DESDE 2023
https://rictrevista.org

RICT Revista de Investigación Científica, Tecnológica e Innovación

Publicación Semestral RICT Vol. 3 No. 6 (2025) P. 26 – 35

ISSN: 2992-7315

Aplicación de un modelo de clustering para el análisis del comportamiento de usuarios de la banca en línea para la clasificación de riesgos cibernéticos
Application of a clustering model for the analysis of online banking user behavior for cyber risk classification.

Jasmin-Estephany Guerrero-Lora[a]

[a]*Licenciatura en Tecnologías de la Información y Comunicación, Universidad Nacional Rosario Castellanos, 07969, Ciudad de México, México.*

Resumen

Este estudio se centra en la relación entre los hábitos de los usuarios de banca en línea y su susceptibilidad a ciberataques dentro del sistema bancario mexicano. En un contexto de creciente digitalización de los servicios financieros, se identifica el problema de cómo determinadas prácticas de los usuarios pueden incrementar los riesgos de ser víctimas de fraude financiero. Se utilizó una metodología cuantitativa mediante la aplicación de una encuesta diseñada para descubrir patrones de comportamiento de riesgo entre los usuarios de banca en línea para con ello crear una clasificación utilizando el método de clustering k-means. Los resultados revelaron que hábitos como el uso de conexiones inseguras, la falta de software de seguridad y las malas prácticas de gestión de contraseñas están directamente relacionados con una mayor incidencia de fallos de seguridad. El estudio concluye con recomendaciones para mejorar la educación y las políticas de seguridad dirigidas a los usuarios, así como estrategias para que las entidades financieras refuercen sus sistemas frente a ciberataques.

Palabras clave: Clustering K-Means, análisis del comportamiento, riesgo cibernético, prevención de fraudes bancarios

Abstract

This study focuses on the relationship between online banking users' habits and their susceptibility to cyberattacks within the Mexican banking system. In a context of increasing digitalization of financial services, the problem of how certain user practices can increase the risks of being victims of financial fraud is identified. A quantitative methodology was used through the application of a survey designed to discover patterns of risk behavior among online banking users in order to create a classification using the k-means clustering method. The results revealed that habits such as the use of insecure connections, lack of security software, and poor password management practices are directly related to a higher incidence of security breaches. The study concludes with recommendations to improve education and security policies aimed at users, as well as strategies for financial institutions to strengthen their systems against cyberattacks.

Keywords: keyword 1, Clustering K-Means, behavioral analysis, cyber risk, bank fraud prevention

1. Introducción

El sistema bancario mexicano ha experimentado una transformación significativa en las últimas décadas y ha adoptado tecnologías digitales para mejorar la eficiencia y la accesibilidad de sus servicios (Trillo del Pozo & Alonso Gallo, 2021). Este cambio ha resultado en un aumento en el uso de la banca en línea, que permite a los usuarios realizar transacciones financieras desde la comodidad de sus hogares. Sin embargo, la digitalización también ha atraído a actores maliciosos que buscan explotar vulnerabilidades en los sistemas de seguridad para llevar a cabo ataques cibernéticos (Quintero Peña & Mejía Baños, 2021). Los ataques cibernéticos en el sistema bancario mexicano han mostrado una tendencia al alza, con un aumento en la frecuencia e intensidad de los incidentes (Realpe & Cano, 2020). Las instituciones financieras han enfrentado una variedad de amenazas, que incluyen el phishing, ransomware y ataques a la infraestructura de red (Capeta Mondoñedo et al., 2023). Los

*Autor para la correspondencia: yazlora476@gmail.com
Correo electrónico: yazlora476@gmail.com (Jasmin Estephany Guerrero Lora)

Historial del manuscrito: recibido el 22/07/2025, última versión-revisada recibida el 16/10/2025 aceptado el 18/10/2025, publicado el 06/11/2025. DOI: https://doi.org/10.5281/zenodo.17545595

atacantes no solo buscan robar información financiera valiosa, sino que también intentan socavar la confianza en el sistema bancario (Leiva, 2015). La vulnerabilidad en línea puede tener consecuencias negativas para el bienestar psicológico de un usuario (Moran-Fuentes et al., 2022; Varchetta et al., 2020). Es importante que las instituciones financieras mejoren sus estándares de seguridad y adopten estrategias más efectivas para protegerse contra estos ataques (Realpe & Cano, 2020).

En el contexto descrito, la ciberseguridad en el sector bancario se ha convertido en un aspecto crucial para garantizar la integridad y la confianza en el sistema financiero (Capeta Mondoñedo et al., 2023). Las instituciones financieras almacenan una gran cantidad de información sensible, incluyendo datos personales y detalles de transacciones financieras. Un ataque exitoso podría resultar en la pérdida de grandes sumas de dinero, así como en daños a la reputación de la institución afectada (Moran-Fuentes et al., 2022). Además, la confianza de los clientes en la banca en línea podría disminuir significativamente, lo que tendría un impacto negativo en la adopción de estos servicios (Capeta Mondoñedo et al., 2023). Por lo tanto, fortalecer la ciberseguridad en las instituciones financieras no es solo una cuestión de proteger los activos financieros, sino también de mantener la confianza en el sistema bancario en su conjunto (Capeta Mondoñedo et al., 2023). Las instituciones deben adoptar estrategias de ciberseguridad proactivas, implementando las últimas tecnologías y prácticas de seguridad para prevenir, detectar y responder a los ataques cibernéticos de manera efectiva (Leiva, 2015).

Los ataques cibernéticos en el sistema bancario no son un fenómeno nuevo, sino que han ido evolucionando a lo largo de los años con el aumento de la digitalización de los servicios financieros (Negro & Pons, 2022). Los años 90 marcaron el comienzo de los ataques cibernéticos a bancos, aunque eran menos sofisticados que los actuales, ya se evidenciaban intentos de fraude y robo de información (Sastré, 2022). Con el auge del internet en la década del 2000, los ataques se volvieron más frecuentes y sofisticados (Manssur Nicola, 2023). Uno de los casos más emblemáticos fue el ataque a Bangladesh Bank en 2016, donde los delincuentes lograron robar 81 millones de dólares a través de transferencias fraudulentas (White & Lee, 2021). Este incidente puso de manifiesto la necesidad urgente de fortalecer las medidas de ciberseguridad en el sector bancario (Riveros, 2020). Otro ejemplo significativo fue el ataque a Banco de Chile en 2018, donde un malware fue utilizado para distraer y luego robar 10 millones de dólares (Poveda, 2020).

