Transformación Digital
Agencia de Transformación Digital y Telecomunicaciones

INFOTEC

Biblioteca INFOTEC

Ciudad de México, a 19 de febrero de 2025

VISTO BUENO DE TRABAJO TERMINAL

Maestría en Dirección Estratégica de las Tecnologías de Información y Comunicación (MDETIC)

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Recomendaciones de ciberseguridad para cumplir con la ley para regular las instituciones de tecnología financiera"

Desarrollado por el alumno: **Jesús Robert Hurtado**, bajo la modalidad del **Diplomado en Derecho, TIC e Innovación del INFOTEC**, cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para la entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

Jah

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Jesús Robert Hurtado. – Alumno de la Maestría en Dirección Estratégica de las Tecnologías de Información y Comunicación. – Para su conocimiento.

2025 Año de La Mujer Indígena

MDETIC

MAESTRÍA EN DIRECCIÓN ESTRATÉGICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“Recomendaciones de ciberseguridad para cumplir con la Ley para Regular las Instituciones de Tecnología Financiera”

Bajo la modalidad de Diplomado
Que para obtener el grado de MAESTRO EN DIRECCIÓN ESTRATÉGICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Jesús Robert Hurtado

Ciudad de México, Noviembre, 2024.

CONACYT

INFOTEC POSGRADOS

Recomendaciones de ciberseguridad para cumplir con la Ley para Regular las Instituciones de Tecnología Financiera

Cybersecurity recommendations to comply with the Law to Regulate Financial Technology Institutions

Jesus Robert Hurtado[1*]

RESUMEN

LA TECNOLOGÍA AVANZA A GRAN VELOCIDAD AL IGUAL QUE LOS RIESGOS Y AMENAZAS ALREDEDOR DE ESTA, LOS CUALES CAUSAN UN MAYOR IMPACTO EN LAS OPERACIONES DE LAS EMPRESAS. CUALQUIER EMPRESA REQUIERE YA DE UNA POSTURA EN CIBERSEGURIDAD, DE LA CUAL DERIVE UNA ESTRATEGIA ALINEADA A SUS NECESIDADES, PRESUPUESTOS Y OBJETIVOS.

EN MÉXICO, LAS EMPRESAS FINTECH ADEMÁS DE ESTAR PROTEGIDAS DEBEN DE CUMPLIR CON LA REGULACIÓN EXISTENTE. PARA MUCHAS EMPRESAS ESTO PUEDE REPRESENTAR UN RETO YA QUE POR UN LADO DEBEN DE PROTEGER EL ACTIVO MÁS IMPORTANTE QUE TIENEN QUE

ABSTRACT

Technology is advancing at a rapid pace, as are the risks and threats surrounding it, which have a greater impact on company operations. Any company now requires a cybersecurity posture, from which it derives a strategy aligned with its needs, budgets and objectives.

In Mexico, FinTech companies, in addition to being protected, must comply with existing regulations. For many companies, this can represent a challenge since, on the one hand, they must protect the most important asset they have, which is information, and on the other, comply with the Law. Therefore, this work aims to analyze what the Law states and, based on the NIST Cybersecurity Framework, comply with cybersecurity requirements.

Concepts related to cybersecurity are described as part of the context. The NIST Cybersecurity Framework is taken as a reference since it is used by

[1*] Maestría en Dirección Estratégica de las Tecnologías de la Información y Comunicación (INFOTEC). Correo electrónico: robert123086@gmail.com

ES LA INFORMACIÓN, Y POR OTRO, CUMPLIR CON LA LEY. POR LO TANTO, ESTE TRABAJO TIENE EL OBJETIVO DE ANALIZAR LO QUE MARCA LA LEY Y CON BASE EN EL MARCO DE CIBERSEGURIDAD DEL NIST DAR CUMPLIMIENTO A LOS REQUISITOS DE CIBERSEGURIDAD.

