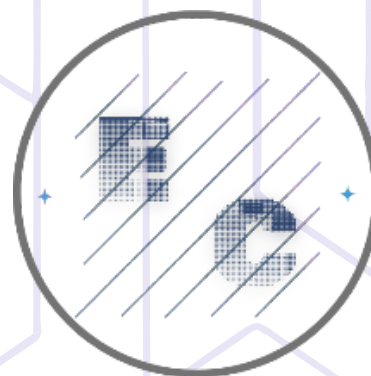
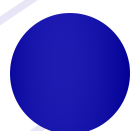
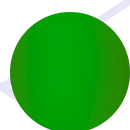




REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS



Universidad de Sonsonate



Volumen 3, Número 3



Julio - Septiembre, 2026
Edición Especial

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3
Julio-Septiembre 2026
Edición Especial

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

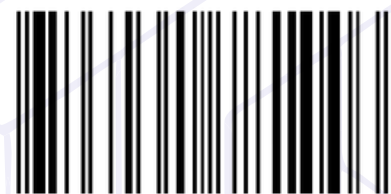
Contacto principal: admin@omniscens.com

Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación

Se autoriza la reproducción total o parcial del contenido de la publicación sin previa autorización de la Revista Multidisciplinar Epistemología de las Ciencias siempre y cuando se cite la fuente completa y su dirección electrónica.



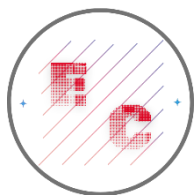
Copyright © 2026: Los autores



9773061781003

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 3, Núm. 3, julio-septiembre 2026, edición especial, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: <https://www.omniscens.com>, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 julio 2026.



Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3, 2026, julio-septiembre, Edición Especial

DOI: <https://doi.org/10.71112/keqj1809>

**COMPRENDIENDO LAS FINTECH: TECNOLOGÍA, COMERCIO ELECTRÓNICO Y
SEGURIDAD**

**UNDERSTANDING FINTECH: TECHNOLOGY, E-COMMERCE, AND DIGITAL
SECURITY**

Niza Lucero Alpizar Martínez

María de Lourdes Lopez García

México

Comprendiendo las Fintech: tecnología, comercio electrónico y seguridad

Understanding Fintech: technology, e-commerce, and digital security

Niza Lucero Alpizar Martínez^{a,*}

niza_am@tesch.edu.mx

<https://orcid.org/0009-0009-8161-5835>

María de Lourdes Lopez García^a

contacto@heliosdigital.com.mx

<https://orcid.org/0000-0002-3011-3888>

*Autor de correspondencia: niza_am@tesch.edu.mx, ^aTecnológico de Estudios Superiores de Chalco, México

RESUMEN

En la era actual, la tecnología ha transformado profundamente la vida cotidiana de individuos y empresas. Herramientas como teléfonos inteligentes, computadoras y tabletas permiten realizar pagos, solicitar créditos, obtener asesoramiento financiero y automatizar múltiples procesos comerciales. La pandemia de COVID-19 aceleró la adopción de servicios financieros digitales, impulsando la transformación tecnológica en tiempo récord. En este contexto, surgieron las empresas Fintech, actores clave que combinan innovación y tecnología para ofrecer soluciones financieras más accesibles, eficientes y personalizadas. Estas organizaciones no solo redefinen la relación entre consumidores e instituciones financieras, sino que también generan nuevas oportunidades y retos para la economía global.

Palabras clave: Fintech; Tecnología; Innovación; Financiera.

ABSTRACT

Today, technology has greatly changed the everyday lives of people and businesses. Smartphones, computers, and tablets now make it easy to make payments, apply for loans, get financial advice, and automate many business tasks. The COVID-19 pandemic sped up the use of digital financial services, pushing technological change faster than ever before. In this setting, Fintech companies appeared as key players, using innovation and technology to offer financial solutions that are more accessible, efficient, and personalized. These companies not only change how consumers and financial institutions interact but also create new opportunities and challenges for the global economy.