La historia de los ataques cibernéticos en el sistema bancario mexicano refleja un crecimiento constante y una evolución en la sofisticación y en la magnitud de los incidentes (Cisneros Zepeda, 2021). A finales de la década de los 2000 y principios de la década de 2010, los bancos en México comenzaron a experimentar los primeros ataques cibernéticos significativos, en su mayoría, enfocados en el fraude en línea y el robo de credenciales de los clientes (Rodríguez, 2017). Durante esos años, los delincuentes cibernéticos aprovecharon principalmente las debilidades en los sistemas de autenticación y en la falta de conciencia de seguridad entre los usuarios para realizar transacciones fraudulentas (Cisneros Zepeda, 2021). Un punto de inflexión se produjo en 2013, cuando los bancos mexicanos experimentaron un aumento en los ataques de phishing, que buscaban engañar a los usuarios para que revelaran sus credenciales bancarias en línea (Guaña-Moya et al., 2022).

En 2018, el sistema bancario mexicano fue víctima de un ataque cibernético sin precedentes, conocido como el "Ciberataque a la Banca Mexicana", en el que los delincuentes lograron infiltrarse en el sistema de pagos interbancarios del país, realizando transferencias ilícitas por un monto total de 15 millones de dólares (Leyva Reus, 2019). Este ataque puso de manifiesto la necesidad urgente de mejorar las medidas de ciberseguridad en el sector bancario y generó una respuesta significativa tanto por parte de las autoridades como de los propios bancos (Admati, 2014). Los incidentes continuaron ocurriendo en los años siguientes, demostrando que, a pesar de los esfuerzos para mejorar la seguridad, los sistemas bancarios aún eran vulnerables (Juárez, 2017). Estos ataques han tenido un impacto significativo en la forma en que los bancos y las autoridades mexicanas abordan la ciberseguridad, lo que ocasionó una mayor inversión en tecnologías de seguridad y la implementación de regulaciones más estrictas para proteger tanto a las instituciones financieras como a sus clientes (Camhaji, 2018). La historia de los ataques cibernéticos en México ilustra claramente la magnitud del problema y la necesidad imperante de adoptar estrategias de ciberseguridad más robustas y eficientes (Redacción, 2018).

El objetivo principal de este trabajo es analizar los elementos que influyen en la severidad de los ataques cibernéticos en el sistema bancario desde el punto de vista de los usuarios e identificar las áreas más vulnerables y proponer estrategias de mitigación de riesgos. Al entender las tácticas, técnicas y procedimientos utilizados por los atacantes, las instituciones financieras pueden mejorar sus defensas y responder de manera más efectiva a los incidentes de seguridad (Realpe & Cano, 2020). Este análisis no solo se limita a los aspectos técnicos, sino que también incluye el comportamiento humano y las prácticas organizativas, ya que estos factores juegan un papel crucial en la seguridad cibernética (Moran-Fuentes et al., 2022). La justificación para este estudio radica en la creciente dependencia de la banca en línea y la necesidad de proteger tanto los activos financieros como la información personal de los clientes (Gavilanes L et al., 2021). Al mejorar las estrategias de ciberseguridad, se contribuye a fortalecer la resiliencia del sistema bancario frente a los ataques cibernéticos, garantizando así la confianza de los usuarios y la estabilidad del sistema financiero (Realpe & Cano, 2020).

2. Materiales y Método

Se llevó a cabo un diseño transversal del tipo descriptivo para profundizar en los hábitos de uso de la banca en línea. Se estudiaron diferencias potencialmente asociadas al género y edad en las variables analizadas. La investigación tiene de igual manera un componente correlacional dado que se exploró la relación entre las diferentes prácticas de

ciberseguridad y la distribución de las respuestas dadas a las preguntas categóricas como el uso de redes públicas, la frecuencia con que se cambia la contraseña de acceso a la banca, así como con las sugerencias de los bancos con relación a la ciberseguridad.

2.1. Instrumento

Para llevar a cabo este estudio se diseñó una encuesta que permite indagar sobre los hábitos y comportamientos al usar la banca móvil que podrían incidir en la vulnerabilidad ante ataques cibernéticos. El cuestionario estaba compuesto por 30 preguntas algunas abiertas y otras cerradas con opciones de respuesta tipo Likert.

Las variables evaluadas fueron: frecuencia de uso de la banca móvil, tipo de actividades realizadas (consultas, transferencias, pagos, etc.), lugar de acceso (casa, trabajo, lugares públicos), dispositivo utilizado (teléfono inteligente, tableta, computadora), hábitos de seguridad (uso de antivirus, contraseñas seguras, etc.), experiencia previa con ataques o intentos de fraude, y conocimiento sobre medidas de protección al usar la banca móvil. El instrumento se puede consultar en la siguiente liga: https://forms.gle/3QTdGfQM7veL84Pg8

El instrumento investiga el comportamiento de los usuarios de la banca móvil y en línea en cuanto a los hábitos de uso, el tipo de operaciones y actividades que se realizan con más frecuencia, los lugares desde donde se accede a la cuenta de banco, que hábitos y precauciones se toman para incrementar la seguridad y si han tenido experiencias previas de ataques o intentos de fraude.

2.2. Participantes

La muestra estuvo conformada por 300 usuarios de la banca móvil en México, seleccionados mediante un muestreo no probabilístico por conveniencia. Los criterios de inclusión fueron: 1) ser mayor de 18 años, 2) ser usuario activo de la banca móvil de al menos un banco mexicano. No se consideraron variables sociodemográficas adicionales a la edad y el género en la selección de participantes. En las Figuras 1 y 2 se observa que la muestra estuvo compuesta por 95 mujeres y 205 hombres con edad comprendidas entre 19 y 59 años edad en donde se tuvo una edad promedio de 23.10 años y una desviación estándar de 5.52 años.