SE DESCRIBEN CONCEPTOS RELACIONADOS CON LA CIBERSEGURIDAD COMO PARTE DEL CONTEXTO. SE TOMA COMO REFERENCIA EL MARCO DE CIBERSEGURIDAD DEL NIST YA QUE ESTE ES UTILIZADO POR DIVERSAS ORGANIZACIONES GUBERNAMENTALES Y PRIVADAS EN ESTADOS UNIDOS Y EN EL MUNDO Y SOLO ES UNA REFERENCIA PARA DEMOSTRAR PORQUE ES IMPORTANTE APEGARSE A UN MARCO DE CIBERSEGURIDAD.

PALABRAS CLAVE: FinTech, Marco de Ciberseguridad, NIST, Ley.

various government and private organizations in the United States and around the world and is only a reference to demonstrate why it is important to adhere to a Cybersecurity Framework.

KEYWORDS: FinTech, Cybersecurity Framework, NIST, Law

Introducción

La ciberseguridad se ha convertido en algo necesario para las personas y para las empresas debido a la evolución constante de atacantes, riesgos y tecnología. Aunado a esto, existen diferentes regulaciones que ya piden un nivel de madurez para que las empresas puedan operar. Uno ejemplo de esto aplica a las empresas FinTech en México, donde deben de cumplir una serie de requisitos para poder tener autorización por parte de las autoridades para poder prestar servicios a los usuarios, garantizando siempre la protección de su información.

El objetivo de este proyecto está en entender lo que marca la Ley para Regular las Instituciones de Tecnología Financiera; también conocida como Ley Fintech, en materia de ciberseguridad, analizarla y con base en el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés), hacer recomendaciones para dar cumplimiento y robustecer la seguridad de las empresas FinTech en México. Hoy en día las empresas de tecnología financiera enfrentan retos importantes en términos de ciberseguridad. De acuerdo con datos del Financiero (2024), el 38% de las empresas Fintech carece de una estrategia en ciberseguridad.

A nivel mundial, el sector Fintech en el mundo ha ido en aumento, así como los ciberataques. Según el informe FinTech Global Vision 2023 (Finnovating, 2023), Estados Unidos, es el país con mayor número de Fintech, seguido por Reino Unido, India y Canadá. México ocupa el lugar número 9 con 773 nacionales y alrededor de 217 extranjeras. Para todas las empresas es importante contar con una estrategia de ciberseguridad, entender los riesgos alrededor de su negocio y cumplir con las regulaciones marcadas por la Ley. A pesar de que existen diferentes tipos de Fintech, la Ley para Regular las IFT (LRITF) solo se enfoca en dos tipos: instituciones de financiamiento colectivo y las instituciones de fondos de pago electrónico. De conformidad con el Reporte de Estabilidad Financiera del Banco de México (2022), las empresas Fintech que no se encuentran reguladas por esta Ley, si lo están por Leyes Federales aplicables en el ámbito que les corresponde. El Reporte de Estabilidad Financiera de Banxico (2024), señala que

el ritmo de regulación ha sido menor al año anterior, con sólo 5.6% de las Fintech en proceso de obtener una licencia como IFC (Instituciones de Financiamiento Colectivo) o IFPE (Instituciones de Fondos de Pago Electrónico). Por otro lado, el 9.9% se encuentra en trámites para operar bajo otra licencia de entidad regulada (banco, casa de bolsa, aseguradora, Sofom, Sofipo, etc.).

Los segmentos de empresas Fintech identificadas en México de acuerdo con el Reporte de Estabilidad Financiera del Banco de México (2022) son:

Préstamos: Uso de tecnología para el otorgamiento de créditos mayoristas, minoristas y entre pares, mediante análisis de datos.

Pagos y Remesas: Uso de tecnología para realizar transferencias nacionales, internacionales y de remesas.

Empresas de Tecnologías para Instituciones Financieras: Proveer soluciones tecnológicas para las instituciones financieras (seguridad, contratos, chatbots, gestión de riesgos, prevención y fraude, etc.)