Keywords: Fintech; Technology; Financial; Innovation.

Recibido: 18 febrero 2026 | Aceptado: 19 julio 2026 | Publicado: 20 julio 2026

INTRODUCCIÓN

Con el avance de la tecnología, se han destapado nuevas herramientas para el uso de actividades cotidianas como lo son los servicios financieros. En los últimos años ha resonado en el mundo de la tecnología el término Fintech, por sus siglas en inglés (Financial Technologies), que se refiere a soluciones financieras propiciadas por la tecnología. A lo largo de su historia, las Fintech han evolucionado en tres etapas principales. La primera de ellas, se denomina Fintech 1.0 que estaba soportada por infraestructura tecnológica cableada, sigue la era de las Fintech 2.0 que vivió el cambio de la era digital en las telecomunicaciones y desarrolló de los servicios financieros digitales tradicionales. Finalmente, las Fintech 3.0, la tercera era que no se define por los productos o servicios que se ofertan, es más bien, por las entidades que los ofrecen (Bancomext, 2018).

Las empresas Fintech con ayuda de la tecnología brindan servicios financieros de manera ágil, cómoda y segura. Estos servicios abarcan áreas como medios de pago, transferencias, infraestructura para servicios financieros, soluciones financieras para empresas, finanzas personales y asesoría, financiamiento alternativo, criptomonedas y *blockchain* (Rodríguez y Morales, 2018).

Las Fintech promueven la inclusión financiera, gracias al uso de la tecnología pueden llegar a diversos sectores de la población que están excluidos de los servicios financieros tradicionales. Sin embargo, es importante cuestionar la seguridad que ofrecen estas empresas, puesto que, al ofrecer servicios financieros, manejan gran cantidad de información que debe ser protegida. En este sentido, la seguridad de la información a través de los protocolos criptográficos debe ser aplicada. En este artículo, se propone un protocolo de seguridad que usa herramientas criptográficas como las funciones Hash, las firmas digitales RSA y el cifrador por bloques AES, para proteger la información en una empresa que trabaja con monedero electrónico.

METODOLOGÍA

Regulación de las FINTECH

Las empresas Fintech están reguladas por la Ley Fintech, publicada en el 2018 que tiene como objetivo regular los servicios financieros, su funcionamiento, organización y operación. Con esta ley, las Fintech son más seguras para sus clientes, por supuesto, cada país tiene sus propias leyes regulatorias. En México, las empresas reguladas se clasifican de la siguiente manera (CONDUSEF, 2020):

- 1) Instituciones de Financiamiento Colectivo (crowdfunding): usan una plataforma para tener contacto a inversionistas con solicitantes. Al ser colectivo, distintas personas

contribuyen con aportaciones (pequeñas o grandes) para financiar algún proyecto, que puede subclasificarse como colectivo de deuda, de capital o de copropiedad.

- 2) Instituciones de fondo de pago electrónico (monederos electrónicos): se utilizan para realizar pagos, transferencias electrónicas o domiciliaciones.

Respecto al monedero electrónico, sus principales regulaciones son (CONDUSEF, 2018):

- Uso de monedas nacionales, extranjeras o activos virtuales como criptomonedas.
- Goce de liquidez inmediata sin generar cargos a los clientes.
- Registro de operaciones por cliente.

