenamiento en la nube con un cifrado de extremo a extremo, además de bases de datos distribuidas que las hacen menos vulnerables a ataques cibernéticos. Según Kuner (2020), un experto en derecho de la información, “el uso de tecnologías de encriptación y anonimización resulta indispensable para minimizar riesgos y cumplir con las normativas internacionales de protección de datos”. Esto es súper importante, porque en algunos sectores, que se filtre un dato puede destrozar la reputación y la confianza del usuario. Por lo tanto, usar estas tecnologías se vuelve no solo un requisito legal fundamental, sino también una estrategia esencial para gestionar crisis y mantener la confianza a largo plazo.

Guardar los datos de forma segura implica más que solo protegerlos de quien no debe verlos; también hay que asegurarse de que esos registros estén disponibles y sean fáciles de seguir para cualquier auditoría interna o regulatoria. Por eso, es vital tener políticas claras de gobernanza de datos que definan muy bien quién es responsable de qué a lo largo de todo el ciclo de la información. Por ejemplo, al establecer límites de tiempo para guardar los datos, evitamos acumular registros innecesarios y reducimos el riesgo ante cualquier fallo de seguridad. Además, usar controles de acceso por roles (RBAC) garantiza que solo el personal autorizado pueda acceder o cambiar información sensible, lo que nos protege mucho más de las amenazas que vienen de dentro. En las plataformas de apuestas online, estas medidas de seguridad aseguran que los datos de los usuarios solo se usen con los fines autorizados y que se cumplan las leyes de todos los reguladores. Un aspecto clave que no podemos olvidar es la responsabilidad social que implica recoger datos de los jugadores. Más allá de cumplir con la ley, esta información se convierte en una herramienta para detectar patrones de juego problemático y crear programas de juego responsable. Al tener registros exactos de cuánto apuestan, el tiempo que pasan jugando y su frecuencia, las plataformas pueden identificar a los usuarios en riesgo y ofrecerles medidas preventivas directas, como ponerles límites de depósito, darles pausas temporales o facilitarles asesoramiento especializado cuando se usa la gestión de datos de forma socialmente responsable, no solo mejoramos la percepción de la empresa, sino que demostramos que nos tomamos en serio la protección de los usuarios, logrando balancear el negocio con la ética. La Organización para la Cooperación y el Desarrollo Económicos OECD (2022), lo subraya con fuerza: una buena gestión de datos 'debe orientarse no solo al cumplimiento regulatorio, sino también a la generación de confianza y valor social en entornos digitales'. Si manejas datos sensibles, este punto es clave. Convierte la gestión de información, que antes era solo un gasto para cumplir la ley, en algo que

realmente da valor y credibilidad, reforzando la relación con clientes que necesitan confiar al cien por cien.

Para concluir, la recolección y el almacenamiento seguro de los datos son la base de la gestión en las plataformas de juegos online. Implementarlos correctamente no solo garantiza que se cumpla la normativa, sino que también refuerza la confianza del usuario, cuida la integridad de la empresa y permite usar la información de manera responsable, como en la lucha contra el juego problemático. Eso sí, este proceso exige una dedicación continua a la innovación tecnológica, adoptar buenas prácticas de gobernanza de datos y ser transparentes con la ética. Solo de esta manera la gestión de datos se transformará en una herramienta estratégica que beneficia tanto a la empresa como a los usuarios que confían en ella. La Agencia de Ciberseguridad de la Unión Europea ENISA (2021) enfatiza un punto clave: “la confianza digital solo puede sostenerse mediante esquemas sólidos de protección de datos y gobernanza transparente que garanticen seguridad y responsabilidad en el manejo de la información”. Esto nos dice que la tecnología por sí sola no es suficiente para que la gente confíe; tiene que estar apoyada por reglas y políticas claras que aseguren tanto la seguridad técnica (cifrado, firewalls) como la responsabilidad ética en todo el manejo de los datos del usuario.

Procesamiento y análisis de datos para la personalización de la experiencia del usuario:

El procesamiento y análisis de datos representa una de las fases más cruciales en la gestión de la información de los usuarios en el ámbito de los juegos de azar online. Esta fase permite transformar enormes cantidades de datos en conocimiento estratégico que mejora tanto la experiencia del jugador como la toma de decisiones del negocio. A diferencia de simplemente acumular y archivar, esta etapa requiere meter técnicas avanzadas como la minería de datos, la analítica predictiva y el aprendizaje automático. La meta es clara: descubrir los patrones de comportamiento, clasificar a los usuarios y crear experiencias que realmente se sientan personalizadas para cada jugador. En el entorno digital, donde abunda la información, la

capacidad de procesar y analizar los datos en tiempo real es una ventaja gran ventaja competitiva. El experto en gestión y tecnología Davenport (2018) “expreso: "el análisis de datos se ha convertido en el nuevo motor de la innovación empresarial, pues permite a las organizaciones anticiparse a las necesidades de los clientes y ofrecer soluciones adaptadas a sus expectativas, generando mayor valor y fidelidad". Esta gran habilidad para convertir grandes volúmenes de información en decisiones útiles es fundamental en el sector del juego de azar en línea, ya que no solo sirve para optimizar las operaciones y la seguridad, sino también para personalizar y mejorar la experiencia del usuario y fortalecer su compromiso a largo plazo.

El análisis de datos en las apuestas online sirve para muchísimas cosas: desde crear ofertas promocionales a la medida de cada persona hasta detectar comportamientos raros que podrían ser señal de fraude o de juego problemático. Por ejemplo, al examinar la frecuencia de apuestas, los montos promedio y los juegos preferidos, los operadores logran segmentar a los usuarios y diseñar campañas de marketing muy precisas. Al mismo tiempo, los algoritmos de recomendación, similares a los de Netflix o Amazon, permiten sugerir juegos o modalidades de apuestas que se ajustan a los gustos individuales de cada usuario, lo que incrementa su satisfacción y el tiempo que pasan en la plataforma. La investigación de Chen, Chiang, y Storey (2012), afirma que esta analítica "permite no solo mejorar la eficiencia operativa de las empresas, sino también aumentar la competitividad al transformar la información en conocimiento accionable". Un punto importante en este proceso es el uso de la analítica predictiva, esta ofrece la capacidad de adelantarse a comportamientos futuros basándose en los datos ya obtenidos. Esta cualidad predictiva es indispensable en sectores como el juego en línea, ya que el análisis de patrones históricos de apuestas y comportamiento del usuario es esencial para prevenir el fraude y personalizar la experiencia del cliente de manera proactiva. En el ámbito de los juegos de azar en línea, esta técnica es fundamental para prever

cómo gastarán los clientes, identificar a aquellos que puedan estar por marcharse, e incluso estimar el riesgo de que el juego se vuelva adictivo. Por lo tanto, las plataformas consiguen dos objetivos: mejorar sus tácticas para conservar a los clientes y aplicar medidas de prevención que se enfocan en el juego responsable. Por ejemplo, si un algoritmo detecta que un usuario apuesta mucho más y con mayor frecuencia en poco tiempo, el sistema puede emitir alertas, poner límites de forma automática o sugerir descansos, manteniendo así un equilibrio entre los intereses comerciales y la responsabilidad social.

El análisis de datos es clave para detectar y evitar el fraude. Usando técnicas de machine learning, los sistemas son capaces de identificar al momento cualquier patrón extraño en las transacciones, como si se hacen varios retiros desde lugares diferentes o si un comportamiento no coincide con lo que el usuario suele hacer. Estos mecanismos no solo salvan a las plataformas de perder dinero, sino que también consiguen que los jugadores confíen más en el servicio y ayudan a las empresas a ajustarse más rápido a cualquier cambio en la regulación. Sin embargo, el uso intensivo de análisis de datos plantea desafíos éticos y legales importantes, especialmente relacionados con la privacidad y la transparencia; aunque la personalización mejora la experiencia, también puede generar riesgos de manipulación si no se aplican criterios claros de responsabilidad y consentimiento, ya que, por ejemplo, recomendar juegos de manera excesiva a usuarios vulnerables podría incentivar adicciones y contravenir principios de protección al consumidor. Por eso, es clave adoptar modelos de ética para la inteligencia artificial que pongan reglas claras al uso de la información y busquen un balance entre ganar más dinero y proteger a los usuarios. Como señala la Comisión Europea Commission (2021) en su propuesta de Reglamento de Inteligencia Artificial (AI Act), la transparencia, la supervisión humana y la gestión de riesgos son principios fundamentales para garantizar un uso confiable y seguro de estas tecnologías. Esto implica que las empresas que usen IA para verificación o analítica deben crear mecanismos claros que permitan auditar

los sistemas, mantener el control humano en las decisiones de alto riesgo y reducir activamente los sesgos y las vulnerabilidades.

Para terminar, procesar y analizar los datos es una pieza clave en la gestión de información de los usuarios en el juego online. Con esto se logra personalizar la experiencia, hacer más eficiente el negocio y asegurar que todas las transacciones sean seguras. Mediante técnicas de big data, analítica predictiva y machine learning, las plataformas consiguen anticipar necesidades, prevenir riesgos y diseñar servicios que se ajustan a los gustos individuales de cada jugador. No obstante, esta implementación debe ir de la mano de políticas de transparencia, consentimiento informado y responsabilidad ética para evitar cualquier manipulación indebida de los usuarios De esta manera el análisis de datos, de esta manera, se transforma no solo en una herramienta tecnológica, sino en la base de la sostenibilidad y la confianza dentro del ecosistema digital de apuestas. Los expertos Mayer-Schönberger y Cukier (2013) señalan que "el verdadero valor del análisis de datos no radica únicamente en su volumen, sino en la capacidad de convertirlo en conocimiento útil y accionable que transforme la toma de decisiones". Esta visión es clave, pues en el juego online el éxito no tiene que ver con la cantidad de datos que se guarden, sino con la habilidad de procesarlos deprisa y usarlos para hacer más seguros los sistemas, personalizar la experiencia y cumplir con todas las reglas.

Protección y privacidad de datos personales:

La protección y la privacidad de los datos personales son un eje central en la gestión de la información de los usuarios en los juegos de azar online. Esto se debe a que es un sector que maneja constantemente información muy delicada: desde datos de identidad y detalles financieros hasta historiales de juego y patrones de comportamiento digital. La confianza de los usuarios en estas plataformas depende mucho de la seguridad con la que se maneja su

información, ya que cualquier fallo de seguridad podría traducirse en pérdidas económicas, robo de identidad o la exposición indebida de sus hábitos de consumo. En este punto, las normativas de otros países como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos han establecido un modelo que se puede seguir. Estos reglamentos definen estándares de privacidad digital que exigen a las organizaciones transparencia, la obtención del consentimiento informado y garantías sólidas sobre el uso de la información. Como señalan los expertos en gobernanza de datos Cate, Cullen, y Mayer-Schönberger (2014), “la privacidad no puede concebirse únicamente como un derecho individual, sino también como un valor social indispensable para la preservación de la confianza en los entornos digitales”. Esta perspectiva subraya que la solidez de cualquier ecosistema digital, incluyendo el sector de las apuestas online, depende de la certeza colectiva de que los datos son manejados con responsabilidad. Por lo tanto, asegurar la privacidad se convierte en una función social esencial para fomentar la participación y el desarrollo económico digital.

Para proteger los datos personales en el juego online, es necesario establecer normas claras de secreto, asegurarse de pedir la menor cantidad de datos posible y obtener el permiso explícito del usuario. Esto obliga a las plataformas a pedir solo la información necesaria para dar el servicio, a explicar con total claridad qué se hará con esos datos y a permitir que los usuarios decidan qué condiciones aceptan o rechazan. De la misma forma, la privacidad debe asegurarse en todo momento, desde que se recogen los datos por primera vez hasta que se almacenan, se procesan y, finalmente, se eliminan los registros. Una de las prácticas más importantes aquí es hacer anónimos o seudonimizar los datos. Esto baja el riesgo de que alguien pueda identificar directamente a los usuarios, manteniendo su privacidad a salvo incluso si hay una filtración o hackeo. De acuerdo con Cate, Cullen, y Mayer-Schönberger, (2014), esta estrategia forma parte del modelo "Privacy by Design", el cual propone que la

privacidad se piense como un principio guía desde que se diseñan los sistemas y servicios digitales, y no como algo que se añade al final.