Gestión de Finanzas Empresariales: Soluciones enfocadas a las tecnologías de facturación electrónica, contabilidad digital, gestión financiera, inteligencia de negocio y cobranza.

Bienestar Financiero: Plataformas de comparación y gestión de deuda, educación financiera y recomendaciones de ahorro e inversión basadas en datos personales.

Seguros: Plataformas para la provisión o comparación de seguros, aseguradoras digitales y soluciones tecnológicas para aseguradoras.

Banca Digital: Aplicaciones de banca empresarial y banca de consumo.

Servicios para Bienes Raíces: Compra o renta de bienes raíces, financiamiento colectivo para bienes raíces y soluciones tecnológicas para bienes raíces.

Finanzas Abiertas: Proveedoras de servicios de Datos Abiertos y Capacidades Abiertas para la conexión al sistema financiero.

Gestión Patrimonial: Plataformas para la gestión patrimonial digital, asesores de inversión robotizados y soluciones para los mercados de divisas, de valores y exchanges de activos virtuales.

Financiamiento Colectivo: Transmisión de necesidades de financiamiento de proyectos mediante plataforma digital para obtener apoyo de inversionistas, fondeadores y donantes (Banco de México, 2022).

Si bien nunca se podrán mitigar los riesgos cibernéticos en su totalidad para ninguna empresa o persona, la intención es disminuir la probabilidad de que se presenten incidentes de ciberseguridad o se materialice un ataque. Los riesgos cibernéticos pueden tener un impacto en los resultados financieros o de reputación de una persona u organización. Existen diversos factores que han incrementado los ataques cibernéticos, de acuerdo con el Global Financial Stability Report (Adrian, Natalucci, & Wu, 2024), el número de ciberataques se ha duplicado desde antes de la pandemia Covid-19, siendo el sector financiero uno de los más expuestos a los ciberataques, pues casi una quinta parte de todos los incidentes lo afectan. La nueva era del trabajo remoto ha vuelto a todas las personas y empresas más vulnerables. Los ataques más comunes son la ingeniería social, el malware, los ataques a redes y usuarios finales. De acuerdo con Alcalá (2023), los delitos informáticos en México se incrementaron 400 veces, pasando a ser la banca en línea la más afectada con el 60% de los ataques dirigidos a esta.

Para enfrentar los riesgos cibernéticos alrededor de una organización, es importante que esta tome una postura de seguridad. De acuerdo con la definición de NIST (2011), la postura de seguridad es el estado de seguridad de las redes, la información y los sistemas de una empresa basado en los recursos de seguridad de la información (por ejemplo, personas, hardware, software, políticas) y las capacidades existentes para gestionar la defensa de la empresa y reaccionar a medida que cambia la situación. Para las empresas Fintech es muy importante detectar su infraestructura crítica, la cual pueden ser sistemas físicos o virtuales vitales para su operación. Debido a que hay riesgos tanto adentro de la organización como afuera y estos evolucionan diariamente, la postura de

seguridad debe evolucionar constantemente con la intención de estar al día de las amenazas y riesgos alrededor de su negocio.

Para mejorar la ciberseguridad y dar cumplimiento a la Ley, en este trabajo se profundiza en las actividades que marca el núcleo del Marco de Seguridad Cibernética (CSF) 2.0 del NIST, actualizado en febrero 2024, el cual se actualiza para contar con seis funciones simultáneas y continuas: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.

Marco Teórico

Es importante entender el concepto FinTech, cómo lo indica su nombre en inglés, proviene de las palabras *finance* y *technology*, finanzas y tecnología. Alvarado (2023) hace referencia a que son empresas que utilizan las tecnologías de la información para ofrecer productos y servicios financieros innovadores. Como se comento anteriormente, en México existen diversos tipos. Estas empresas están en constante evolución y dependen directamente de la digitalización para dar sus servicios. Previamente se mencionaron los diferentes riesgos a las que se enfrentan y que es importante contar con una postura de ciberseguridad.