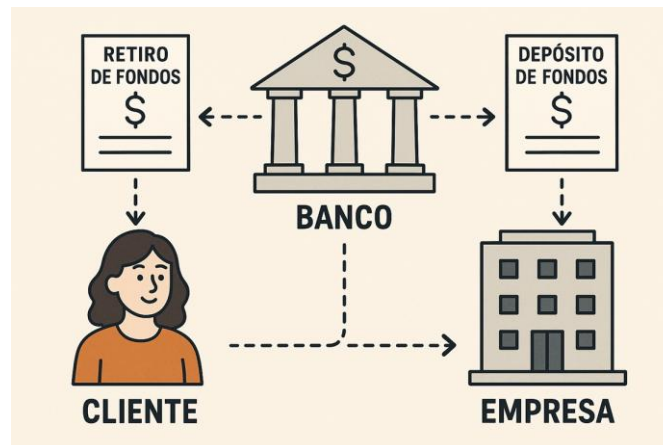
México se consolidó como un país pionero en la normatividad para las Fintech, buscando la confianza de los usuarios en servicios financieros. La tecnología es utilizada para agilizar los procesos financieros, no obstante, los riesgos en esta era digital son altos. Los ciberdelincuentes ejecutan ataques sofisticados como la suplantación de la identidad con gran facilidad por los huecos de seguridad, por lo cual, los expertos en ciberseguridad recomiendan distintas soluciones para la prevención y protección de la Fintech (Infosecurity México). Es fundamental realizar pruebas con versiones preliminares (beta) de la aplicación móvil antes de su lanzamiento oficial. Esto permite identificar y corregir posibles errores, asegurando un mejor funcionamiento en su versión final. Asimismo, toda aplicación debe contar con un sistema de autenticación de usuarios que utilice contraseñas seguras, con el fin de prevenir accesos no autorizados y proteger contra posibles ataques cibernéticos. En este sentido, el cifrado de datos representa un elemento clave, ya que la información transmitida por internet debe llegar de forma segura a su destino, evitando que sea interceptada, clonada o comprometida. El algoritmo de cifrado más utilizado para este propósito es el AES (Advanced Encryption Standard).

Tanto las aplicaciones móviles como las plataformas web deben incorporar mecanismos que detecten y bloqueen automáticamente actividades sospechosas o provenientes de fuentes poco confiables. Además, la implementación de la norma ISO 27001 es altamente recomendable, ya que garantiza una gestión adecuada de la seguridad de la información, generando confianza en los usuarios sobre la protección de sus datos. Cierta información sensible requiere un nivel de seguridad más elevado para evitar su pérdida o robo. Dado que la información es un recurso esencial en el funcionamiento de los sistemas y aplicaciones tecnológicas, es crucial realizar respaldos periódicos, capacitar al personal en la prevención y respuesta ante incidentes de ciberseguridad, y minimizar al máximo el riesgo de pérdida de datos. Del mismo modo, el usuario final debe tener acceso a su información y tomar las medidas necesarias para resguardarla adecuadamente (Alpízar Martínez, 2023).

Según la ISO, el comercio electrónico es la actividad de vender o comprar productos en las redes abiertas (International Organization for Standardization, 2015). De tal manera, que se puede entender como la interacción e intercambio de diferentes productos, servicios e información, a través de los medios tecnológicos entre empresas y clientes, haciendo uso de la Internet. Existe una relación de interdependencia de las empresas Fintech con el comercio electrónico que de alguna manera ha transformado la forma en que las personas, compran, pagan y acceden a los servicios financieros con la era digital. El comercio electrónico requiere de métodos seguros para reducir fraudes. En la Figura 1 se muestran las entidades y la comunicación que se tiene entre ellas.