Para proteger la privacidad, es fundamental usar tecnología de punta. Hablamos de cosas como el cifrado total (de extremo a extremo), protocolos de seguridad como SSL/TLS y la verificación con múltiples pasos (autenticación multifactor). Con estas herramientas se asegura que nadie sin permiso pueda interceptar o cambiar los datos mientras se envían o se guardan. Además, los sistemas de control de acceso y auditoría permiten vigilar quién entra a la información y por qué, lo cual reduce mucho el riesgo de que haya abusos desde dentro de las empresas. Para los juegos de azar online, donde los intentos de fraude y ciberataques son frecuentes, la combinación de estas tecnologías con una política de ciberseguridad proactiva resulta esencial para asegurar la integridad de los datos y la confianza del usuario. No obstante, la protección de la privacidad enfrenta múltiples desafíos en un entorno globalizado y altamente interconectado. El manejo de los datos transfronterizos es uno de los problemas más complejos, ya que muchas plataformas de apuestas online trabajan en distintas zonas con reglas de privacidad diferentes. Esto provoca agujeros legales y conflictos normativos que pueden reducir la protección de los usuarios si no se adoptan estándares comunes. Además, otro gran desafío es encontrar el punto medio entre la privacidad y el uso de datos con fines comerciales. Aunque la personalización de los servicios es una ventaja, puede chocar con el derecho de los usuarios a mantener el control sobre su propia información. Como indica el experto en derecho y tecnología Solove (2021), este desafío se conoce como "asimetría de información", donde las empresas tienen mucho más conocimiento sobre los usuarios que estos sobre el manejo de sus propios datos. Esto reduce la posibilidad de que el consentimiento sea verdaderamente informado. En la práctica, esta desigualdad genera un desequilibrio de poder que resta libertad al usuario. Por eso es tan necesario que haya reglas

claras y formas transparentes para que la gente entienda de verdad cómo se están usando sus datos.

En conclusión, la protección y privacidad de los datos personales en los juegos de azar en línea representan no solo una obligación legal, sino también un compromiso ético que incide directamente en la sostenibilidad del negocio digital. La adopción de políticas de privacidad transparentes, la integración de medidas de seguridad tecnológica y la implementación de modelos de privacidad proactiva como el “Privacy by Design” permiten fortalecer la confianza de los usuarios y cumplir con las exigencias regulatorias internacionales. Para cerrar, la protección y la privacidad de los datos personales en el juego online no son solo una obligación legal, sino un compromiso ético que afecta directamente la permanencia del negocio digital. Adoptar políticas de privacidad transparentes, sumar medidas de seguridad tecnológica e implementar modelos de privacidad proactiva como el "Privacy by Design", permite ganar la confianza de los usuarios y cumplir con todo lo que exigen las regulaciones internacionales. Sin embargo, este esfuerzo debe completarse con una reflexión continua sobre los nuevos desafíos, como la gestión de datos transfronterizos y la asimetría de información, problemas que exigen soluciones coordinadas a nivel global. Solo de esta forma, las plataformas lograrán ofrecer una experiencia digital que sea segura, responsable y que cumpla con los derechos básicos del usuario en el mundo digital de hoy. Como señala (Cavoukian, 2011), la privacidad debe incorporarse al diseño de los sistemas desde el inicio y no al final, lo que convierte al modelo Privacy by Design en un estándar esencial para construir la confianza digital.

La gobernanza y ética en la gestión de datos de los usuarios:

La gobernanza y ética en el manejo de los datos de los usuarios son fundamentales en el mundo de los juegos de azar online. No basta solo con recolectar, guardar y procesar la información, hay que hacerlo siguiendo principios de responsabilidad, transparencia y equidad.

Dado que los datos personales son hoy un recurso estratégico en el ámbito digital, las organizaciones se enfrentan al desafío de establecer estructuras de gobernanza sólidas. Dichas estructuras deben garantizar que cada decisión sobre cómo se usa la información cumpla con la ética y con las leyes. La gobernanza de datos, en esencia, es el conjunto de reglas, pasos y controles que definen cómo se manejan los datos en la empresa, asegurando que sean de calidad, estén seguros, siempre disponibles y se usen de forma correcta. Según el experto en derecho de la información Weber (2019), "una gobernanza eficaz de la información es fundamental para generar confianza en los usuarios y garantizar la legitimidad de las operaciones digitales en sectores altamente regulados". Esto quiere decir que las empresas que trabajan en mercados sensibles deben hacer más que solo cumplir la ley: tienen que establecer políticas internas fuertes que demuestren que los datos se manejan de forma transparente y segura. Esto es clave para que la marca se mantenga y para asegurar la lealtad del cliente.

En el juego online, la gobernanza de datos se trata de armar una estructura clara que diga quién es responsable de qué en el manejo de la información. Esto incluye crear equipos especiales de gobernanza, nombrar a los encargados de la protección de datos (Data Protection Officers) y tener manuales con el paso a paso para manejar fallas de seguridad o cuando un usuario pide ver sus datos. Para que funcione bien, la gobernanza también requiere sistemas de supervisión y auditoría que revisen constantemente que se cumplan las reglas, asegurando así que los datos no se usen mal o sin permiso. De esta forma, las plataformas no solo acatan la ley, sino que demuestran un compromiso ético con los derechos digitales de sus clientes. Las decisiones sobre cómo se usan los datos, como al personalizar ofertas, segmentar clientes o para detectar riesgos, tienen que basarse en una ética que evite manipular y que proteja a los usuarios más débiles. Los filósofos de la información Floridi y Taddeo (2016) proponen que el uso de datos personales se rija por la "infonomía responsable",

un concepto que equilibra el uso legítimo de la información con la obligación moral de proteger la autonomía y dignidad de las personas. Esto es muy importante en el juego online, donde usar mal los datos solo para ganar más dinero podría fomentar adicciones, creando un conflicto ético evidente entre el lucro de la empresa y la responsabilidad social.

La ética en la gestión de datos también exige adoptar principios de justicia algorítmica en los sistemas de análisis y predicción que usan las plataformas. Muchos de estos sistemas, que funcionan con inteligencia artificial y aprendizaje automático, pueden repetir sin querer los mismos prejuicios que existen en la sociedad. Esto puede afectar la forma en que se trata a los usuarios. Por ejemplo, un modelo creado para detectar fraudes podría terminar señalando injustamente a jugadores de ciertos países o niveles económicos si no se construye con cuidado, tomando en cuenta la diversidad y la transparencia. Para contrarrestar este riesgo, las empresas deben realizar auditorías algorítmicas, hacer pruebas de sesgo y usar procesos de explicabilidad que permitan a los usuarios entender el cómo y el porqué de las decisiones automatizadas El crecimiento acelerado de la inteligencia artificial y la automatización ha hecho que la ética de los algoritmos sea más importante que nunca. Como señalan Mittelstadt, Allo, Taddeo, Wachter, y Floridi (2016), este tema se ha convertido en uno de los desafíos de la era digital más difíciles, ya que implica garantizar que los sistemas automatizados actúen de manera responsable y transparente. En los negocios digitales, esto significa que los programas que usan para chequear identidades, evitar fraudes o hacer predicciones tienen que ser creados y vigilados con mucho cuidado y responsabilidad. El objetivo es prevenir cualquier sesgo que pueda llevar a decisiones injustas y garantizar que las determinaciones más importantes sean comprensibles y puedan explicarse claramente a los usuarios.

Para finalizar, la gobernanza y ética en el manejo de los datos de los usuarios son pilares clave para que las plataformas de juegos de azar online sean sostenibles y legítimas. Una gobernanza sólida permite crear políticas y procedimientos claros que regulen todo el ciclo de

vida de los datos. Una gestión ética, por su parte, busca que todas estas prácticas estén enfocadas en proteger los derechos de los usuarios y en promover un entorno digital más justo y responsable. Al unir ambos enfoques, aumenta la confianza de los jugadores y las empresas demuestran que actúan con honestidad, responsabilidad y transparencia. Como lo indica la Organización para la Cooperación y el Desarrollo Económicos OECD (2021), el beneficio se basa en la "capacidad de gestionarlos con ética, equidad y respeto hacia quienes los generan". Esta perspectiva convierte la responsabilidad social y la gobernanza de datos transparente en factores clave para diferenciarse, sobre todo en el sector digital, donde la confianza del usuario es esencial para el éxito a largo plazo.

3.3. Definición de términos básicos

Aumento de Seguridad uno de los procesos para confirmar la identidad de una persona utilizando la tecnología como reconocimiento facial, biometría y documentos de identidad, para evitar fraudes y robo de identidad.

Autenticación de Dos Factores Es una práctica recomendada para añadir una capa adicional de seguridad mediante dos elementos de verificación de identidad, como una contraseña y un código temporal.

Control Estadístico de Procesos técnica que permite monitorear y controlar los procesos mediante métodos estadísticos. Ayuda a identificar variaciones y verificación de usuarios en plataformas de juegos en línea.

Cumplimiento Regulatorio es esencial contar con las normas legales y regulaciones establecidas por organismos de control para evitar fraudes, lavado de dinero y proteger a los usuarios.

Herramientas Digitales aplicaciones y plataformas de tecnología que permiten realizar tareas de manera eficiente y automatizada. Estas herramientas se presentan en diferentes áreas.

Internet de las Cosas (Iot) interconexión de dispositivos a través de internet, así como interactúen entre sí o con usuarios de manera automática, y su funcionalidad depende de la capacidad del dispositivo.

KPIs indicadores de rendimiento que se usan para medir la efectividad de un proceso o sistema.

Mejora Continua estrategia que busca optimizar al realizar ajustes y mejoras constantes en los procesos para aumentar la eficiencia, la calidad y la seguridad. Evolucionando el sistema de registro y verificación frente a nuevos desafíos.

Seguridad de la Información conjunto de prácticas y políticas diseñadas para proteger la información sensible dentro de la organización, asegurando su confidencialidad, integridad y disponibilidad.

Transformación Digital proceso en el cual implica una reestructuración tecnológica que permite a las empresas ser eficientes e innovadoras. Además, tener la colaboración entre todas las áreas.

CAPÍTULO IV: HIPOTESIS Y VARIABLES

4.1. Formulación de hipótesis

4.1.1. Hipótesis general

La implementación de la tecnología de verificación de identidad mejora la gestión de datos de los usuarios en juegos de azar en línea.

4.1.2. Hipótesis específicas

La implementación de la tecnología de verificación de identidad puede mejorar las funciones de tecnologías implementadas en juegos de azar en línea.

La implementación de la tecnología de verificación de identidad puede mejorar la seguridad de información de los usuarios en juegos de azar en línea.

La implementación de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea.

4.2. Operacionalización de variables

Variable 1 Tecnología de verificación de identidad

Definición Conceptual

La tecnología de verificación de identidad son el uso de sistemas digitales como biometría, reconocimiento facial y validación documental para autenticar usuarios, prevenir fraudes y proteger datos personales en entornos digitales. Arce, A. Y Villamizar, L. (2022).

Variable 2 Gestión de datos de los usuarios

Definición Conceptual

La gestión de datos de los usuarios implica la recopilación, almacenamiento, procesamiento y protección de información personal mediante sistemas tecnológicos, asegurando integridad, confidencialidad y disponibilidad para optimizar la toma de decisiones y cumplir con normativas de privacidad Villar (2020).