Un marco de ciberseguridad ayuda a las empresas a construir e incrementar su nivel de madurez en cuestión de ciberseguridad, además de otorgar controles base de seguridad. Las organizaciones pueden ocupar marcos de control para establecer sus políticas de seguridad. De acuerdo con Blum (2020), un marco de control es una lista de objetivos de control o requisitos de seguridad que por lo regular dicen que se debe de hacer, pero no cómo.

La Guía del CISO sobre los principales marcos de ciberseguridad de AttackIQ publicada en 2020 menciona que los marcos de ciberseguridad suelen tener distintos propósitos y una organización normalmente adoptará y utilizará más de uno. Además, muestra una tabla de los principales:

Marco de Ciberseguridad	Descripción
ISO 27001/27002	Es un marco y una norma ampliamente implementados que proporcionan requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), aunque existen muchas más normas en la familia ISO/IEC 27000
CIS-CSC	*CIS Controls* es utilizado para establecer defensas cibernéticas para las organizaciones. Ofrece una serie de 20 acciones de ciberseguridad básicas y avanzadas.
NIST CSF	Es un marco destinado a que las organizaciones de infraestructura crítica gestionen y mitiguen los riesgos de ciberseguridad según las normas, directrices y prácticas existentes.
ISACA COBIT 2019 (versión anterior COBIT 5)	Es el marco de gestión de TI de ISACA para ayudar a las empresas a desarrollar, organizar e implementar estrategias en torno a la información y la gobernanza.
Lockheed Martin Cyber Kill Chain	Es parte del modelo Intelligence Driven Defense para la identificación y prevención de intrusiones cibernéticas. El modelo identifica lo que los adversarios deben completar para lograr su objetivo: una visión de las actividades del atacante.
MITRE ATT&CK	Es una base de conocimiento accesible a nivel mundial sobre tácticas y técnicas de adversarios basadas en observaciones del mundo real. Se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

Nota. Se muestran los 6 principales marcos de ciberseguridad de acuerdo con *La Guía del CISO sobre los principales marcos de ciberseguridad* (AttackIQ, 2020).

Aunque cualquier marco de seguridad puede servir para incrementar el nivel de seguridad de una empresa, es importante hacer un análisis de cual puede ser el más efectivo para cada organización. Este proyecto se basa en el Marco del NIST. Este marco no ofrece alguna certificación por la cual se requiera un pago, y ha sido adoptado por diferentes empresas y gobiernos en Estados Unides y el resto del mundo por sus buenas prácticas, además de contar con varios controles de ciberseguridad. En su versión 1.1 “Marco para la mejora de la seguridad cibernética en infraestructuras críticas” se enfocó en dar más importancia a las infraestructuras críticas de Estados Unidos, como la seguridad de la nación, la economía, la salud y la seguridad pública. De acuerdo con Romero (2018) quien cita al *Global Forum on Cyber Expertise*, las infraestructuras críticas son como aquellas infraestructuras de información y comunicaciones interconectadas que son esenciales para mantener funciones societales vitales (bienestar social, económico, de seguridad o salud de la gente). Por ende, las empresas FinTech pueden ser consideradas así debido a su importancia económica en la sociedad. Otra de las razones por las que este proyecto se basa en el Marco de NIST, es porque Banxico lo toma como parte de sus referencias de interés en materia de ciberseguridad.

El Marco de NIST es solo una referencia para que las empresas puedan administrar mejor los riesgos de ciberseguridad. De acuerdo con NIST, cada empresa tiene riesgos únicos: diferentes amenazas, diferentes vulnerabilidades, y diferentes tolerancias de riesgo.

Regresando al contexto nacional sobre las FinTech, a partir de 2018, México se ha transformado en ser uno de los principales mercados para estas empresas en América Latina. Existen diferentes tipos de Fintech en el mercado.