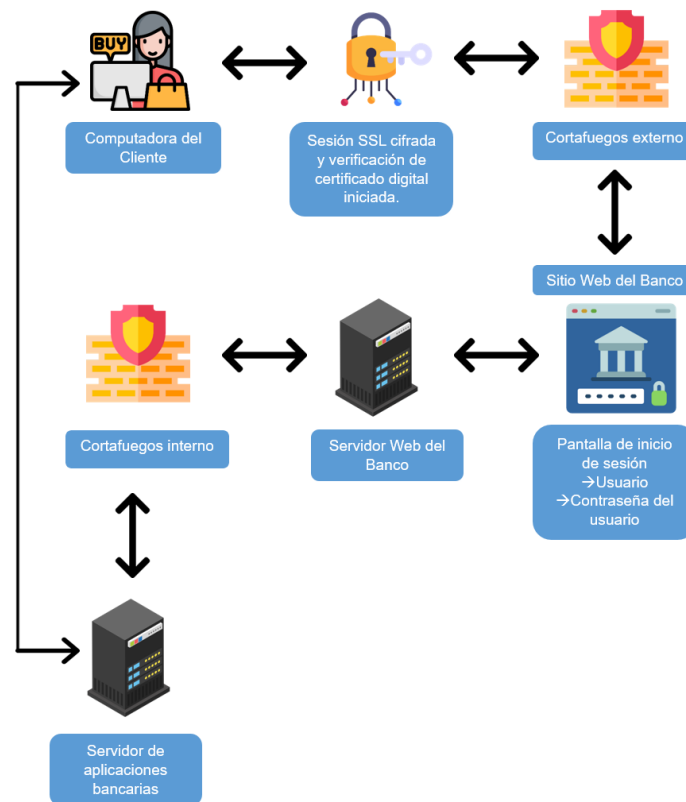
Figura 1

Funcionamiento de las transacciones electrónicas.



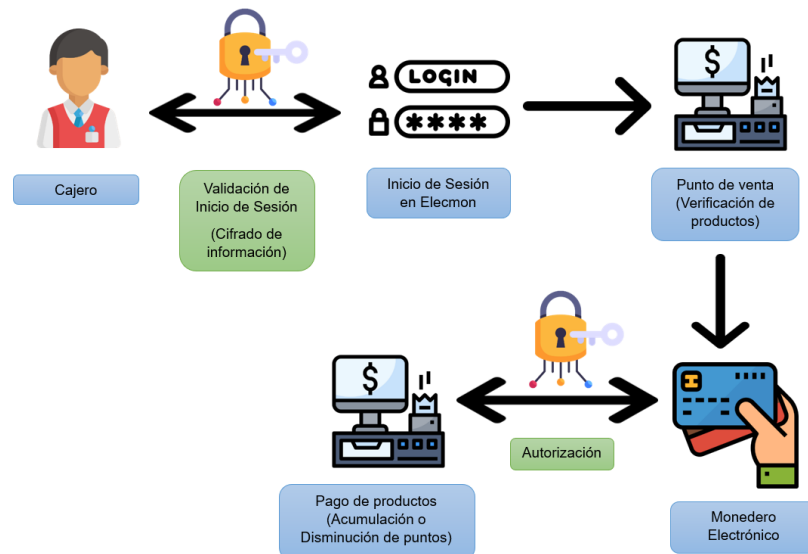
En una transacción en línea intervienen tres actores principales: el cliente, la empresa y el banco. El cliente selecciona productos o servicios, ingresa sus datos bancarios (nombre, número de tarjeta, CVV y fecha de vencimiento) y el sistema valida la información para aprobar o rechazar el pago. Una vez autorizado, el monto se descuenta de la cuenta del cliente y se abona a la de la empresa. Actualmente, también se emplean tarjetas digitales con CVV dinámico, que ofrecen mayor seguridad. Para proteger la información, las operaciones utilizan protocolos como SSL/TLS, los cuales cifran los datos y generan confianza en el usuario.

Cuando se realiza una transacción por la Internet se utilizan diversos protocolos de seguridad, el más utilizado es el protocolo SSL/TLS, la función principal es proteger la información que viaja en el navegador y producir confianza en el usuario. En la Figura 2 se muestra la seguridad al momento de realizar una transacción bancaria.

Figura 2*Seguridad en las transacciones bancarias*

Al analizar el funcionamiento de las transacciones electrónicas es imperativo utilizar herramientas criptográficas que permitan mantener la seguridad de la información. En ese sentido, el monedero electrónico es utilizado como herramienta de pago que puede ser como transferencia, pagos con tarjeta en línea o en efectivo a través de líneas de referencia.

Es importante tener en cuenta la diferencia entre el comercio electrónico y el monedero electrónico, el primero es una actividad comercial usando plataformas digitales como páginas web o aplicaciones móviles, mientras que la segunda es una tienda en línea. La Figura 3, muestra el flujo de información entre las entidades que forman la plataforma de comercio electrónico y cómo se encuentran inmersas las funciones del monedero electrónico.