Tabla 1: Matriz de operalización de variables

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN	ITEMS	INST	ESCALAS				
								1	2	3	4	5
Variable 1 Tecnología de verificación de identidad	La tecnología de verificación de identidad son el uso de sistemas digitales como biometría, reconocimiento facial y validación documental para autenticar usuarios, prevenir fraudes y proteger datos personales en entornos digitales. (Arce, A., & Villamizar, L. 2022).	Se evaluara mediante un cuestionario midiendo la efectividad del sistema, la gestión de riesgos y los efectos de mejora continua. Se recogera la percepcion de los encuestados respecto a la facilidad de uso y rapidez, proteccion de datos y precisión del sistema de verificación de identidad de los usuarios en juegos de azar en línea. Operacionalmente está conformada por 3 dimensiones	Efectividad del sistema	Frecuencia de autenticación	ORDINAL	1 3 5	CUESTIONARIO	NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE
			Gestión de riesgos	Registro de incidentes		8 9 10						
			Efectos de mejora continua	Evaluaciones realizadas		15 16 17						
Variable 2 Gestión de datos de los usuarios	La gestión de datos de los usuarios implica la recopilación, almacenamiento, procesamiento y protección de información personal mediante sistemas tecnológicos, asegurando integridad, confidencialidad y disponibilidad para optimizar la toma de decisiones y cumplir con normativas de privacidad (García & López, 2022).	Se medira con un cuestionario considerando incorporacion de tecnologías avanzadas, seguridad de la información y eficiencia operativa. Permitira identificar el nivel de adopción tecnológica, el grado de protección de datos y uso adecuado durante la verificación de identidad de los usuarios en juegos de azar en línea.	Funciones de tecnologÍas implementadas	Incorporacion de tecnologias avanzadas	ORDINAL	1 2 3	CUESTIONARIO	NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE
			Seguridad de la información	Controles de acceso aplicados		6 7 8						
			Uso de recursos del sistema	Eficiencia operativa		13 14 20						

CAPÍTULO V: METODOLOGÍA DE LA INVESTIGACIÓN

5.1. Diseño metodológico

Tipo:

La presente investigación es de tipo aplicada, debido a que se brinda una solución practica al problema encontrado, tangibilizando el resultado en acciones y/o productos que permitan mitigar dicho problema. La investigación aplicada se enfoca en la utilidad, ya que "está dirigida fundamentalmente hacia un objetivo o propósito específico práctico" OCDE (2015)

Enfoque:

La presente investigación es de un enfoque cuantitativo debido a que se busca determinar cómo la implementación de la tecnología de verificación de identidad puede mejorar la gestión de datos de los usuarios en juegos de azar en línea. Según Hernández-Sampieri y Mendoza (2018), el enfoque cuantitativo "utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y el uso de la estadística para establecer con exactitud patrones de comportamiento en una población"

Diseño:

Para la presente investigación se aplicará el diseño descriptivo porque se enfoca en observar, medir y describir las características de una población. "Los estudios descriptivos buscan 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, miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar. El énfasis se sitúa en describir, no en

explicar ni predecir." Hernández-Sampieri, Fernández-Collado, y Baptista-Lucio, Metodología de la investigación (2014)

Nivel:

La investigación se encuentra en un nivel correlacional ya que busca medir cómo la implementación de la tecnología de verificación de identidad puede mejorar la gestión de datos de los usuarios en juegos de azar en línea. "El propósito del estudio correlacional es determinar el grado de relación, asociación o dependencia entre dos o más variables que no han sido controladas o manipuladas por el investigador. Lo que se busca es establecer un vínculo entre las variables y, con base en ello, predecir el comportamiento de una conociendo el de las otras." Sabino (2007)

5.2 Población

Población:

Para el presente estudio se tomó en cuenta un universo de 51 personas. considerando a los Clientes que acceden a las plataformas en el rango de 3- 5 pm. "Población es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación." Arias (2012)

5.3 Muestra

Para la presenta investigación se aplicó el tipo de muestra censal para lo cual se empleará la misma cantidad de participantes que la población. "La muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto de casos que llamamos población. Pocas veces es posible medir a toda la población, por lo

que se elige una muestra y se espera que esta sea representativa de la población para poder generalizar los resultados." Hernández-Sampieri, Fernández-Collado, y Baptista-Lucio (2014)

5.4 Técnica e instrumentos de recolección de datos

Para la presente investigación se decidió usar como recolección de datos la técnica de encuesta y como herramienta un cuestionario estructurado ya que es el indicado para un enfoque cuantitativo seleccionado. La primera variable será medida por 9 preguntas, y la segunda variable por otras 9 preguntas, 16 en escala Likert y dos en opciones múltiples.

La técnica mencionada fue usada en 51 personas.

5.5 Técnica de procesamiento de la información

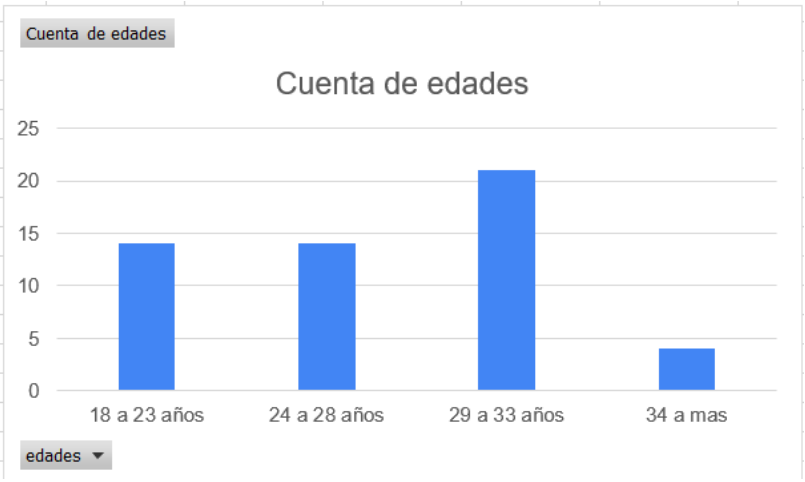
El cuestionario fue hecho en Google forms, debido a su sencillez y facilidad de usar, así pudiendo distribuirla entre los participantes de manera simple, siempre y cuando tengan una cuenta de Google y acceso a internet.

Después de realizar las encuestas mediante Google forms Se procedió a la transferencia de los datos a la plataforma de hoja de cálculo Excel. En este entorno, fueron aplicadas diversas fórmulas con el objetivo de obtener los porcentajes correspondientes a la distribución de los datos.

Una vez calculados dichos valores, se elaboraron las tablas pertinentes, cuya función es organizar la información para su posterior aplicación en los análisis estadísticos. Con ello, se posibilita la realización de las interpretaciones y conclusiones requeridas.

5.5.1. Análisis descriptivo

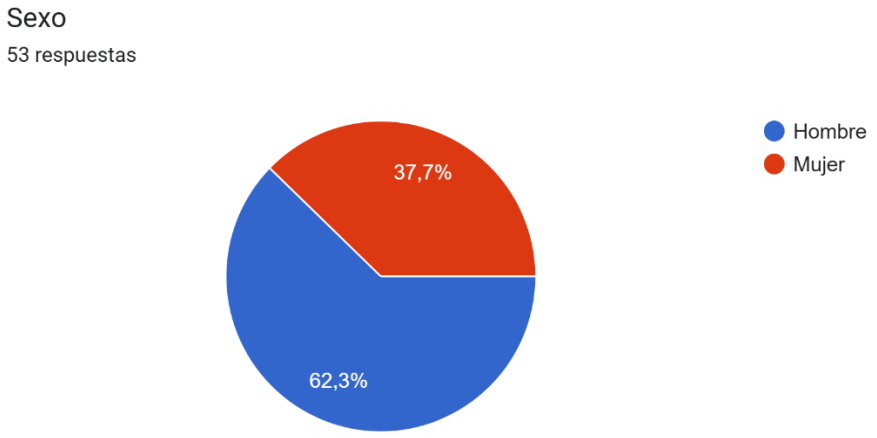
Gráfico 1: El rango de edad de los participantes



Nota: elaboración propia

El rango de edad nos indica que es más común el uso de estos aplicativos en usuarios de entre 29 a 33 años, cabe resaltar que para la presente encuesta no se le permitieron participar a los menores de edad.

Gráfico 2: El sexo de los participantes



Nota: elaboración propia

En el grafico se muestra que la mayoría de encuestados son hombres, lo cual demuestra que la mayoría de usuarios de esta aplicación son varones.

Tabla 2:

Efectividad del sistema de verificación en el inicio de sesión en diferentes dispositivos

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nunca	1	2%	2%	2%
Rara vez	3	6%	6%	8%
A veces	4	8%	8%	16%
Frecuentemente	39	76%	76%	92%
Siempre	4	8%	8%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados muestran que el sistema de verificación de identidad desde múltiples dispositivos suele operar de una manera óptima y efectiva. El dato muestra de que para un 8% la verificación funciona “siempre”, mientras que para un 76% la verificación funciona

"frecuentemente", mientras que para un 8% solo "a veces", por último, solo para el 2% nunca nos indica que el sistema de verificación estándar está bien implementado.

Esta frecuencia alta de solicitud de verificación nos indica una fortaleza en la seguridad en la plataforma, lo cual garantiza una seguridad para los datos los usuarios evitando el ingreso desde dispositivos no autorizados.

La propuesta de implementación debe centrarse en indagar y corregir la pequeña parte que indico que nunca se solicitan estas verificaciones.

Tabla 3:

Autenticación para ingresar o realizar transacciones

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nunca	0	0%	0%	0%
Rara vez	1	2%	2%	2%
A veces	12	24%	24%	25%
Frecuentemente	31	61%	61%	86%
Siempre	7	14%	14%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados demuestran que, el sistema pide autentificaciones "frecuentemente" como lo expreso el 61% y "siempre" como marco el 14%, por lo cual se muestra que a pesar de que el sistema ya implementado es percibido por la gran mayoría de encuestados como adecuado hay una gran parte también que experimenta poca frecuencia en la autentificación de la aplicación para estas transacciones.

El punto clave a indagar es porque ese 24% marco "a veces" ya que esto puede deberse a una falta de consistencia en el proceso antes mencionado, ya que la aplicación puede no estar aplicado la verificación en todos los usuarios por igual, o a una mala comunicación en la política de este apartado ya que los usuarios pueden no entender cuando es necesaria una verificación y cuando no, y esto puede llevar a una percepción de aleatoriedad.

El punto de mejora empieza por investigar los casos de ese 24% para mejorar la experiencia y satisfacción de usuario.

Tabla 4:

Autenticación según el tipo de operación o nivel de riesgo

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	2	4%	4%	4%
Ni de acuerdo ni en desacuerdo	17	33%	33%	37%
De acuerdo	27	53%	53%	90%
Totalmente de acuerdo	5	10%	10%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados nos indican que existe una aceptación muy positiva, estando “totalmente de acuerdo” un 10% y “de acuerdo” un 53% hacia la adopción de una autentificación dinámica o por niveles de riesgo.

El gran apoyo que recibió esta medida ayuda a la justificación en invertir más en tecnologías de verificación de ayuden en puntos críticos de autentificación y también ayuden a la satisfacción y seguridad del usuario.

El 33% que marco “ni de acuerdo ni en desacuerdo” se puede deber a que no comprenden bien cómo funcionan estas tecnologías adaptativas, pero pueden cambiar de opinión explicándoles de manera concreta los beneficios que estas les pueden ofrecer.

El punto de mejora está en que los usuarios desean un sistema de verificación que priorice la protección de sus datos y su dinero, lo cual se alinea perfectamente con nuestra propuesta para así mejorar el proceso de conocer a tu cliente y mitigar el fraude.

Tabla 5:

Registro de intentos fallidos o sospechosos

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	1	2%	2%	2%
Ni de acuerdo ni en desacuerdo	14	27%	27%	29%
De acuerdo	23	45%	45%	74%
Totalmente de acuerdo	13	25%	25%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados muestran que el sistema actual si registra las actividades sospechosas detectadas, estando un 45% “de acuerdo” y un 25% “totalmente de acuerdo”, lo cual es algo positivo del sistema de verificación actual, pero también impone una gran expectativa.

EL 27% que opto por “ni de acuerdo ni en desacuerdo” se puede deber a que no han podido registrar los fallos por su cuenta o de plano no sepan que es un registro fallido o sospechoso, lo cual se puede mejorar con una explicación sobre este concepto al usuario final.

La implementación de una nueva tecnología de verificación se debe integrar directamente con la función de registro y esta debe asegurarse de: mejorar el registro en el aplicativo creando una auditoria de todos los intentos erróneos de ingreso, y también bloquear momentáneamente a los usuarios con múltiples intentos erróneos de ingreso.

El punto de mejor aquí es claro, desarrollar un sistema de verificación que ayude al sistema de ingreso ya establecido y afiance la seguridad y satisfacción de los usuarios.

Tabla 6:

Gestión de riesgos de acceso no autorizado

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nunca	0	0%	0%	0%
Rara vez	2	4%	4%	4%
A veces	17	33%	33%	37%
Frecuentemente	26	51%	51%	88%
Siempre	6	12%	12%	100%
Total	51	100%	100%	

Nota: elaboración propia

En los datos se muestran que el 51% de los encuestados consideran que “frecuentemente” el sistema actual puede gestionar los riesgos de acceso no autorizados, sumado al 12% que considera que lo logra hacer “siempre”, lo cual nos indica una que el sistema actual cumple con la gestión de los riesgos la mayor parte del tiempo.

Lo verdaderamente preocupante viene en el 33% que considera que se gestiona de manera correcta “a veces” o peor aún el 4% que indica que “rara vez”, estos juntos suman un 37% (casi 4 de cada 10 encuestados) los cuales no tienen plena confianza en el sistema actual, esto es una peligro reputacional y financiero alto ya que se comprometen los datos sensibles de los usuarios.