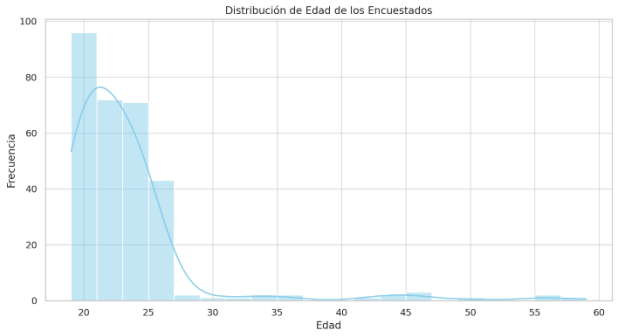

Figura 1: Distribución de edad de los 300 encuestados con una edad mínima de 19 años y una edad máxima de 59.

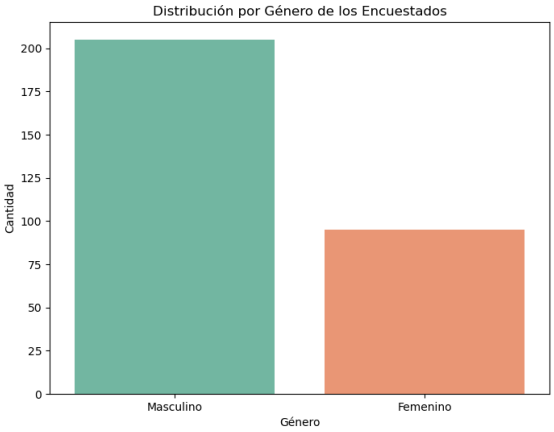

Figura 2: Distribución por género de los encuestados donde se obtuvieron 95 mujeres y 205 hombres.

2.3. Procedimiento

La encuesta fue contestada de forma anónima y confidencial por los participantes mediante un formulario virtual diseñado en Google Forms. El enlace al cuestionario fue compartido a través de redes sociales y grupos de usuarios de banca móvil y algunas escuelas de educación superior donde se aplicó de manera presencial.

Previo a contestar, los participantes debían otorgar su consentimiento informado. No se ofreció ningún incentivo por participar. Los datos fueron recolectados durante un periodo de dos meses y posteriormente exportados y capturados para su análisis.

2.4. Análisis de datos

Los datos fueron analizados con estadística descriptiva utilizando Python versión 3.8 como lenguaje de programación de scripts. Se obtuvieron frecuencias, porcentajes, medias y desviaciones estándar para describir los hábitos y comportamientos de los usuarios de la banca móvil. También se realizaron comparaciones de medias entre grupos y análisis de correlaciones para determinar relaciones entre variables. El propósito fue caracterizar el perfil de uso y los hábitos de seguridad de los usuarios, así como determinar comportamientos de riesgo que podrían incidir en la efectividad de ataques cibernéticos al sistema bancario.

La metodología del análisis incluyó las siguientes fases:

- Análisis descriptivo. Estadísticas descriptivas para analizar medidas de tendencia central y dispersión para las variables cuantitativas. Análisis de frecuencias para analizar la distribución de las respuestas para las preguntas categóricas.

- Análisis de relaciones entre variables. Correlaciones para identificar si hay alguna correlación entre diferentes comportamientos o prácticas de ciberseguridad. Análisis de contingencia que permitió examinar la relación entre dos variables categóricas.

- Identificación de Patrones o Tendencias. Para ello se utilizó el clustering k-means con técnicas de agrupamiento para identificar grupos de individuos con comportamientos similares. Análisis de tendencias para verificar si hay tendencias en el tiempo respecto a las prácticas de ciberseguridad.

- Evaluación de riesgos. Identificación de comportamientos de riesgo determinando qué prácticas están más asociadas con riesgos de ciberseguridad.

- Recomendaciones para mejorar la seguridad. Basado en los resultados, se proporcionan recomendaciones para mejorar las prácticas de ciberseguridad

3. Resultados

Con los análisis descriptivos se obtuvieron los siguientes resultados de acuerdo con las respuestas a las preguntas de la encuesta:

- El 81% de los encuestados no ha sido víctima de algún fraude financiero. Solo el 19% reportó haber sido víctima.

- La transacción realizada con mayor frecuencia es transferencia bancaria (46% de los encuestados).

- El 72% considera la ciberseguridad como "Muy Importante", mientras que el 24% la considera "Importante". Solo un 4% la consideró "Poco Importante".

- El 49% cree que la responsabilidad de la ciberseguridad en el sistema bancario es compartida entre el banco, el gobierno y el usuario.

- El 36% cambia su contraseña de banca en línea una vez al año. Solo el 13% la cambia cada 6 meses.

- El 68% utiliza las aplicaciones oficiales de su banco para evitar ser víctima de fraude.

- El 62% protege su teléfono móvil con contraseña.

- El 49% considera que el precio de los antivirus es accesible.

- El 85% sigue las recomendaciones de seguridad de su banco.

- El 67% toma en cuenta las notificaciones de alerta de seguridad que recibe.

- El 54% renueva su equipo celular cada 18 meses y su computadora cada 18 meses también.

Con el análisis de frecuencias se observa que la mayoría de los participantes son jóvenes, con una edad promedio de alrededor de 23 años. Hay más hombres que mujeres en la muestra. La gran mayoría de los participantes no han sido víctimas de fraude financiero como usuarios del sistema bancario mexicano, sólo 37 participantes han sido víctimas de fraude. Muchos participantes no cambian su contraseña de la banca en línea con frecuencia. La mayoría sigue las recomendaciones de seguridad de su banco y actualiza su sistema operativo cuando reciben notificaciones. Hay una cantidad considerable de personas que utilizan redes públicas y/o abiertas para navegar en internet, 42%, lo cual puede ser un riesgo de seguridad.

En el análisis de correlaciones entre variables cuantitativas y algunas variables categóricas que fueron codificadas para el análisis como las respuestas a las preguntas "¿Sigue las recomendaciones de seguridad de su banco?" o "¿Utiliza redes públicas y/o abiertas para navegar en internet?" para analizar su relación con la edad, se tuvieron los resultados mostrados en la Fig. 3.

Figura 3. Matriz de correlación entre las variables: frecuencia de cambio de contraseña, sigue las recomendaciones de seguridad del banco, uso de redes públicas para el acceso al banco y la edad.