Figura 3*Funcionalidad de un escenario de Comercio Electrónico*

El protocolo criptográfico consiste en proteger la información que fluye entre las entidades. La Figura 4 muestra un ejemplo de las operaciones que realiza un protocolo criptográfico para una empresa ficticia denominada FinPap que cumple el flujo de información de la Figura 3. En una fase inicial de registro, la información del cliente y de su monedero electrónico se almacenan cifrados en la base de datos. Cuando el cliente realiza una compra o un canje de puntos, y desea actualizar su monedero, debe proporcionar el código generado en el registro.

Figura 4*Protocolo criptográfico para la empresa ficticia FinPap*

Registro	
Servidor (d_s, e_s, n_s)	Punto de venta (e_s, n_s) $h = \text{Hash}(NIP)$ $m = ME h$ $c = m^{e_s} \bmod n_s$
$\leftarrow c \leftarrow$	
$m' = c^{d_s} \bmod n_s$ $m' = ME h$ $CS = n \in \mathbb{Z}_{n_s}^+$ $k = \text{Hash}(CS)$ $c_{ME} = \text{AES}_C(k, ME h)$	
Actualización	
$ME = \text{Monedero Electrónico}$	
$c = (ME \text{Hash}(NIP) \text{saldo})^{e_s} \bmod n_s$	
$\leftarrow c \leftarrow$	
$m' = c^{d_s} \bmod n_s$ $m' = ME \text{Hash}(NIP) \text{saldo}$ $\text{msg} = \text{AES}_D(k, c_{ME})$ $\text{msg} = (ME h)$ Si h es igual a $\text{Hash}(NIP)$ → Msj ok Si no → Msj declinado	

Esta información viaja cifrada hasta el servidor, donde se descifra y se valida que el código coincida con el original. Si la verificación es correcta, se realiza la actualización; en caso contrario, la operación se rechaza.

RESULTADOS

Para garantizar el correcto funcionamiento del protocolo criptográfico se implementó el sistema de comercio electrónico denominado Elecmon que consta de cuatro módulos:

- 1) Registro producto: el cajero almacena la información del producto, hecho que produce la actualización el inventario.
- 2) Compra producto: el cajero indica el nombre o la clave del producto con la finalidad de ser agregado a la compra.
- 3) Gestiona monedero: el sistema registra/actualiza/elimina un monedero electrónico, el cliente puede tener uno o varios monederos.

4) Autoriza compra: el cliente autoriza la compra a través de los cuatro dígitos de seguridad, únicamente para utilizar los puntos en su monedero electrónico.

5) Seguridad: este módulo se encarga de cifrar y descifrar la información en las transacciones entre entidades.

En general, el funcionamiento del protocolo en el sistema es el siguiente. El cifrado comienza en el inicio de sesión, cuando se da de alta un nuevo monedero electrónico y al momento en el que el cliente autoriza su compra, sin embargo, el sistema también solicita la clave de autorización del cajero para continuar y finalizar la compra. El cliente se encarga de autorizar su compra mediante un número de seguridad de 4 dígitos, información que también es cifrada en el módulo de seguridad y queda lista para viajar de una entidad a otra.

Las operaciones van en orden, por lo que, al estar en el punto de venta, se busca el producto mediante su clave y se agrega a la lista colocando la cantidad requerida. Una vez agregados los productos por el cajero, el sistema realiza el cálculo del monto y solicita el monedero electrónico del cliente, con la finalidad de acumular o utilizar sus puntos. El cajero, introduce el número de monedero electrónico, se consulta en la base de datos y pasa al módulo de seguridad para ser cifrado. Para autorizar la compra, el cliente tiene el NIP (Código de seguridad) del monedero electrónico. El cajero solicita al cliente la autorización mediante teclado. El cliente ingresa el código de seguridad. Finalmente, se verifica la información y se hace la acumulación o disminución de puntos, cumpliendo así, los servicios de seguridad de integridad, confidencialidad y autenticación.