La implementación de una tecnología de verificación de identidad es la solución directa esta desconfianza ya que ayuda directamente a la primera línea de defensa contra el acceso no autorizado.

Tabla 7:

Implementación de alertas automáticas

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
SMS	11	22%	22%	22%
Llamada	3	6%	6%	27%
Correo electrónico	37	73%	73%	100%
Ninguna	0	0%	0%	100%
Total	51	100%	100%	

Nota: elaboración propia

En los datos se muestran que el canal predilecto de los usuarios para recibir alertas de seguridad, para ser más específicos, intentos fallidos de ingreso a su cuenta es el correo electrónico. Esta función es muy importante en la verificación de identidad ya que permite identificar los intentos de fraude antes de que se consumen.

Un 73% de encuestados, siendo la gran mayoría, voto por el correo electrónico como su medio preferido esto se puede dar debido a que el correo electrónico es muy útil al poder almacenar datos detallados como la IP, lugar, hora o el dispositivo que quiere tener acceso a nuestra cuenta.

Es también interesante notar que el 22% opto por el SMS esto debido a su facilidad de uso y accesibilidad sin internet, pero carece de almacenamiento de datos como el correo electrónico, esto método puede resultar útil pero lo recomendable es usarlo como un método secundario.

Estos resultados muestran que la tecnología de verificación propuesta debe tener como canal principal de alerta al usuario el correo electrónico.

Tabla 8:

Actualizaciones o mejoras recientes

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	5	10%	10%	10%
Ni de acuerdo ni en desacuerdo	20	39%	39%	49%
De acuerdo	21	41%	41%	90%
Totalmente de acuerdo	5	10%	10%	100%
Total	51	100%	100%	

Nota: elaboración propia

En los datos se muestran que poco más de la mitad de los encuestados estuvieron conformes, siendo un 41% “de acuerdo” y un 10% “totalmente de acuerdo”, esto nos indica que la plataforma ha hecho mejoras en su sistema de seguridad la cual ha sido percibido por gran parte de sus usuarios.

Lo preocupante viene en el 39% que dijo no estar “ni de acuerdo ni en desacuerdo”, bajo el contexto desarrollado esto nos hace ver que una gran parte no nota mejoras en la inversión de su seguridad.

El 10% que está en “desacuerdo” nos hace ver que así sea una pequeña porción de participantes estos sienten que el sistema de verificación actual este detenido y no presenta mejoras.

La propuesta de mejora mediante la implementación de la tecnología de verificación de identidad se justifica porque no será un pequeño cambio si no que será una gran mejora en seguridad que hará que los que se mejore la satisfacción de los usuarios que se encuentran indiferentes en este aspecto.

Tabla 9:

Mejoras en la precisión y facilidad

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nunca	0	0%	0%	0%
Rara vez	7	14%	14%	14%
A veces	19	37%	37%	51%
Frecuentemente	24	47%	47%	98%
Siempre	1	2%	2%	100%
Total	51	100%	100%	

Nota: elaboración propia

En los datos se muestran que hay una percepción positiva de la mejora, entre el 47% que ha respondido “frecuentemente” y 2% “siempre”, por lo cual se muestra que casi la mitad de los usuarios notan una inversión y mejora constante en la tecnología actual que gestiona su identidad.

Lo resaltante viene en el punto de los que votaron por “a veces” lo cual muestra que muchas veces la tecnología actual puede ser lenta y otras veces confusa o hasta imprecisa, esta inconsistencia puede ser perjudicial ya que puede llevar a la frustración o al abandono del proceso de registro.

Por último, el grupo que voto por “rara vez” (14%) nos indica que un grupo significativo nota que no ha habido mejora en la precisión y fiabilidad de la tecnología actual.

El desequilibrio entre estos dos puntos (precisión y facilidad de uso) muestra que la propuesta de la tecnología de verificación que se está haciendo debe enfocarse en dos puntos claves: el primero, asegurar la precisión ósea evitar los falsos errores, y segundo garantiza la facilidad de su uso para los usuarios equilibrando así la seguridad de los datos con una experiencia de usuario simple y fluida.

Tabla 10:

Necesidad de realizar evaluaciones continuas

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	5	10%	10%	10%
Ni de acuerdo ni en desacuerdo	11	22%	22%	31%
De acuerdo	31	61%	61%	92%
Totalmente de acuerdo	4	8%	8%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados muestran que la gran mayoría está a favor de una evolución en este aspecto, estando un 61% “de acuerdo” y un 8% “totalmente de acuerdo” esta gran mayoría desea que la plataforma no se quede como esta si no que se continue invirtiendo en una seguridad que proteja sus datos personales y bancarios.

El segmento del 22% que no está “ni acuerdo ni es desacuerdo” puede no estar familiarizado con los softwares de seguridad o con la verdadera amenaza que representa no aplicar mejoras continuas en la seguridad de los datos, lo que también nos sugiere que puedan cambiar a una opinión positiva explicándole estos puntos clave y sus beneficios.

La gran aprobación a una mejora es calve para poder justificar la propuesta de implementación de verificación de identidad no solo como una nueva tecnología si no también como una estrategia de mejora continua.

Tabla 11:

Nuevas tecnologías de verificación disponibles

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Reconocimiento facial	22	43%	43%	43%
Biometría	6	12%	12%	55%
Autenticación en dos pasos	17	33%	33%	88%
Encriptación	5	10%	10%	98%
Ninguna	1	2%	2%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los resultados muestran un claro dominio del reconocimiento facial siendo la más votada con 43%, luego se nota que la autentificación por dos pasos obtuvo un 33% de elección lo que nos demuestra que los usuarios ya están familiarizados con esta tecnología que nos permite mitigar los fallos de seguridad, y también su alta visibilidad ayuda a los usuarios a sentirse protegidos.

El 12% que opto por biometría nos da a entender que la gran mayoría tienen el conocimiento de que existen métodos de verificación avanzados que se basan en características biológicas, esto nos hace ver que esta tecnología no es desconocida y que su implementación es notada y deseada junto con el reconocimiento facial.

La propuesta de implementación de tecnología de verificación de identidad debe centrarse en la alta familiaridad con el reconocimiento facial y la autentificación en dos pasos, esto debido a que el reconocimiento facial es el más simple y entendido por el usuario lo cual facilitaría su adopción por parte de este; la estrategia de seguridad planteada debe contar con la biometría y la autentificación en dos pasos, creando así una tecnología de verificación robusta y segura.

Tabla 12:

Utilidad de las tecnologías implementadas

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nada útil	0	0%	0%	0%
Poco útil	4	8%	8%	8%
Moderadamente útil	15	30%	30%	38%
Bastante útil	30	60%	60%	98%
Muy útil	1	2%	2%	100%
Total	50	100%	100%	

Nota: elaboración propia

Como notamos una gran mayoría lo consideran útil, entre el 60% que lo ve “bastante útil” y el 2% que lo ve “muy útil” lo que demuestra que la mayoría percibe como útiles las medidas de

seguridad ya establecidas, esto nos hace ver que los usuarios comprenden la importancia de la seguridad para proteger sus datos personales.

Una 30% siendo una parte muy significativa lo considera “moderadamente útil” lo que nos puede indicar que el proceso es útil pero lento o inconsistente lo que puede causar cierta insatisfacción del usuario.

El punto de mejora no pasa por cambiar las tecnologías actuales si no en mejorar la eficiencia y la satisfacción actualmente percibida, por ello debemos enfocarnos en: aumentar la eficiencia, la tecnología de verificación aplicada debe ser simple y reducir el tiempo de espera; y mejorar la gestión de datos hacia un proceso más rápido y más sencillo.

Tabla 13:

Necesidad de ampliar o mejorar las funciones tecnológicas

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	1	2%	2%	2%
En desacuerdo	1	2%	2%	4%
Ni de acuerdo ni en desacuerdo	11	22%	22%	25%
De acuerdo	23	45%	45%	71%
Totalmente de acuerdo	15	29%	29%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos muestran que la gran mayoría demanda una mejora el 45% “de acuerdo” y el 29% totalmente de acuerdo, lo cual muestra que es necesario mejorar o ampliar las funciones del sistema de seguridad actual, el hecho de que específicamente 29% hayan escogido “totalmente de acuerdo” nos hace ver que una significativa parte de los usuarios nota las limitaciones del sistema actual y ve de carácter urgente corregirlas.

El 22% que marcaron “ni de acuerdo ni en desacuerdo” nos indica que un grupo puede no experimentar fallas, pero tampoco ven una mejora en el sistema actual.

El gran apoyo a mejorar este sistema es el respaldo y la viabilidad de la propuesta de una tecnología de verificación de identidad, ya que la mayoría de usuarios está de acuerdo en que se invierta en una solución avanzada.

Tabla 14:

Mecanismos utilizados para la autenticación

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Contraseña	3	6%	6%	6%
Código SMS	21	41%	41%	47%
Biometría	10	20%	20%	67%
Doble factor	15	29%	29%	96%
Ninguno	2	4%	4%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos muestran en primer lugar una idea en común de preferir medidas avanzadas de autentificación, aunque actualmente el medio preferido con el 41% es el código SMS debido a su inmediatez, el 29% prefiere el doble factor (lo cual puede indicar que los usuarios ya estén familiarizados con los controles doble factor incluido el código SMS y aunque la biometría es la tercera más preferida con el 20% esto es bueno ya que nos indica que hay una buena base para poder implementar tecnologías más avanzadas de verificación de identidad.

Los resultados nos indican que la medida de verificación debe ser doble factor, con la biometría siendo el factor más fuerte pudiendo reservarse solo para los procesos más sensibles y el código SMS o doble factor para tareas más simples.

Tabla 15:

Nivel de seguridad percibida con los sistemas de verificación

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nada seguro	0	0%	0%	0%
Poco seguro	0	0%	0%	0%
Neutral / Ni seguro ni inseguro	18	35%	35%	35%
Bastante seguro	30	59%	59%	94%
Muy seguro	3	6%	6%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos muestran que la gran mayoría se siente seguro con los controles actuales siendo 59% “bastante seguro” y 6% “muy seguro”, esto nos indica que implementar una tecnología de verificación avanzada no generaría desconfianza si no que llega sobre una base sólida ya establecida.

El otro dato a resaltar es que el 35% se mostró neutral, este grupo es vulnerable a la pérdida de confianza en la plataforma, estos usuarios no están convencidos de que sus datos estén del todo seguros. La ausencia de respuestas negativas es buena, pero hay un gran margen de mejora.

La propuesta de implementación de tecnología de verificación de identidad debe ser creada para cambiar esa neutralidad por una convicción positiva reduciendo el riesgo percibido y fortaleciendo la confianza en operaciones críticas.

Tabla 16:

Opinión sobre el reforzamiento de los controles de seguridad

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	0	0%	0%	0%
Ni de acuerdo ni en desacuerdo	10	20%	20%	20%
De acuerdo	30	59%	59%	78%
Totalmente de acuerdo	11	22%	22%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos muestran que una abrumadora mayoría está de acuerdo, estando 59% “de acuerdo” y 22% “totalmente de acuerdo”, este alto nivel de encuestados de acuerdo nos hace ver la necesidad de reforzar los sistemas actuales con un proceso robusto de verificación de identidad.

El 20% que expreso “ni de acuerdo ni en desacuerdo” nos hace ver que hay una capacidad de mejora, puede que este grupo no esté en contra, si no que carece del entendimiento de los refuerzos propuestos, por lo cual la estrategia de implementación efectiva y clara de cómo estos refuerzos los protegen de futuros problemas como fraudes o robo de identidad.

Los resultados no son solamente positivos, sino que también nos proporciona un fundamento solido para la propuesta de implementación de identidad, haciendo que se minimice el riesgo de rechazo del usuario y mejora el aumento de confianza y cumplimiento normativo.

Tabla 17:

Efectividad del sistema de verificación

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nunca	0	0%	0%	0%
Rara vez	2	4%	4%	4%
A veces	7	14%	14%	18%
Frecuentemente	35	69%	69%	86%
Siempre	7	14%	14%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos nos indican un nivel alto de satisfacción, marcando el 69% “frecuentemente” lo cual nos deja ver que la mayoría de usuarios perciben una efectividad frecuente, mientras que un 14% voto “siempre” lo cual nos deja ver la seguridad de la plataforma como eficiente y confiable, este es un buen indicador de satisfacción de usuario.