En las variables edad y seguir las recomendaciones de seguridad del banco hay una correlación positiva muy débil. Las personas mayores tienden a seguir ligeramente más las recomendaciones de seguridad de su banco. Se observa que en la relación entre la edad y el utilizar redes públicas hay una correlación positiva muy débil. Las personas mayores tienden ligeramente a usar menos redes públicas y/o abiertas para navegar en internet. En el último caso sobre la frecuencia de cambio de contraseña hay una correlación negativa también muy débil. Las personas mayores tienden a cambiar sus contraseñas de banca en línea con más frecuencia.

La correlación más fuerte se observa entre la edad y el uso de redes públicas, lo que sugiere que las personas mayores podrían ser más conscientes de la importancia de no utilizar redes públicas para el acceso a los servicios de banca en línea. Las otras correlaciones son bastante débiles, lo que indica que no hay una relación lineal fuerte entre la edad y estas prácticas de ciberseguridad.

Posteriormente en el análisis de contingencia entre ser víctima de fraude bancario o financiero con las variables de la frecuencia de cambio de contraseña, uso de redes públicas para navegar en internet y seguir las recomendaciones de seguridad del banco se tuvieron los resultados mostrados en las tablas I, II y III.

En cuanto a la frecuencia de cambio de contraseña se tiene que de los que cambian la contraseña cada año, el 18% ha sido víctima de fraude. El 24% de los que cambian la contraseña cada 6 meses, ha sido víctima de fraude financiero. Dado que no parece haber una relación fuerte entre estas variables se realizó el estadístico de Chi-Cuadrado para la tabla de contingencia mostrada en la tabla 1 y se obtuvo un valor de chi-cuadrada de 0.6757 con un valor p igual 0. 8788, lo cual es mucho mayor que 0.05. Esto sugiere que no hay una relación estadísticamente significativa entre la frecuencia con la que las personas cambian sus contraseñas de la banca en línea y si han sido víctimas de fraude financiero. Lo que significa que, de acuerdo con los datos de la encuesta, cambiar las contraseñas con más o menos frecuencia no parece tener un impacto significativo en el riesgo de experimentar fraude financiero.

Tabla 1: Análisis de contingencia: Ser víctima de fraude y frecuencia de cambio de contraseña

	Frecuencia de cambio de contraseña			
Víctima de Fraude Financiero	Cada año	Cada seis meses	Una vez al mes	Otro
No	94	35	30	104
Si	11	5	4	17

Tabla 2: Análisis de contingencia: Ser víctima de fraude y seguimiento de las recomendaciones de seguridad del banco

¿Usted ha sido víctima de algún fraude financiero?	¿Sigue las recomendaciones de seguridad del Banco?	
	No	Si
No	56	9
Si	207	28

El estadístico de Chi-Cuadrado arrojó un valor 0. 0.0424 con un valor p de 0. 0.8367 lo cual es mucho mayor que 0.05. Esto también significa que no hay evidencia suficiente para rechazar la hipótesis nula de independencia entre ser víctima de un fraude financiero y el seguimiento de las recomendaciones de seguridad del banco. En otras palabras, no se encontró una relación estadísticamente significativa entre haber sido víctima de fraude financiero y seguir las recomendaciones de seguridad del banco en este conjunto de datos.

Tabla 3: Análisis de contingencia: Ser víctima de fraude y uso de redes públicas y/o abiertas para navegar en internet

¿Usted ha sido víctima de algún fraude financiero?	¿Utiliza redes públicas o abiertas para navegar en Internet?	
	No	Si
No	153	21
Si	110	16

Para el estadístico de Chi-Cuadrado se obtuvo un valor de 0.0002 y el valor para p fue 0.9886 lo cual también es mucho mayor que 0.05. Esto significa que no hay evidencia suficiente para rechazar la hipótesis nula de independencia entre ser víctima de un fraude financiero y el uso de redes públicas y/o abiertas para navegar en internet. En otras palabras, no se encontró una relación estadísticamente significativa entre haber sido víctima de fraude financiero y el uso de redes públicas y/o abiertas para navegar en internet en este conjunto de datos.

Tabla 4. Análisis de contingencia: Ser víctima de frade y frecuencia de instalación de actualizaciones del sistema

¿Usted ha sido víctima de algún fraude financiero?	Frecuencia en la instalación de actualizaciones del sistema			
	Cada 6 meses	Cada mes	Cada vez que llegan notificaciones	Nunca
No	74	78	110	1
Si	9	9	19	0

En este análisis de contingencia se obtuvo un valor para el estadístico de Chi-Cuadrado de 1.3138 y un valor p de 0.7258, lo cual es mayor que 0.05. Esto significa que no hay evidencia suficiente para rechazar la hipótesis nula de independencia entre ser víctima de un fraude financiero y la frecuencia de instalación de actualizaciones del sistema. En otras palabras, no se encontró una relación estadísticamente significativa entre haber sido víctima de fraude financiero y la frecuencia de instalación de actualizaciones del sistema en este conjunto de datos.

En la exploración de algunas variables con relación a haber sido víctima de un fraude financiero, no se encontraron relaciones estadísticamente significativas en este conjunto de datos.

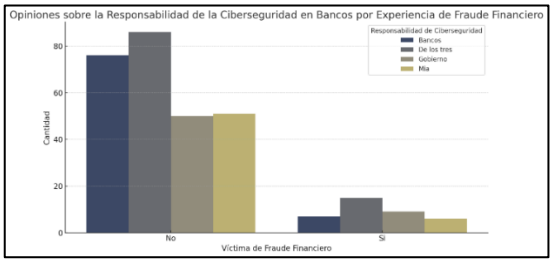

Figura 4. Opiniones sobre la responsabilidad de ciberseguridad dada la experiencia de fraude financiero.

Los análisis sobre las opiniones de quién debería ser responsable de la ciberseguridad en el sistema bancario se obtienen dos perspectivas clave (Fig. 4), como resultado de la experiencia de haber sido víctima de fraude hay una clara influencia en la percepción sobre quién debería asumir la responsabilidad de la ciberseguridad en el sector financiero. El resultado permite entender cómo las experiencias personales y las percepciones generales influyen en las opiniones sobre la ciberseguridad bancaria.