DISCUSIÓN

La tecnología ha permitido una transformación en el sector financiero, ofreciendo así, a las empresas Fintech. Actualmente, esta combinación de innovación digital y servicios financieros está al alcance de cualquier persona, al tener la posibilidad de desarrollar una aplicación o plataforma de comercio electrónico que facilite pagos, créditos o inversiones. Esta facilidad, plantea retos en materia de seguridad, en varios ámbitos, el primero de ellos es la regulación de operaciones para una empresa Fintech, que cumpla con lo estipulado en la ley para la protección, principalmente, del cliente; y segundo, la seguridad de la información, que exige aplicar herramientas criptográficas para proteger las transacciones, por ejemplo, en aplicaciones de monedero electrónico.

CONCLUSIONES

En resumen, el surgimiento de empresas Fintech abre la puerta a cualquier emprendedor para participar en el ámbito financiero, utilizando herramientas digitales. En este artículo, se presentó un sistema de comercio electrónico que opera con un protocolo de seguridad para el monedero electrónico que permite proteger la información del cliente y mantiene el resguardo de la información tanto en su almacenamiento como en su consulta y actualización, comprobando así, que es posible innovar en esta área financiera, aunque siguen siendo necesarios marcos regulatorios sólidos y una cultura digital responsable para aprovechar todo su potencial de manera segura y sostenible.

Declaración de conflicto de interés

Los autores declaran no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría

Niza Lucero Alpizar Martínez desarrolló las ideas principales del estudio, administró la información para su análisis, diseñó el sistema usando la metodología PUDS (Proceso Unificado de Desarrollo de Software), implementó el sistema y el protocolo criptográfico, así como, validó el software y redactó el manuscrito.

María de Lourdes López García, generó las ideas principales del estudio, supervisó y verificó el diseño del protocolo de seguridad, del sistema de comercio electrónico y la implementación del monedero electrónico. Realizó una revisión y corrección de la versión final del artículo.

Declaración de uso de inteligencia artificial

Los autores declaran que utilizaron la inteligencia artificial como apoyo para este artículo, y también que esta herramienta no sustituye de ninguna manera la tarea o proceso intelectual. Después de rigurosas revisiones con diferentes herramientas en la que se comprobó que no existe plagio como constan en las evidencias, los autores manifiestan y reconocen que este trabajo fue producto de un trabajo intelectual propio, que no ha sido escrito ni publicado en ninguna plataforma electrónica o de IA.

REFERENCIAS

- Alpízar Martínez, N. L. (2023). Desarrollo de un protocolo criptográfico para empresas financiero tecnológicas (Tesis de maestría). Universidad Autónoma del Estado de México. <https://ri.uaemex.mx/handle/20.500.11799/140239>
- Banco Nacional de Comercio Exterior (Bancomext). (2018). Fintech en el mundo. [<https://www.bancomext.com/wp-content/uploads/2018/11/Libro-Fintech.pdf>]
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2018, noviembre). El ABC de la Ley Fintech. Revista Proteja su Dinero. <https://revista.condusef.gob.mx/usuario-inteligente/ponlo-en-la-balanza/2018/11/el-abc-de-la-ley-fintech/>
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2020, agosto). Fintech: nuevas instituciones financieras. Revista Proteja su Dinero. <https://revista.condusef.gob.mx/usuario-inteligente/ponlo-en-la-balanza/2020/08/fintech-nuevas-instituciones-financieras/>
- Infosecurity Mexico. Estrategias de ciberseguridad en fintech. Infosecurity Mexico, 2020.
- International Organization for Standardization. (2015). ISO 32110:2015 — Information technology — Software quality management — Requirements for software quality evaluation (ISO Standard No. 32110:2015). <https://www.iso.org/standard/62179.html>
- Morales Rodríguez, M. V., & Rodríguez Suárez, J. S. (2018). México: Nación Fintech-Ethic. ProMéxico. <http://ethic.com.mx/docs/estudios/Mexico-Nacion-Fintech.pdf>