Un total de 18% de usuarios notan interrupciones y lentitud con cierta regularidad, aunque es una minoría es importante que el sistema funcione siempre de manera óptima ya que en este ámbito de apuesta en líneas un fallo puede llevar a un descontento del usuario y aun cambio de plataforma.

La propuesta debe basarse en mejorar la estabilidad y la mejora continua.

Tabla 18:

Eficiencia del sistema en tiempos de respuesta, estabilidad y velocidad de funcionamiento

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Nada eficiente	0	0%	0%	0%
Poco eficiente	3	6%	6%	6%
Moderadamente eficiente	11	22%	22%	27%
Bastante eficiente	34	67%	67%	94%
Totalmente eficiente	3	6%	6%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos reflejan que el sistema de verificación actual es eficiente, notándola un 67% “bastante eficiente” y un 6% “totalmente eficiente” esto sugiere que, generalmente, el sistema de verificación actual no genera una frustración y es capaz de procesar las verificaciones en un tiempo razonable y estable.

Se puede observar también que un 22% lo noto como “moderadamente eficiente”, aunque este grupo no está insatisfecho siente el proceso como mejorable, esto debido a que pueden sufrir de errores no deseados o más pasos de los deseados. Este punto es importante para proponer una tecnología de verificación de identidad avanzada, que haga un proceso de verificación más rápido y estable.

Basándonos en este punto el sistema de verificación debe los procesos poco eficientes y convertirlos en procesos rápidos y estables para una experiencia óptima para el usuario.

Tabla 19:

Optimización del sistema para la mejora del rendimiento y la experiencia del usuario

Categoría	Frecuencia	Porcentaje (%)	Porcentaje válido (%)	Porcentaje acumulado (%)
Totalmente en desacuerdo	0	0%	0%	0%
En desacuerdo	0	0%	0%	0%
Ni de acuerdo ni en desacuerdo	13	25%	25%	25%
De acuerdo	28	55%	55%	80%
Totalmente de acuerdo	10	20%	20%	100%
Total	51	100%	100%	

Nota: elaboración propia

Los datos muestran que la gran mayoría está de acuerdo en la propuesta de optimización, estando un 55% “de acuerdo” y un 20% “totalmente de acuerdo”, este nivel de apoyo valida cualquier iniciativa de inversión en una tecnología de verificación la cual mejorara el rendimiento y la experiencia del usuario.

Ahora bien, un 25% se mantiene en posición neutral, este grupo no se opone la optimización, pero tampoco muestra un gran entusiasmo por ella, esto puede deberse a que consideran los sistemas actuales suficiente, pero con una correcta estrategia de comunicación pueden comprender lo importante que es esta optimización para ellos y como mejorara directamente su experiencia, reduciendo tiempos y espera y mejorando la seguridad de sus datos.

Con estos resultados muestra que la implementación de una tecnología de verificación de identidad es viable ya que los usuarios están deseosos y listos para una nueva solución que mejore su experiencia y su seguridad al usar la plataforma.

5.5.2. Análisis ligados a las hipótesis

Hipótesis principal

La implementación de la tecnología de verificación de identidad mejora la gestión de datos de los usuarios en juegos de azar en línea.

El análisis de los resultados confirma la hipótesis de que una implementación de una tecnología de verificación en juegos de azar en línea mejora la gestión de los datos de los usuarios. Esto lo podemos notar al ver que la mayoría de encuestados ha notado mejoras o actualizaciones últimamente en el sistema de verificación, con un 41% “de acuerdo” y un 10% “totalmente de acuerdo”. De igual manera el nivel de satisfacción del usuario con la seguridad del sistema es alto ya que el 59% se siente “bastante seguro” y el 6% “muy seguro” con los controles implementados para cuidar sus datos. La relación entre la sensación positiva de los usuarios con las actualizaciones constantes y la alta sensación de seguridad nos deja ver que las mejoras implementadas en la tecnología de verificación de identidad contribuyen a una efectiva y mejor gestión de los datos de los usuarios.

Hipótesis específica 1:

La implementación de la tecnología de verificación de identidad puede mejorar las funciones de tecnologías implementadas en juegos de azar en línea

El análisis de los resultados analizados logra confirmar la hipótesis de que la implementación de la tecnología de verificación de identidad consigue mejorar las funciones de tecnologías

implementadas en juegos de azar en línea. Esto lo podemos comprender del hecho de que la mayoría de usuarios encuestados han logrado percibir las mejoras con un 41% “de acuerdo” y un 10% “totalmente de acuerdo”.

Estos datos se pueden complementar con una alta sensación de utilidad del sistema de las funciones del sistema actual donde el 60% lo considera “bastante útil” y 2% “bastante útil”. La relación entre la sensación de mejora en la verificación y la alta utilidad de las tecnologías implementadas nos deja ver que la implementación de esta tecnología no solo cumple su trabajo principal, si no que contribuye a una mejora general del sistema tecnológico lo cual nos da como resultado una mejor experiencia del usuario.

Hipótesis especifica 2:

La implementación de la tecnología de verificación de identidad puede mejorar la seguridad de información de los usuarios en juegos de azar en línea

El análisis de los resultados hallados muestra que la hipótesis de que la implementación de la tecnología de verificación de identidad puede mejorar la seguridad de información de los usuarios en juegos de azar en línea queda justificada debido a que si bien los usuarios encuestados han notado mejoras en el sistema de verificación actual, estando el 41% “de acuerdo” y un 10% “totalmente de acuerdo” evidenciando un esfuerzo por mejorar la verificación actual, el dato crucial es que el 59% de los usuarios están “de acuerdo” y 22% “totalmente de acuerdo” con la necesidad de reforzar los controles para poder proteger de mejor manera su información. Estos resultados se muestran de que, aunque las mejoras implementadas actualmente son buenas lamentablemente son insuficientes para satisfacer del todo al usuario. Por lo cual la implementación de una tecnología de verificación de identidad

avanzada es necesaria para la mejora efectiva de la gestión de usuarios, logrando así una satisfacción del usuario más avanzada.

Hipótesis especifica 3:

La implementación de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea

El análisis de esta hipótesis se muestra que, si bien la tecnología de verificación ha experimentado avances estando el 41% “de acuerdo” y un 10% “totalmente de acuerdo”, estas mejoras de por si no han logrado terminar de satisfacer la necesidad el usuario de una optimización y uso eficiente de los recursos del sistema. El resultado clave es que una gran mayoría de usuarios 55% de acuerdo y 20% totalmente de acuerdo en que se debe optimizar el sistema para lograr mejorar el rendimiento y así mejorar la experiencia de usuario. Esta alta demanda muestra que las actualizaciones anteriores no han logrado subsanar por completo los desafíos de mejora en el sistema.

CAPÍTULO VI: PROPUESTA DE INNOVACIÓN

6.1. Alcance esperado

Esta propuesta aquí planteada está diseñada para generar un impacto positivo en tres puntos del ecosistema de juegos de azar en línea. El alcance esperado beneficiará directamente a los operadores de juegos en línea, al lograr optimizar la gestión de datos de los usuarios se logrará reducir el fraude y lograr el cumplimiento de las leyes de protección de datos, logrando así fortalecer su utilidad operativa y mejorando también su reputación. En segundo lugar, se logrará que los usuarios se beneficien de una experiencia más fluida y segura, protegiendo sus cuentas de intentos falsos de inicio de sesión. Por ultimo los entes reguladores se verán favorecidos al tener un mercado más fácil de auditar, facilitando la detección y previniendo las actividades ilícitas logrando así una correcta aplicación de las políticas de juego responsable.

6.2. Descripción del mercado objetivo del producto o servicio

La propuesta se centra en implementar una verificación de identidad digital, esta será implementada directamente en el registro de las plataformas de juegos de azar en línea. Esta tecnología se basa en inteligencia artificial (IA) y biometría facial, lo cual permite lograr una comprobación instantánea y automatizada del usuario. Este proceso se realiza mediante la captura del DNI mediante la cámara del dispositivo y una selfie, para así garantizar que la persona es realmente quien dice ser y está presente. Esto crea un registro de datos de alta fidelidad, eliminando la suplantación y evitando el acceso de menores de edad, cambiando así una gestión de datos manual y vulnerable a una eficiente, veloz y más segura.

6.2.1. Fuentes de ingreso

Las fuentes de ingreso son tres distintas: primero, nos pagarán una tarifa por la Licencia y Propiedad Intelectual por el diseño de verificación detallado; segundo, se cobrara una comisión

por ser los gestores expertos que organizan la implementación completa del sistema, desde seleccionar y negociar con el proveedor tecnológico hasta supervisar la instalación; y por último, se tendrá una fuente de ingresos continua a través de las tarifas de Mantenimiento y Auditoría, ofreciendo un servicio post-implementación clave para vigilar el rendimiento del sistema, asegurar el cumplimiento legal y hacer ajustes estratégicos.

6.2.2. Canales de distribución

La distribución de esta propuesta de implementación se centrará en B2B (Business-to-Business) que es un modelo de negocio en el que las transacciones, como la venta de productos o servicios, se realizan entre empresas, no directamente con el consumidor final, este será dirigido directamente a los operadores de las plataformas de juegos de azar en línea. El canal principal será la venta directa de consultoría, la cual se basa en contactarse con la alta dirección de estas empresas y los departamentos de compliance, a través de reuniones y presentaciones ejecutivas, en donde se destacará la importancia de la mitigación de riesgos y el cumplimiento normativo. Por último, el marketing de contenidos especializados funcionara como un generador de oportunidades, compartiendo logros y ventajas.

6.2.3. Estrategias de penetración en el mercado

La estrategia se basará en demostrar un retorno de la inversión (ROI) rápido y apreciable para los encargados de estas plataformas, superando así la resistencia al cambio tecnológico y los costos de cumplimiento. Se empezará con una estrategia de prueba de concepto y descuento inicial, la cual se basará en la implementación de un sistema piloto (esta se puede hacer implementado el sistema solo en área específica como el registro de nuevos usuarios) a una tarifa más pequeña o de forma gratuita, de esta manera se lograrán medir los resultados con métricas clave como la reducción de del fraude y la mejora de la satisfacción de los usuarios.

6.2.4. Alianzas estratégicas

Para que esta propuesta sea un éxito total a nivel técnico y legal, primero se necesita un socio clave, una alianza con una empresa local de desarrollo de software que tenga experiencia en seguridad de datos. Este socio será nuestro pilar técnico, la pieza fundamental que garantizará que nuestra tecnología de verificación se instale sin problemas y de forma totalmente segura dentro de los sistemas que el cliente ya tiene. En segundo lugar, es importante aliarse con firmas de abogados y con empresas de consultoría de compliance regulatorio especializados en la gestión de datos personales. Esta alianza funcionara como canales de distribución indirecta y validadores de la propuesta, siendo vitales para poder garantizar el cumplimiento legal.

6.2.5. Benchmarking

La propuesta planteada es mucho más rápida y eficiente que los métodos de verificación actuales, que son lentos porque tienen la necesidad de ingresar datos a mano o, peor aún, requieren la revisión humana de los documentos cargados. La gran diferencia con la propuesta planteada es que mientras los sistemas viejos son manuales o semiautomáticos, nuestra solución es de nueva generación y usa Inteligencia Artificial y biometría facial en tiempo real para verificar la identidad en un instante. La innovación está en la velocidad y la precisión que esta tecnología ofrece: se reduce el tiempo de verificación a segundos, con una tasa de detección de documentos falsos y suplantación de identidad muy superior a la ya implementada. La propuesta va mucho más allá de ser solo una herramienta para cumplir con la ley. De hecho, es un factor clave para que los clientes estén más contentos, ya que hace el proceso más rápido y fluido.

6.3. Desarrollo del proyecto de innovación

6.3.1. Etapa 1

Etapa 1: Fase de conceptualización y diseño (desarrollo del modelo)

Esta primera fase se basara en la investigación aplicada y el diseño del software central de verificación de identidad.

- Investigación y generación de datos: En este punto se definiran que datos la IA debe extraer del documento, esto inluye generar una base de datos con los recursos necesarios para entrenar al modelo de IA logrado asi que logre identificar que documento es verdadero y cual es falso.
- Diseño de arquitectura y algoritmos: Aquí se diseñara la arquitectura modular del proyecto. Esto implica el desarrollo de los algoritmos necesarios para lograr el reconocimiento óptico de caracteres para lograr asi una extraccion precisa de los datos del DNI y la creacion de los modelos para la deteccion de vida (mediante una selfie) basados en biometria facial para asi combatir falsos intentos de registro e intentos mal intensionados de inicio de sesion.
- Prototipado del flujo de UX/UI: En este punto de diseñaran un flujo de usuario mas rapido y simple para la captura de los documentos y las selfies via dispositivos moviles o web, logrando asi una mayor seguridad y gestión de los datos.