Para encontrar la relación entre la edad y haber sido víctima de fraude financiero se utilizó la prueba de Mann-Whitney U dado que no es posible asumir que la distribución de las

edades sea normal, una prueba no paramétrica como Mann-Whitney U resultó apropiada para comparar las distribuciones de edad entre los dos grupos. La edad promedio de las víctimas de fraude financiero es de 23.62 años y la edad promedio de las personas no víctimas de fraude financiero es de 23.02 años. El estadístico U arrojó un valor de 4,290.0 con valor de p igual a 0.12 que al ser mayor que 0.05, significa que no hay evidencia suficiente para rechazar la hipótesis nula de que las distribuciones de edad son iguales entre los que han sido víctimas de fraude financiero y los que no lo han sido. En otras palabras, no se encontró una diferencia estadísticamente significativa en las edades entre las víctimas de fraude financiero y las no víctimas en este conjunto de datos. Aunque la edad promedio es ligeramente mayor en el grupo de víctimas de fraude financiero, esta diferencia no es estadísticamente significativa. Esto sugiere que, aunque puede haber una tendencia, no se podría afirmar con certeza que la edad esté relacionada con ser víctima de fraude financiero basándonos en este conjunto de datos.

Figura 5. Distribución de las edades entre los dos grupos: aquellos que han sido víctimas de fraude financiero y aquellos que no lo han sido.

Se identificaron algunas tendencias en las prácticas de ciberseguridad de los encuestados. La mayoría sigue las recomendaciones de seguridad de su banco, pero también hay un uso significativo de redes públicas y/o abiertas para navegar en internet. Además, la frecuencia de cambio de contraseña y de instalación de actualizaciones del sistema varía entre los encuestados.

La identificación de patrones o tendencias en un conjunto de datos implica analizar las variables y sus relaciones para descubrir información útil o insights. En ese sentido, el análisis de clustering o agrupamiento se utilizó para segmentar los datos en grupos basados en las respuestas a las preguntas relacionadas con las prácticas de ciberseguridad.

Se utilizó el método del codo para determinar un número adecuado de clusters o grupos lo que implica graficar la suma de las distancias al cuadrado de cada punto a su centro asignado para varios valores de k (número de clusters) y buscar el "codo" en la gráfica. En el análisis de clustering se utilizó el modelo no jerárquico K-Means utilizando la librería scikit-learn.

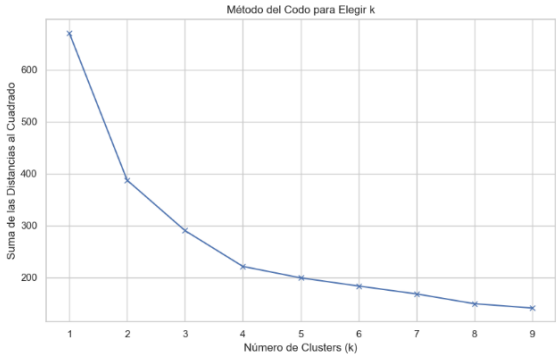

Figura 6. Gráfica del método del codo para determinar el número de clusters k en el método de agrupamiento.

Se observa un cambio significativo en la pendiente de la gráfica en k=4, lo que sugiere que 4 podría ser un buen número de clusters o grupos para este conjunto de datos, la disminución en la suma de las distancias al cuadrado se vuelve más gradual, indicando que añadir más clusters no mejora significativamente la compactación de los datos, por lo que se decidió utilizar 4 para el valor de k.

Se aplicó el análisis de clusters K-Means para identificar patrones o tendencias y que pudieran ayudar a responder las preguntas: ¿Hay diferencias significativas en las prácticas de ciberseguridad entre los clusters?, ¿Cómo varían las características demográficas (edad, sexo) entre los clusters?, ¿Hay una prevalencia de fraude financiero en algunos de los clusters?

Tabla 5. Valores más frecuentes de las respuestas categóricas para cada grupo. Columna A: Frecuencia de cambio de contraseña de la banca en línea. Columna B: Seguir las recomendaciones de seguridad del banco. Columna C: Uso de redes públicas para navegar. Columna D: Frecuencia de instalación de actualizaciones del sistema.

Grupo	A	B	C	D
Grupo 1	Cada año	Si	No	Cada mes
Grupo 2	Otro	Si	No	Cada mes
Grupo 3	Cada año	Si	No	Cada que llegan notificaciones
Grupo 4	Otro	Si	Si	Cada que llegan notificaciones

Todos los grupos tienen una alta tendencia a seguir las recomendaciones de seguridad de sus bancos. Los tres primeros grupos tienden a no usar redes públicas y/o abiertas para navegar en internet, mientras que el Grupo 4 tiene una frecuencia del 50% en uso de redes públicas. El Grupo 1 y el Grupo 2 tienden a cambiar su contraseña de la banca en línea cada año, mientras que los Grupo 3 y 4 tienen una tendencia diferente (categoría "Otro"). Ambos grupos, Grupo 1 y Grupo 2 tienden a instalar actualizaciones del sistema cada mes mientras que los Grupos 3 y 4 lo realizan cada vez que llegan las notificaciones.

Posteriormente se llevó a cabo el análisis de características demográficas y experiencia con fraude financiero en cada

grupo con lo que se obtuvieron los resultados mostrados en la tabla 6.

Basado en las características encontradas en cada subgrupo se pudo definir ciertos rasgos que nos ayudan a perfilarlos, el Grupo 1 es el de usuarios indiferentes pero responsables ya que no que cambian contraseña ni instalan actualizaciones de manera regular, pero si evitan las redes abiertas y siguen las recomendaciones del banco; el Grupo 2 son usuarios jóvenes y moderados debido a que es el grupo donde prevalece una edad más baja de todos los grupos y que siguen las recomendaciones del banco, no se conectan a redes publica e instalan las actualizaciones; el Grupo 3 está conformado por usuarios cautos pero confiados porque instalan actualizaciones, no usan redes publicas y siguen las recomendaciones del banco, pero no cambian de contraseña de manera frecuente. Por último, el Grupo 4 consiente en usuarios precavidos pero arriesgados porque se conectan a redes abiertas a pesar de seguir las recomendaciones del banco e instalar actualizaciones.