6.3.2. Etapa 2

Etapa 2: Fase de construcción del modulo y entrenamiento del sistema

Esta segunda fase se basa en el desarrollo y validación técnica del software de verificación.

- Desarrollo del módulo core: En este punto se construira el software y las API RESTful que lograran que los operadores de las plataformas de juegos de azar en línea se puedan

conectar con su sistema. El punto principal se basa en fortalecer la extracción y manejo de datos, y asi mejorar la velocidad de repsuesta.

- Entrenamiento del modelo de la IA: Para este entrenamiento se utilizara la base de datos creada para entrenar, poner a prueba y mejorar el modelo de IA y ML (machine learning) para lograr detectar la de fraude en los documentos y la presicion de la prueba de vida (selfie), Se debe lograr un umbral minimo de error, lo suficiente para que sea aceptable en el sector.
- Verificación del cumplimiento normativo: En este punto se realizara una auditoria interna del sistema para verificar que cada paso realizado hasta ese momento cumpla con los requisitos legales de el mercado objetivo.

6.3.3. Etapa 3

Etapa 3: fase de integración piloto y optimización (validación de negocio)

Una vez el sistema este construido se pasara a la integración real y la validación en un entorno controlado.

- Selección e integración piloto: Para este punto se seleccionara un operador de juegos de azar de bajo riesgo para poder lograr una prueba piloto supervisada. Aquí se integraran las APIS para lograr la verificación mas rapido y eficaz, logrando asi tambien que el cliente tenga acceso a ella.
- Pruebas de aceptación del usuario: Aquí se recolectaran los datos obentidos de las pruebas piloto, siendo estos ya datos reales nos serviran para medir el rendimiento del sistema, estos datos incluiran la tasa de finalización del proceso, tiempo de verificación, y por ultimo el impacto de la tasa de fraude en la prueba piloto.
- Optimización y escalabilidad: Se utilizaran los datos de la prueba piloto para mejorar los algoritmos ya creados, ajustar los umbrales de riesgo y mejorar la expriencia del usuario. Luego hay que preparar la arquitectura para una escalabilidad mucho mayor (capacidad para

procesar miles de verificaciones por hora) y tambien crear backups de los datos constantemente.

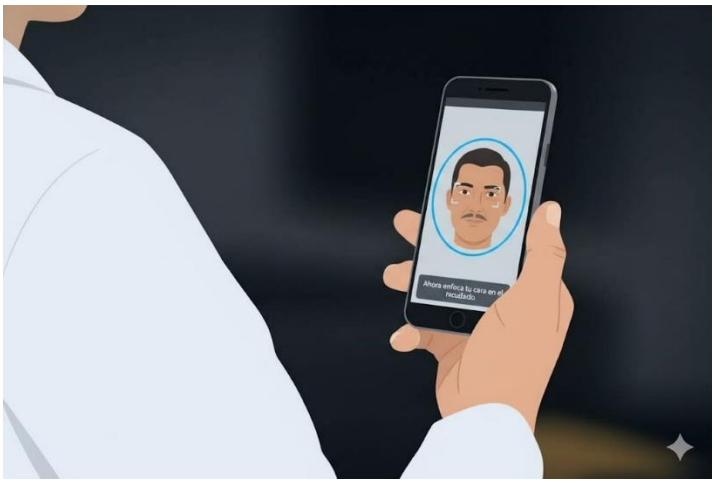
6.3.4. Etapa 4

Etapa 4: Fase de despliegue comercial y monitoreo continuo

La cuarta y última fase se enfoca en lanzamiento de la tecnología y lograr la sostenibilidad a largo plazo.

- Despliegue general y certificación: En este punto se implementara la tecnologia en los sistemas de los primeros clientes comerciales y se buscara una certificación de un tercero (firma legal especializada en compliance y laboratorio de pruebas biometricas) que valide la seguridad y precision de la tecnologia de verificación implementada.

Ilustración 1: Tecnología de verificación



Nota: imagen generada con IA

- Capacitación e implementación: Se proporcionara capacitación detallada al personal de cumplimiento de los clientes para que ellos puedan gestionar las revisiones manuales

secundarias (cuando el sistema detecte un fallo grave). Tambien se debe entregar documentación tecnica completa de las APIS.

- Monitoreo post-implementación y evolución: Se establecera un servicio continuo de monitoreo continuo, esto incluira la vigilancia y actualización constante de nuevas practicas de fraude que puedan surgir. Por ultimo se planificara la evolución del software para adaptarse a los cambios en regulaciones legales y a las nuevas formas de documentos de identificación que puedan surgir.

6.4. Presupuesto

El presupuesto planteado para el desarrollo e implementación inicial la propuesta se basa principalmente en los recursos humanos especializados y la infraestructura tecnológica necesaria para poder desarrollar y entrenar los modelos de IA. La mayor inversión se destina hacia el equipo de desarrollo Core (Analistas, científicos de datos y desarrolladores backend) y los costes de la infraestructura en la nube, estos son indispensables para el procesamiento masivo de datos y el entrenamiento de los algoritmos biométricos. Esto presupuesto tiene una duración estimada de 6-9 meses, dejando todo listo para el despliegue comercial.

Rubro	Descripción del Gasto	Costo Estimado (USD)	Costo Estimado (SOLES)
I. Recursos Humanos (6 meses)			
Desarrollador Principal (Semi-Senior)	Diseño e implementación de algoritmos clave (OCR/Biometría).	$ 15,000.00	S/57,000
Desarrollador Web/APIs (Junior/Semi)	Desarrollo de las APIs de integración y flujo UX/UI.	$ 10,000.00	S/38,000
Consultor Legal/Cumplimiento (Part-time)	Revisión y validación de requisitos KYC/AML.	$ 4,000.00	S/15,200
II. Tecnología e Infraestructura			
Servidores en la Nube (Piloto)	Uso de nivel gratuito / créditos iniciales	$ 2,500.00	S/9,500
Adquisición de Datos / Datasets	Compra de datos/licencias para entrenamiento inicial de modelos.	$ 3,000.00	S/11,400
Licencias de Software Básico	Herramientas de desarrollo, seguridad y gestión de código.	$ 1,500.00	S/5,700
III. Pruebas y Certificación (Fase Piloto)			
Auditoría de Seguridad Externa (Mínima)	Pen-testing de APIs clave.	$ 3,000.00	S/11,400
Gastos Operativos de Piloto	Pruebas internas, documentación, soporte limitado.	$ 2,000.00	S/7,600
TOTAL ESTIMADO DEL PROYECTO (Fases Iniciales)		$ 41,000.00	S/155,800

CONCLUSIONES

La investigación confirma de manera concluyente la hipótesis de que la implementación de tecnología de verificación de identidad avanzada en los juegos de azar en línea mejora sustancialmente la gestión de datos de los usuarios.

También establece que la implementación de la tecnología de verificación de identidad no solo cumple su propósito principal, sino que también impulsa la mejora de las funciones tecnológicas generales implementadas en los juegos de azar en línea, confirmando así la hipótesis.

Aunque la investigación confirma que la implementación de la tecnología de verificación de identidad ha generado una percepción positiva de mejora en el sistema, esta mejora resulta ser insuficiente para satisfacer la demanda de seguridad del usuario. Este contraste subraya que, si bien las mejoras son un paso en la dirección correcta, la implementación de una tecnología de verificación de identidad más avanzada o robusta es necesaria para abordar plenamente la brecha de seguridad percibida, logrando así una gestión de usuarios más efectiva y una satisfacción del usuario completa.

Aunque la tecnología de verificación de identidad ha avanzado y se han percibido mejoras en el sistema, estas actualizaciones no han sido suficientes para satisfacer plenamente la demanda de una optimización y un uso eficiente de los recursos del sistema.

La propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea tiene como objetivo mejorar tres puntos clave, beneficiando a los operadores de estas plataformas debido a que les ayuda al cumplimiento legal y normativo de la gestión de datos de sus usuarios y ayudando a la reducción del fraude en sus plataformas. También beneficiara a los usuarios, dándoles la

seguridad de que sus datos estarán protegidos por una seguridad muy difícil de vulnerar, dándoles también un sistema de verificación más rápido y efectivo que el actual, y por último ayudando a los reguladores y auditores a realizar un trabajo más simple y efectivo a la hora de cumplir con sus labores.

La innovación de esta propuesta se basa en que actualmente los sistema de verificación actuales son lentos y suele fallar mientras que en este proyecto se busca implementar una solución propia basada en IA y biometría facial en tiempo real que supera los controles actuales, reduciendo el proceso de verificación actual que puede ser tedioso y presentar fallos a un proceso rápido y sencillo, lo cual se logra mediante una metodología rigurosa que lleva desde la creación y entrenamiento de modelos de Machine Learning hasta la integración de un proceso piloto que nos permitirá optimizar y mejorar los algoritmos creados para poder presentar una tecnología bien entrenada, todo esto sustentado por un presupuesto aproximado de $41,000 dólares, enfocado en el talento humano especializado necesario y la infraestructura cloud necesaria para el desarrollo del proyecto.

Para lograr su penetración de mercado, la estrategia se basa en un retorno de inversión (ROI) rápido a través de pruebas de concepto y también se apoya en alianzas estratégicas con firmas de abogados y empresa de consultoría que cuenten con área de compliance, estos servirán como aliados estratégicos en la implementación legal del proyecto. La fuente de ingresos del proyecto proviene de los honorarios de consultoría, licencias por propiedad intelectual y las tarifas de mantenimiento post-implementación. Logrando así no solo que la propuesta sea viable si no que sea una excelente opción para poder garantizar el cumplimiento normativo, la seguridad de los usuarios y la satisfacción de estos mismos.

RECOMENDACIONES

Se recomienda priorizar una auditoría constante del sistema para identificar y resolver de manera eficiente los fallos que puedan afectar el rendimiento general. Es crucial que la inversión en la tecnología de verificación de identidad no degrade, sino que contribuya directamente a la velocidad y eficiencia de los recursos del sistema, asegurando así que las mejoras tecnológicas se traduzcan en una experiencia de usuario final superior y sin fricciones.

Se debe desarrollar una estrategia de comunicación proactiva que enfatice cómo la tecnología de verificación de identidad funciona como un catalizador para mejorar la utilidad y funcionalidad de otras características de la plataforma. Esta comunicación debe ir más allá de la seguridad, demostrando a los usuarios que la verificación se traduce en beneficios tangibles, como procesos más rápidos y una interacción sistémica más segura y eficiente.

Para mantener el alto nivel de satisfacción inicial y adelantarse a las expectativas, la plataforma debe establecer un ciclo de mejora continua para la gestión de datos y la tecnología de verificación. Este proceso debe implicar la realización de evaluaciones periódicas del usuario y el uso de la retroalimentación obtenida para iterar y actualizar proactivamente la tecnología, asegurando que la plataforma siempre se mantenga a la vanguardia en seguridad y calidad de servicio.

Para asegurar el éxito y la máxima rentabilidad de la tecnología de verificación de identidad propuesta, se recomienda a los Operadores de Juegos de Azar en línea que adopten una mentalidad de innovación continua en la gestión de datos, tratando la solución propuesta no solo como un requisito de cumplimiento sino como un motor de crecimiento y fidelización; esto

implica asignar recursos continuos para la monitorización de patrones de fraude emergentes y la reentrenamiento periódico de los modelos de IA para mantener la ventaja obtenida.

Asimismo, el Proyecto se debe enfocar en la certificación de terceros, buscando la validación de organismos internacionales de biometría o seguridad para aumentar la confianza y credibilidad ante los reguladores y grandes operadores. Finalmente, es crucial que las alianzas estratégicas se formalicen rápidamente, priorizando la colaboración con las firmas de cumplimiento, ya que ellas serán el canal más efectivo para la rápida penetración en el mercado, permitiendo que la propuesta sea incluida directamente en los dictámenes legales como la solución tecnológica preferida para la mitigación efectiva de riesgos de fraude o lavado de dinero.

Es importante implementar una tecnología de verificación de identidad avanzada, acompañada de un monitoreo continuo, para atender la clara demanda de seguridad expresada por la gran mayoría de usuarios. Esta medida no solo debe satisfacer la baja sensación seguridad percibida, sino que también consolidará la gestión de datos de la plataforma como segura y confiable, elevando así la confianza y la satisfacción final del consumidor.

REFERENCIAS BIBLIOGRÁFICAS

Allen, D. W. (2016). The path to self-sovereign identity. *Future of FinTech, 1* (2) 10-12. https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

Arias, F. G. (2012). *El Proyecto de Investigación: Guía para su Elaboración.* Episteme.

Arner, D. W., Barberis, J. Y Buckley, R. P. (2017). FinTech, RegTech and the future of financial intermediation. *Columbia Business Law Review 2017* (2), 585-611. https://doi.org/10.1093/cblr/2017.2.585

Biega, A., Gummadi, K. P. Y Weikum, G. (2018). Equity and fairness in algorithmic decision making. *Proceedings of the 2018 World Wide Web Conference (WWW '18)* (págs. 1655-1664). Lyon: ACM. https://doi.org/10.1145/3178876.3186159

Cate, F. H., Cullen, C. M. Y Mayer-Schönberger, V. (2014). *The Future of Privacy: Private Conversations with Government.* Oxford University Press.

Cavoukian, A. (2011). *Privacy by Design: The Seven Foundational Principles.* Information and Privacy Commissioner of Ontario .

Chen, H., Chiang, R. H. Y Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 36*(4), 1165-1188. https://www.google.com/search?q=https://doi.org/10.2307/41703498

Commission, E. (2021). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).* Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/%3Furi%3DCOM%253A2021%253A206%253AFIN

Davenport, T. H. (2018). *The AI Advantage: How to Put the Artificial Intelligence Revolution to Work.* Cambridge: The MIT Press.

Deloitte. (2021). *Future of digital identity: Harnessing the power of biometrics and AI.* London: Deloitte Insights.

ENISA. (2021). *The landscape of digital identity in Europe.* Heraklion: ENISA.

Arce, A. Y Villamizar, L. (2022). Análisis de la Ciberseguridad y el Marco Legal de la Biometría. Revista de Tecnología, 21(2), 55–66. https://doi.org/10.18273/revtecn.v21n2-2022005

Filippi, P. D. Y Swan, M. (2017). *Blockchain and the Law: The Rule of Code.* Cambridge, MA: Harvard University Press.

Floridi, L. Y Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374*(2083), 1-10. https://doi.org/10.1098/rsta.2016.0360

Gamarra, N. C. (2024). Desafíos ético-jurídicos en el uso de Inteligencia Artificial para el tratamiento masivo de datos biométricos. *Deusto Journal of Human Rights*, 341-374. https://www.google.com/search?q=https://doi.org/10.18543/djhr-16-1-2024-21

Help, A. (22 de junio de 2025). *Gambling addiction statistics*. https://www.addictionhelp.com/gambling/statistics/

Hernández-Sampieri, R. Y Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw Hill Education.

Hernández-Sampieri, R. Y Fernández-Collado, C. Y Baptista-Lucio, M. d. (2014). *Metodología de la investigación.* McGraw Hill Education.

Jain, A. K., Ross, A., Y Nandakumar, K. (2011). *Introduction to Biometrics.* Springer.

Jain, A. K., Ross, A., Y Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4-20. https://doi.org/10.1109/TCSVT.2003.818349

Kuner, C. (2020). *European Data Protection Law: Regulation and Practice* (3rd ed. ed.). Oxford University Press.

La Madrid Coz, G. R. Y Ruiz Toledo, R. A. (2023). *Implementación de un sistema de autenticación mediante validación biométrica para procesos bancarios.* Universidad Peruana de Ciencias Aplicadas (UPC). Lima: Universidad Peruana de Ciencias Aplicadas (UPC). http://hdl.handle.net/10757/671962

Llanos Fajardo, K. (09 de 06 de 2024). *La epidemia silenciosa: Ludopatía en niños, adolescentes y jóvenes*. https://peru21.pe/peru/la-epidemia-silenciosa-ludopatia-en-ninos-adolescentes-y-jovenes-enfermedad-adiccion-noticia/

Maltoni, D., Maio, D., Jain, A. K. Y Prabhakar, S. (2022). *Handbook of Fingerprint Recognition* (2nd edition ed.). Springer.

Mayer-Schönberger, V. Y Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Houghton Mifflin Harcourt.

Mittelstadt, B. D., Allo, P. Y Taddeo, M., Wachter, S. Y Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Science and Engineering Ethics, 24*(3), 903-925. https://www.google.com/search?q=https://doi.org/10.1007/s11948-016-9792-5

OCDE. (2015). *Manual de Frascati 2015:Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental.* OECD Publishing.

OECD. (2021). *OECD Recommendation on Access to Research Data from Public Funding.* OECD Publishing.

OECD. (2022). *OECD Digital Economy Outlook 2022.* OECD Publishing.

Ortiz Salazar, E. O., Y Morales Torres, J. C. (2021). *Modelo para sistema de fidelización con reconocimiento facial para terminales de juego en casinos, orientado a facilitar el acceso a clientes sin medios externos de identificación.* Universidad Distrital Francisco José de Caldas. Bogotá, Colombia: Universidad Distrital Francisco José de Caldas. http://hdl.handle.net/11349/28934

Peña Román, A. (2022). *Herramienta de reconocimiento facial de emociones para videojuegos.* Universidad de las Ciencias Informáticas. La habana: Universidad de las Ciencias Informáticas, Facultad 4. https://repositorio.uci.cu/handle/123456789/10606

PwC. (2022). *The future of digital identity: Balancing security and convenience.* PricewaterhouseCoopers.

QuitGamble.com. (2024). *Estadísticas de adicción al juego 2024*. https://quitgamble.com/es/estadisticas-de-adiccion-al-juego/

Ratha, N. K., Connell, J. H. Y Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614-634. https://doi.org/10.1147/sj.403.0614

Risco Martínez, S. G. (2020). *Riesgo al trastorno de juego por Internet y su relación con la función parental.* Pontificia Universidad Católica del Perú. Lima: Pontificia Universidad Católica del Perú. http://hdl.handle.net/20.500.12404/17272

Choo, K. R. Y Liu, L. (2006). A review of digital identity and digital identity management. Journal of Research and Practice in Information Technology, 38(3), 229–245. https://doi.org/10.1145/1410191.1410200.

Sabino, C. A. (2007). *El proceso de investigación.* Panapo.

Salud, M. d. (2024). *Establecimientos del MINSA atendieron más de 11,000 casos por trastorno del juego patológico.* https://www.gob.pe/institucion/minsa/noticias/1079929-establecimientos-del-minsa-atendieron-mas-de-11-000-casos-por-trastorno-del-juego-patologico

Sánchez Paytán, S. A. (2021). *Regulación de la ludopatía y el plan de prevención en las salas de juego de Lima.* https://hdl.handle.net/20.500.14005/11547

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.

Schwab, K. (2016). *La cuarta revolución industrial.* World Economic Forum.

Solove, D. J. (2021). *Understanding Privacy.* Harvard University Press.

Swan, M. (2015). *Blockchain: Blueprint for a new economy.* CA: O'Reilly Media.

Tapia Iñíguez, J. A. (2025). *El fenómeno de las loot boxes en adultos jóvenes chilenos.* Universidad de Chile. Santiago: Universidad de Chile. https://repositorio.uchile.cl/handle/2250/206510

Tene, O. Y Polonetsky, J. (2013). Big data for all: Privacy and freedom in the age of early-warning systems. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 1-56. https://doi.org/10.2139/ssrn.2255734

Velasquez Romero, E. F. (2023). *La ausencia de las medidas de protección en la ley 31557 para prevenir la ludopatía en niños y adolescentes frente a las cajas botín en el Perú.* Universidad César Vallejo. https://hdl.handle.net/20.500.12692/123365

Velásquez Santos, C. A. (2021). *¿Es viable la regulación a los juegos de azar virtuales incluidos en los videojuegos multijugador en línea para prevenir a niños y adolescentes*

de la ludopatía?: una aproximación desde el Derecho. Pontificia Universidad Católica del Perú. http://hdl.handle.net/20.500.12404/20901

Velásquez Santos, C. A. (2021). *¿Es viable la regulación a los juegos de azar virtuales incluidos en los videojuegos multijugador en línea para prevenir a niños y adolescentes de la ludopatía?: una aproximación desde el Derecho.* Pontificia Universidad Católica del Perú. Lima: Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/20901

Villar, A. (2020). Desafíos y riesgos de la verificación de identidad digital en el contexto de la ciberseguridad. *Revista Iberoamericana de Derecho y Tecnología, 12*(4), 101-125. https://www.ridet.es/wp-content/uploads/2020/12/2020_villar_ridet_12.pdf

Weber, R. H. (2019). *Digital Data and Information: A Governance Perspective.* Edward Elgar Publishing.

Xu, M., Chen, Y., Kou, G. Y Heijden, J. V. (2019). Blockchain: A review and research agenda. *Journal of Management Information Systems, 36*(2), 643-663. https://doi.org/10.1080/07421222.2019.1620027

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

ANEXOS

ANEXO 01: INFORME TURNITIN

SEBASTIAN PAOLO SOLDEVILLA MAGALLANES

PROPUESTADEIMPLEMENTACION Final PA4.docx

Instituto San Ignacio de Loyola - ISIL

Detalles del documento

Identificador de la entrega
trn:oid:::30163:530336545

Fecha de entrega
19 nov 2025, 9:30 p.m. GMT-5

Fecha de descarga
16 dic 2025, 9:03 p.m. GMT-5

Nombre del archivo
PROPUESTADEIMPLEMENTACION Final PA4.docx

Tamaño del archivo
807.9 KB

103 páginas

24.067 palabras

131.485 caracteres

21% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

18% Fuentes de Internet
4% Publicaciones
16% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Vanessa Carla Uribe Santa Cruz (Autor)

Sebastian Paolo Soldevilla Magallanes (Autor)

Roxana Alexandra Albarracín Aparicio (Asesor)

ANEXO 02: REGISTRO DE IMPACTO Y RESULTADOS

Registro de Impacto y Resultados

Tipo de documento: Trabajo de Investigación

Título del Trabajo de Investigación o Tesis:

"Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea"

Integrantes:

1. Soldevilla Magallanes, Sebastian Paolo

2. Uribe Santa Cruz, Vanessa Carla

Asesor: Albarracín Aparicio, Roxana Alexandra

Impacto de la investigación

El impacto de una investigación se refiere a los efectos, tanto esperados como inesperados, que esta puede generar, abarcando aspectos económicos, políticos, culturales, ambientales, tecnológicos, sociales, entre otros.

La implementación de una tecnología de verificación de identidad basada en inteligencia artificial y biometría facial genera un impacto positivo en las plataformas de juegos de azar en línea al fortalecer la seguridad, mejorar la calidad de los datos y optimizar la experiencia del usuario. Esta solución reduce riesgos como la suplantación de identidad y el acceso de menores de edad, garantiza registros más confiables desde el primer contacto y agiliza los procesos de autenticación, incrementando la confianza del usuario y el cumplimiento normativo por parte de las plataformas.

Resultado del proceso de investigación

Los resultados de un proyecto de investigación son los descubrimientos o conclusiones alcanzadas después de realizar el estudio. Estos reflejan los datos obtenidos durante el proceso investigativo y responden a las preguntas o hipótesis formuladas al comienzo del proyecto. Los resultados son fundamentales para evaluar, interpretar y comprender los efectos o la validez de lo investigado.

Los resultados del estudio evidencian una alta aceptación de la propuesta, ya que el 74% de los usuarios considera necesario mejorar las funciones tecnológicas, el 81% respalda el reforzamiento de los controles de seguridad y el 75% apoya la optimización del sistema. Estos hallazgos confirman la hipótesis planteada, demostrando que la tecnología de verificación actual es percibida como insuficiente y que la implementación de una solución basada en lA y biometría facial permitiría una gestión de datos más segura, eficiente y confiable.

MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea.