Tabla 6. Análisis de las características demográficas H(Hombre), M(Mujer) y experiencia con fraude en los grupos arrojados por el método de K-Means

Grupo	Edad prom.	Dist. de edades	H %	M %	Fraude financiero	
Grupo 1	22.5 años	Dispersas, con una frecuencia significativa de 19,20, 30 y 40 años	71.3	28.7	No 89.6	Si 10.4
Grupo 2	21.87 años	Distribución más concentrada en 20 años	68.4	31.3	89.2	10.8
Grupo 3	24.71 años	Distribución más amplia desde los 20 a los 56 años	65.5	34.5	87.9	12.1
Grupo 4	23.92 años	Distribución más dispersa desde los 19 a los 59 años	66.7	33.3	83.3	16.7

4. Discusión

La elección del muestreo no probabilístico por conveniencia nos permitió realizar este estudio en un periodo corto de tiempo (dos meses), así como reducir los costos de la investigación sin comprometer la viabilidad del trabajo. Asimismo, al ser diseñado con un enfoque transversal del tipo descriptivo, los resultados obtenidos de la encuesta sobre ciberseguridad y fraude financiero proporcionan una perspectiva única sobre las prácticas de seguridad de los usuarios en el contexto del sistema bancario mexicano. La discusión que sigue se basa en la interpretación de estos resultados en relación con los objetivos originales de la investigación, las hipótesis planteadas y su alineación con el conocimiento existente en el ámbito de la ciberseguridad financiera.

La segmentación de los participantes en cuatro grupos principales reveló patrones distintivos en las prácticas de ciberseguridad. Notablemente, aquellos agrupados en el Grupo 4 mostraron una mayor tendencia al uso de redes públicas y abiertas para navegar en internet, lo cual coincide con una ligeramente mayor incidencia de haber sido víctimas de fraude financiero (Chawla, 2022). Esta relación refuerza la noción bien establecida en la literatura de seguridad informática de que las redes no seguras son vectores de amenazas potenciales y pueden incrementar la vulnerabilidad a ataques fraudulentos (Cremer et al., 2022).

En el análisis de las prácticas de ciberseguridad, las características demográficas y la experiencia con fraude financiero en cada uno de los grupos identificados por el algoritmo K-Means. Basados en las respuestas a las preguntas y los grupos generados, se pueden identificar algunas acciones o actividades que podrían aumentar el riesgo de fraude financiero. Es importante tomar en cuenta que estos son patrones observados en los datos y no implican necesariamente una relación causal directa. Las acciones o actividades que podrían aumentar el riesgo de fraude financiero son principalmente el uso de redes públicas y/o abiertas para navegar en Internet: Se observa que el Grupo 4, el cual tiene una mayor prevalencia de haber sido víctima de fraude financiero, tiende a usar redes públicas y/o abiertas para navegar en internet. Este comportamiento puede aumentar el riesgo de exposición a ataques maliciosos y fraude (Cremer et al., 2022).

Contrario a la hipótesis inicial, la frecuencia de cambio de contraseña no mostró una relación directa con la incidencia de fraude financiero en los clusters identificados (Soltani et al., 2023). Sin embargo, la esta nula correlación no significa que por ello no se deba de cambiar la contraseña con cierta frecuencia dado que existen prácticas como el Phising que son usadas para crear bases de datos con todo tipo de información (bancaria, de redes sociales, empresarial, etc.); por lo cual es muy recomendable que a pesar de no ser víctima de fraude se actualicen y/o modifiquen las credenciales de autenticación para mantener prácticas robustas en la gestión de contraseñas, las cuales son ampliamente recomendadas por expertos en seguridad (Maurer & Nelson, 2021).En la frecuencia de cambio de contraseña de la banca en línea que, aunque no se observó una relación clara con el fraude financiero, mantener prácticas seguras de gestión de contraseñas, como cambiarlas regularmente y utilizar contraseñas fuertes, es crucial para la seguridad en línea debido a las filtraciones y/o robo de bases de datos a las instituciones que manejan información financiera directa o indirectamente (Maurer & Nelson, 2021).

Se observa que las víctimas de fraude financiero tienden a ser ligeramente mayores en promedio. Sin embargo, esta diferencia no fue estadísticamente significativa en la muestra. Esto podría deberse a que los adultos mayores tienen un bajo conocimiento en el uso de las TIC’s provocando que los ataques sean más efectivos, caso contrario es el de los jóvenes que suelen estar más conectados por medio del internet volviéndolos más vulnerables. Y dado los resultados que

obtuvimos podríamos dejar esto pendiente para que realizar un trabajo que verifique estas hipótesis.

Dado que no se encontró correlación entre ser víctima de fraude financiero y seguir las recomendaciones de seguridad del banco podríamos decir que los ciberataques se están concentrando en el usuario final a través de ataques de ingeniería social, por ello se debería de realizar una investigación que nos permita profundizar y analizar cuál de ellos es el más utilizado para definir estrategias que nos ayuden a subsanar y mejorar las recomendaciones que los bancos emiten.

Pero como conclusión se recomienda evitar el uso de redes públicas para transacciones financieras o acceder a información sensible, al mismo tiempo es recomendable seguir las recomendaciones de seguridad del banco, aunque la mayoría de los participantes indicaron seguir las recomendaciones de seguridad de su banco, también es importante mantener el software actualizado, asegurándose de instalar actualizaciones del sistema y de las aplicaciones dado que ello puede ayudar a protegerse contra vulnerabilidades de seguridad.

Sorprendentemente, la edad promedio más alta en el Grupo 3 sugiere que puede haber una relación entre la edad y la susceptibilidad al fraude financiero, aunque este hallazgo no fue estadísticamente significativo en el conjunto de datos. Es posible que este resultado sea un artefacto del tamaño de la muestra o de factores no medidos en la encuesta, lo cual subraya la necesidad de una investigación más profunda en esta área.

Los hallazgos respaldan y amplían el conocimiento actual en ciberseguridad, especialmente en el contexto del comportamiento de los usuarios finales (Cremer et al., 2022). El uso predominante de redes inseguras como factor de riesgo destaca la importancia crítica de la conciencia y educación en ciberseguridad (Chawla, 2022). Además, el seguimiento de las recomendaciones de seguridad del banco, que fue una práctica común entre los encuestados, demuestra un nivel de diligencia que debe ser continuamente fomentado (Gotelaere & Paoli, 2022).