PROBLEMA	OBJETIVOS	HIPÓTESIS	IMPLEMENTACION DE TECNOLOGÍA DE VERIFICACIÓN DE IDENTIDAD			
Problema Principal	**Objetivo General**	**Hipótesis General**	**Dimensiones**	**Indicadores**	**Preguntas**	**Item**
Determinar cómo la implementación de la tecnologia de verificación de identidad puede mejorar la gestión de datos de los usuarios en juegos de azar en línea.	Proponer la implementación de la tecnologia de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea.	La implementación de la tecnologia de verificación de identidad mejora la gestión de datos de los usuarios en juegos de azar en línea.	Efectividad del sistema	Frecuencia de autenticación	¿El sistema solicita verificación de identidad cada vez que accedes a tu cuenta en la plataforma de diferentes dispositivos? Escala Likert de frecuencia (1 = nunca, 5	
					¿Considera adecuada la frecuencia con la que el sistema le solicita autenticación para ingresar o realizar transacciones? Escala Likert de frecuencia (1 = nunca, 5 =	
					¿Le gustaría que la frecuencia de autenticación varíe según el tipo de operación o nivel de riesgo? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 =	
			Gestión de riesgos	Registro de incidentes	¿El sistema registra intentos fallidos o sospechosos de verificación de identidad? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 = totalmente de	
					¿Cree que el sistema actual permite gestionar adecuadamente los riesgos de acceso no autorizado? Escala Likert de frecuencia (1 = nunca, 5 = siempre)	
					¿Recomendaría implementar alertas inmediatas ante intentos fallidos de autenticación? Opciones múltiples (sms, llamada, correo electronico,ninguna)	
			Efectos de mejora continua	Evaluaciones realizadas	¿Ha notado alguna actualización o mejora reciente en el sistema de verificación de identidad? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 =	
					¿Considera que la tecnología utilizada ha mejorado en precisión y facilidad de uso recientemente? Escala Likert de frecuencia (1 = nunca, 5 = siempre)	
					¿Considera necesario realizar evaluaciones continuas para actualizar y mejorar el sistema? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 = totalmente	
Problema específicos	**Objetivos Específicos:**	**Hipótesis específicas:**				
			GESTION DE DATOS			
			Dimensiones	**Indicadores**	**Preguntas**	**Item**
¿Determinar Cómo la implementacion de la tecnología de verificación de identidad puede mejorar las funciones de tecnologías implementadas en juegos de azar en línea?	Determinar cómo la implementacion de la tecnología de verificación de identidad puede mejorar las funciones de tecnologías implementadas en juegos de	La implementacion de la tecnología de verificación de identidad puede mejorar las funciones de tecnologias implementadas en juegos de azar en línea	Funciones de tecnologías implementadas	Incorporacion de tecnologías avanzadas	¿Qué tecnológias nuevas ha notado que están disponibles cuando interactúa con nuestro servicio? Opciones múltiples (reconocimiento facial, biometría, autenticación en dos pasos,	
					¿Qué tan útiles le parecen las tecnologías implementadas en nuestro sistema durante su experiencia como usuario? Escala Likert de utilidad (1 = nada util, 5 = muy util).	
					¿Qué tan necesario considera que es mejorar o ampliar las funciones tecnológicas actuales del sistema? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 = totalmente de	
¿Determinar Cómo la implementacion de la tecnología de verificación de identidad puede mejorar la seguridad de informacion de los usuarios en juegos de azar en línea?	Determinar cómo la implementacion de la tecnología de verificación de identidad puede mejorar la seguridad de informacion de los usuarios en juegos de	La implementacion de la tecnología de verificación de identidad puede mejorar la seguridad de informacion de los usuarios en juegos de azar en línea	Seguridad de la información	Controles de acceso aplicados	¿Qué mecanismos debe usar para autenticarse en la plataforma? Opciones Multiples (Contraseña, código SMS, biometría, doble factor, ninguno)	
					¿Qué tan seguro se siente con los controles de acceso actuales que se aplican para proteger su información? Escala Seguridad (1 = nada seguro, 5 = muy seguro)	
					¿Está de acuerdo con reforzar los controles para proteger mejor su información? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo)	
¿Determinar Cómo la implementacion de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea?	Determinar cómo la implementacion de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea	La implementacion de la tecnología de verificación de identidad puede mejorar el uso de recursos del sistema en juegos de azar en línea	Uso de recursos del sistema	Eficiencia operativa	¿Con qué frecuencia el sistema funciona sin interrupciones y con rapidez? Escala Likert de frecuencia (1 = nunca, 5 = siempre)	
					¿Qué tan eficiente considera que es el sistema en tiempos de respuesta, estabilidad y velocidad? Escala Likert de eficiencia (1 = nada eficiente, 5 = totalmente eficiente)	
					¿Está de acuerdo con que se optimice el sistema para mejorar su rendimiento y la experiencia del usuario? Escala Likert de acuerdo (1 = totalmente en desacuerdo, 5 = totalmente de	

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN	ITEMS	INST	ESCALAS				
								1	2	3	4	5
Variable 1 Tecnología de verificación de identidad	La tecnología de verificación de identidad son el uso de sistemas digitales como biometría, reconocimiento facial y validación documental para autenticar usuarios, prevenir fraudes y proteger datos personales en entornos digitales. (Arce, A., & Villamizar, L. 2022).	Se evaluara mediante un cuestionario midiendo la efectividad del sistema, la gestión de riesgos y los efectos de mejora continua. Se recogera la percepcion de los encuestados respecto a la facilidad de uso y rapidez, proteccion de datos y precisión del sistema de verificación de identidad de los usuarios en juegos de azar en línea. Operacionalmente está conformada por 3 dimensiones	Efectividad del sistema	Frecuencia de autenticación	ORDINAL	1 3 5	CUESTIONARIO	NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE
			Gestión de riesgos	Registro de incidentes		8 9 10						
			Efectos de mejora continua	Evaluaciones realizadas		15 16 17						
Variable 2 Gestión de datos de los usuarios	La gestión de datos de los usuarios implica la recopilación, almacenamiento, procesamiento y protección de información personal mediante sistemas tecnológicos, asegurando integridad, confidencialidad y disponibilidad para optimizar la toma de decisiones y cumplir con normativas de privacidad (García & López, 2022).	Se medira con un cuestionario considerando incorporacion de tecnologías avanzadas, seguridad de la información y eficiencia operativa. Permitira identificar el nivel de adopción tecnológica, el grado de protección de datos y uso adecuado durante la verificación de identidad de los usuarios en juegos de azar en línea.	Funciones de tecnologÍas implementadas	Incorporacion de tecnologias avanzadas	ORDINAL	1 2 3	CUESTIONARIO	NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE
			Seguridad de la información	Controles de acceso aplicados		6 7 8						
			Uso de recursos del sistema	Eficiencia operativa		13 14 20						

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Hola somos Sebastian y Vanessa estudiantes de la escuela de negocios de Isil y estamos haciendo una encuesta para nuestro de trabajo de investigación

Pregunta	**1**	**2**	**3**	**4**	**5**
1.- ¿El sistema solicita verificación de identidad cada vez que accedes a tu cuenta en la plataforma de diferentes dispositivos?	Nunca	Rara vez	A veces	Frecuen-temente	Siempre
2.- ¿Considera adecuada la frecuencia con la que el sistema le solicita autenticación para ingresar o realizar transacciones?	Nunca	Rara vez	A veces	Frecuen-temente	Siempre
3.- ¿Le gustaría que la frecuencia de autenticación varíe según el tipo de operación o nivel de riesgo?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
4.- ¿El sistema registra intentos fallidos o sospechosos de verificación de identidad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
5.- ¿Cree que el sistema actual permite gestionar adecuadamente los riesgos de acceso no autorizado?	Nunca	Rara vez	A veces	Frecuen-temente	Siempre
6.- ¿Recomendaría implementar alertas inmediatas ante intentos fallidos de autenticación?	SMS	Llamada	Correo electrónico	Ninguna	

7.- ¿Ha notado alguna actualización o mejora reciente en el sistema de verificación de identidad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
8.- ¿Considera que la tecnología utilizada ha mejorado en precisión y facilidad de uso recientemente?	Nunca	Rara vez	A veces	Frecuen-temente	Siempre
9.- ¿Considera necesario realizar evaluaciones continuas para actualizar y mejorar el sistema?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
10.- ¿Qué tecnologías nuevas ha notado que están disponibles cuando interactúa con nuestro servicio?	Reconocimiento facial	Biometría	Autenticación en dos pasos	Encriptación	Ninguna
11.- ¿Qué tan útiles le parecen las tecnologías implementadas en nuestro sistema durante su experiencia como usuario?	Nada útil	Poco útil	Moderada-mente útil	Bastante útil	Muy útil
12.- ¿Qué tan necesario considera que es mejorar o ampliar las funciones tecnológicas actuales del sistema?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
13.- ¿Qué mecanismos debe usar para	Contraseña	Codigo SMS	Biometría	Doble factor	Ninguno

autenticarse en la plataforma?					
14.- ¿Qué tan seguro se siente con los controles de acceso actuales que se aplican para proteger su información?	Nada seguro	Poco seguro	Neutral / Ni seguro ni inseguro	Bastante seguro	Muy seguro
15.- ¿Está de acuerdo con reforzar los controles para proteger mejor su información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
16.- ¿Con qué frecuencia el sistema funciona sin interrupciones y con rapidez?	Nunca	Rara vez	A veces	Frecuen-temente	Siempre
17.- ¿Qué tan eficiente considera que es el sistema en tiempos de respuesta, estabilidad y velocidad?	Nada eficiente	Poco eficiente	Moderada-mente eficiente	Bastante eficiente	Totalemente eficiente
18.- ¿Está de acuerdo con que se optimice el sistema para mejorar su rendimiento y la experiencia del usuario?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

VALIDACIÓN DE EXPERTOS

INFORME DE JUCIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN VARIABLE 1

1.1. Apellidos y Nombres del experto:	Albarracín Aparicio Roxana Alexandra
1.2. Cargo e institución del experto:	Asesor Isil
1.3. Nombre del instrumento:	Encuestas
1.4. Autor del instrumento:	Sebastian Soldevilla y Vanessa Uribe
1.5. Título de la investigación	Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea

II. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	Deficiente 00-20%	Regular 21-40%	Buena 41-60%	Muy buena 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado y específico.				X	
2. OBJETIVIDAD	Está expresado en conductas observables.				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología.				X	
4. ORGANIZACION	Existe organización lógica				X	
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias.				X	
7. CONSISTENCIA	Basados en aspectos teóricos-científicos				X	
8. COHERENCIA	Entre los índices, indicadores y dimensiones.				X	
9. METODOLOGIA	La estrategia responde al propósito del diagnóstico.				X	
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.				X	
PROMEDIO DE VALIDACION					85%	

PERTINENCIA DE LOS ÍTEMS O REACTIVOS DEL INSTRUMENTO

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE
Ítem 1	X		
Ítem 2	X		
Ítem 3	X		
Ítem 4	X		
Ítem 5	X		
Ítem 6	X		
Ítem 7	X		
Ítem 8	X		
Ítem 9	X		
Ítem 10	X		

III. PROMEDIO DE VALORACIÓN:

IV. _____85_____%. V: OPINIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado.

Firma del experto:

Lugar y fecha: Lima, 3/07/2024

DNI Nº 41981490

ORCID 0000-0002-6930-3718

INFORME DE JUCIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN VARIABLE 2

1.1. Apellidos y Nombres del experto:	Albarracín Aparicio Roxana Alexandra
1.2. Cargo e institución del experto:	Asesor Isil
1.3. Nombre del instrumento:	Encuestas
1.4. Autor del instrumento:	Sebastian Soldevilla y Vanessa Uribe
1.5. Título de la investigación	Propuesta de implementación de la tecnología de verificación de identidad para mejorar la gestión de datos de los usuarios en juegos de azar en línea

VI. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	Deficiente 00-20%	Regular 21-40%	Buena 41-60%	Muy buena 61-80%	Excelente 81-100%
11. CLARIDAD	Está formulado con lenguaje apropiado y específico.				X	
12. OBJETIVIDAD	Está expresado en conductas observables.				X	
13. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología.				X	
14. ORGANIZACION	Existe organización lógica				X	
15. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.				X	
16. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias.				X	
17. CONSISTENCIA	Basados en aspectos teóricos-científicos				X	
18. COHERENCIA	Entre los índices, indicadores y dimensiones.				X	
19. METODOLOGIA	La estrategia responde al propósito del diagnóstico.				X	
20. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.				X	
PROMEDIO DE VALIDACION					85%	

PERTINENCIA DE LOS ÍTEMS O REACTIVOS DEL INSTRUMENTO

INSTRUMENTO	SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE
Ítem 1	X		
Ítem 2	X		
Ítem 3	X		
Ítem 4	X		
Ítem 5	X		
Ítem 6	X		
Ítem 7	X		
Ítem 8	X		
Ítem 9	X		
Ítem 10	X		

VII. PROMEDIO DE VALORACIÓN:

VIII. _____85____%. V: OPINIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado.

Firma del experto:

Lugar y fecha: Lima, 3/07/2024

DNI Nº 41981490

ORCID 0000-0002-6930-3718