La literatura actual en ciberseguridad financiera y comportamiento del consumidor sugiere que las prácticas de seguridad personal son esenciales para mitigar el riesgo de fraude (Cremer et al., 2022; Kannelønning & Katsikas, 2023). Nuestros resultados corroboran estas afirmaciones y sugieren que, aunque los usuarios pueden ser conscientes de las recomendaciones de seguridad, todavía existen brechas en la aplicación constante de estas prácticas, como se evidencia en el uso de redes públicas (Chawla, 2022).

Fomentar la educación y la concienciación sobre ciberseguridad puede ayudar a reducir el riesgo de fraude financiero, especialmente en grupos demográficos más susceptibles (Machín Nieva Gazapo, 2016). Identificar y mitigar los riesgos de fraude financiero es crucial para proteger la seguridad financiera y la información personal (Aguilar Antonio & Aguilar Antonio, 2021). Las prácticas seguras de navegación en internet, junto con la educación y la concienciación sobre ciberseguridad, son componentes clave para reducir estos riesgos (Aguilar Antonio & Aguilar Antonio, 2021; Machín Nieva Gazapo, 2016).

Los análisis sobre los comportamientos de seguridad ofrecen una visión detallada en varios aspectos:

- Frecuencia de Cambio de Contraseñas de Banca en Línea: En el gráfico de la figura 5 se muestra cómo los encuestados varían en la frecuencia con la que cambian sus contraseñas de banca en línea. Esta información es crucial para entender las prácticas de seguridad de contraseña entre los usuarios.

- Uso de Redes Públicas y/o Abiertas para Navegar en Internet: El análisis revela el porcentaje de usuarios que utilizan redes públicas o abiertas para navegar en internet, lo cual es un factor importante en la seguridad en línea.

- Frecuencia de Instalación de Actualizaciones del Sistema: la frecuencia con la que los usuarios instalan actualizaciones del sistema, un comportamiento clave en la protección contra amenazas de seguridad.

5. Conclusiones

Los resultados de este estudio enfatizan la relevancia de las estrategias preventivas en ciberseguridad, tales como evitar redes inseguras y seguir las recomendaciones de seguridad bancaria. Además, resaltan la importancia de la educación continua y la conciencia sobre la ciberseguridad como herramientas cruciales en la lucha contra el fraude financiero. Para fortalecer la seguridad financiera en línea, las instituciones financieras y los responsables de la formulación de políticas deben considerar estos hallazgos y trabajar hacia el fortalecimiento de la infraestructura de seguridad digital y las iniciativas de educación del consumidor.

Dado que una gran mayoría considera la ciberseguridad como muy importante, sería beneficioso implementar programas de educación y conciencia sobre ciberseguridad específicos para usuarios bancarios. Esto podría incluir consejos sobre cómo detectar fraudes, la importancia de actualizar regularmente las contraseñas y el uso seguro de redes públicas.

- Promoción de Buenas Prácticas de Seguridad: Fomentar el cambio regular de contraseñas y el uso de contraseñas más complejas que integren caracteres especiales y alfanuméricos. A pesar de que muchos usuarios no cambian sus contraseñas con frecuencia, educar sobre los riesgos asociados a esto puede fomentar mejores prácticas.

- Uso de Antivirus y Actualizaciones de Seguridad: Animar a los usuarios a instalar y mantener actualizados los programas de antivirus, dada su percepción como eficientes y accesibles. Además, promover la instalación regular de actualizaciones del

sistema, ya que ayudan a proteger contra vulnerabilidades de seguridad.

- Responsabilidad Compartida en Ciberseguridad: Resaltar la importancia de la responsabilidad compartida entre bancos, gobierno y usuarios en la ciberseguridad. Esto puede incluir campañas que muestren cómo cada parte contribuye a un sistema bancario más seguro.

- Enfoque en la Seguridad Móvil y de Computadoras: Ofrecer recomendaciones sobre seguridad en dispositivos móviles y computadoras, especialmente considerando que muchos usuarios renuevan sus dispositivos cada 12 a 18 meses. Esto podría incluir el uso seguro de aplicaciones bancarias y la protección de dispositivos con contraseñas o autenticación biométrica.

- Alertas y Recomendaciones de Seguridad del Banco: Aprovechar el hecho de que la mayoría sigue las recomendaciones de seguridad de su banco para proporcionar consejos frecuentes y actualizados sobre ciberseguridad. Asimismo, se recomienda atenderlas de manera pronta para evitar que hagan un daño mayor.

- Investigación y Desarrollo de Seguridad: Para bancos y entidades gubernamentales, es crucial seguir invirtiendo en tecnologías de seguridad y en investigaciones para mantenerse al día con las amenazas cambiantes en ciberseguridad.

Estas sugerencias pueden ayudar a mejorar la seguridad general y la conciencia sobre ciberseguridad entre los usuarios bancarios. Es vital que tanto las instituciones bancarias como los usuarios trabajen juntos para garantizar un entorno seguro y protegido.

Mientras que este estudio proporciona una visión valiosa de las prácticas de ciberseguridad, también reconoce las limitaciones inherentes a la naturaleza auto informada de los datos y el alcance del análisis. Investigaciones futuras deberían buscar expandir la muestra y considerar el análisis longitudinal para observar cómo evolucionan las prácticas de ciberseguridad y su impacto en la incidencia del fraude financiero a lo largo del tiempo.

6. Agradecimientos

Los autores agradecen al editor y a los revisores por sus valiosos comentarios y sus sugerencias que permiten mejorar esta investigación significativamente. Los autores reconocen y agradecen el apoyo otorgado por la Universidad Rosario Castellanos, así como al Tecnológico de Estudios Superiores de Ecatepec por permitirnos la aplicación de la encuesta y facilitarnos el tiempo para el desarrollo de este proyecto de investigación.

7. Referencias

Admati, A. R. (2014). The Compelling Case for Stronger and More Effective Leverage Regulation in Banking. The Journal of Legal Studies, 43(S2), S35–S61. https://doi.org/10.1086/677557

Aguilar Antonio, J. M., & Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales (Santiago), 53(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Camhaji, E. (2018, May 18). El mayor ciberatraco en la historia de México mantiene en vilo al sistema bancario | Economía | EL PAÍS. El País. https://elpais.com/economia/2018/05/18/actualidad/1526663135_029795.html

Capeta Mondoñedo, F. S., Franco Del Carpio, C. M., & Villafuerte Barreto, H. O. (2023). Ciberseguridad y su relación con la empleabilidad para egresados de Ingeniería de Sistemas en una Universidad Pública. Revista de Climatología, 23, 1510–1519. https://doi.org/10.59427/rcli/2023/v23cs.1510-1519

Chawla, V. (2022, March 16). A Unified Response to Cyberattacks, Fraud and Financial Crime. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/a-unified-response-to-cyberattacks-fraud-crime

Cisneros Zepeda, D. S. (2021). Los efectos del crédito bancario otorgado a la industria y al consumo en el crecimiento económico: evidencia de México, 1994-2017. Revista Mexicana de Economía y Finanzas, 17(2), 1–25. https://doi.org/10.21919/remef.v17i2.560

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice 2022 47:3, 47(3), 698–736. https://doi.org/10.1057/S41288-022-00266-6

Gavilanes L, M. J., Aucatoma, K., Moreno Piedrahita, F., & Rivas, A. (2021). La cultura de seguridad del paciente como estrategia para evitar errores médicos. Mediciencias UTA, 5(3), 2. https://doi.org/10.31243/mdc.uta.v5i3.1189.2021

Gotelaere, S., & Paoli, L. (2022). Prevention and Control of Financial Fraud: a Scoping Review. European Journal on Criminal Policy and Research, 1–21. https://doi.org/10.1007/S10610-022-09532-8/METRICS

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., Jaramillo-Flores, P. del C., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). Phishing attacks and how to prevent them. Iberian Conference on Information Systems and Technologies, CISTI, 2022-June. https://doi.org/10.23919/CISTI54924.2022.9820161

Juárez, G. S. (2017). Análisis De Contagio en El Sistema Financiero Mexicano Combinando El Modelo De Merton Y Redes Aleatorias. Contaduría Y Administración. https://doi.org/10.1016/j.cya.2016.10.006

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. Information and Computer Security, 31(4), 463–477. https://doi.org/10.1108/ICS-08-2022-0139/FULL/PDF

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingenieria de Software, 3(4), 161. https://doi.org/10.18294/relais.2015.161-176

Machín Nieva Gazapo, M. (2016). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA. Revista UNISCI. https://www.redalyc.org/articulo.oa?id=76747805002

Manssur Nicola, A. (2023). Autenticación multifactor, el nuevo “imperativo” en ciberseguridad - TintaTIC. https://tintatic.com/autenticacion-multifactor-el-nuevo-imperativo-en-ciberseguridad/

Maurer, T., & Nelson, A. (2021). Cyber threats to the financial system are growing, and the global community must cooperate to protect it GLOBAL CYBER THREAT. Finance and Development. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk

Moran-Fuentes, J. J., Carlos-Ornelas, C. E., & Soto-Morones, H. (2022). Prácticas De Gestión De Seguridad Y Salud en El Trabajo: Una Revisión

Sistemática De La Literatura. Ciencias Administrativas Teoría Y Praxis. https://doi.org/10.46443/catyp.v18i1.304

Negro, P., & Pons, C. (2022). Artificial Intelligence techniques based on the integration of symbolic logic and deep neural networks: A systematic review of the literature. Inteligencia Artificial, 25(69), 13–41. https://doi.org/10.4114/intartif.vol25iss69pp13-41

Poveda, M. U. (2020). Riesgo De Crédito: Evidencia en El Sistema Bancario Ecuatoriano. Bolentín De Coyuntura. https://doi.org/10.31164/bcoyu.23.2019.842

Quintero Peña, J. W., & Mejía Baños, M. A. (2021). Factores asociados a la adopción de la banca electrónica en México. Revista Mexicana de Economía y Finanzas, 17(2), 1–23. https://doi.org/10.21919/remef.v17i2.659

Realpe, M. E., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. In Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020. Universidad del Rosario. https://doi.org/10.12804/si9789587844337.10

Redacción. (2018, May 18). México: el ciberataque “sin precedentes” a los bancos del país que causó pérdidas millonarias - BBC News Mundo. BBC Mundo. https://www.bbc.com/mundo/noticias-america-latina-44130887

Riveros, A. (2020, June 29). Qué es la criptografía y por qué es útil en Ciberseguridad. EALDE Business School. https://www.ealde.es/que-es-criptografia/

Rodríguez, J. (2017, March 21). Cómo usar la tecnología aplicada para prevenir riesgos. Forbes México. https://www.forbes.com.mx/tecnologia-aplicada-para-prevenir-riesgos/

Sastré, A. (2022). La ciberseguridad debe planearse desde el comportamiento del usuario. Expansión. https://expansion.mx/opinion/2022/04/23/ciberseguridad-planearse-desde-comportamiento-usuario

Soltani, M., Kythreotis, A., & Roshanpoor, A. (2023). Two decades of financial statement fraud detection literature review; combination of bibliometric analysis and topic modeling approach. Journal of Financial Crime. https://doi.org/10.1108/JFC-09-2022-0227

Trillo del Pozo, D., & Alonso Gallo, N. (2021). La banca pública como instrumento de estabilización en la crisis del COVID-19. Papeles de Europa, 33(2), 79–90. https://doi.org/10.5209/pade.76523

Varchetta, M., Fraschetti, A., Mari, E., & Giannini, A. M. (2020). Adicción a redes sociales, Miedo a perderse experiencias (FOMO) y Vulnerabilidad en línea en estudiantes universitarios. Revista Digital de Investigación En Docencia Universitaria, 14(1), e1187. https://doi.org/10.19083/ridu.2020.1187

White, G., & Lee, J. H. (2021, June 24). El “impactante” atraco del Grupo Lázaro, el equipo de élite de Corea del Norte que casi roba US$1.000 millones en un solo asalto - BBC News Mundo. BBC News. https://www.bbc.com/mundo/noticias-internacional-57562592