> *“… la mayor cantidad de startups se encuentran en pagos y remesas, que abarcan el 23% de las empresas existentes. Luego se encuentran las encaminadas a préstamos, con 74 startups, que conforman el 22%; gestión de finanzas personales con el 13%, con 45 empresas; finanzas personales con cerca de 36 empresas, que abarcan el 11%; crowdfunding, con 9%,*

> *conformada 30 startups; 7% las tecnologías empresariales para las instituciones financieras, que suman 23 compañías; mientras que las startups de análisis como seguros tienen el 6%; gestión patrimonial el 3%; puntaje alternativo, identidad de un fraude, también con 3%; trading y capital de mercados con 2% y, por último, la banca digital con solo el 1%".* (García Gallegos, 2019, p.4)

Es importante crear una base de seguridad informática para todos los tipos de Fintech. La regulación puede ser una justificación para que los CIO, CTO, CISO, soliciten los presupuestos para atender esta necesidad, sin embargo, estar consciente de los riesgos siempre será mejor.

La seguridad de la información abarca muchos conceptos clave importantes para contextualizar los riesgos y amenazas que existen en el ciberespacio. Adicionalmente, es importante conocer los conceptos alrededor de las Fintech y lograr entender la relación de la seguridad informática y las Instituciones de Tecnología Financiera.

La información es el activo más valioso de las organizaciones y empresas, y debido al riesgo que enfrenta en diversos escenarios esta tiene que ser protegida, de acuerdo con Rodríguez, la Seguridad de la Información "*es el proceso de proteger la información de la pérdida, de la alteración no autorizada y de la divulgación inapropiada. Los objetivos de la Seguridad de la Información son, entonces, la confidencialidad, la integridad y la disponibilidad de la información*." (Rodríguez Parra, 210).

Es crucial que las empresas FinTech manejen la información como confidencial y que esta siempre este íntegra y disponible cuando se necesite. Estos conceptos deben de conocerse para saber cómo protegerse.

La confidencialidad se refiere a mantener la información fuera del conocimiento de personas que no están autorizadas para acceder a ella. La integridad trata de asegurar que la información permanezca inalterada y completa. La disponibilidad intenta que la información y los sistemas de comunicación permanezcan accesibles para sus usuarios oportunamente. (Rodríguez Parra, 210).

El concepto de ciberseguridad tiene que ver con dos términos de acuerdo con Blum (2020), la primera Ciber; que hace referencia a la combinación de gente y máquinas, y la segunda Seguridad; la cual indica estar libre de riesgos o peligro. Para adicionar al concepto de ciberseguridad, es importante conocer el término ciberespacio. De acuerdo Romero, fue en el útlimo año de la administración del expresidente Bush que el término de ciberespacio fue definido por el Gobierno Federal: "*Las redes interdependientes de infraestructuras de tecnologías de información incluyendo Internet, redes de telecomunicaciones, sistemas de cómputo y procesadores, y controladores embebidos en industrias críticas*" (Romero Galicia, 2018).

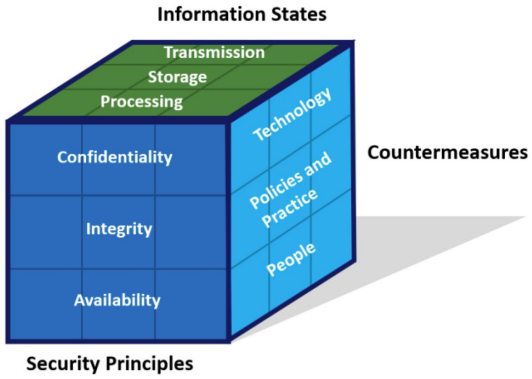
Una vez que se tiene entendido el concepto de ciberespacio, se debe entender que no solo abarca la parte de internet, sino que abarca más conceptos. Por lo tanto, la ciberseguridad tiene un impacto mayor al tratar de proteger la información que existe en el ciberespacio. Existen diferentes definiciones para la ciberseguridad, para fines de este proyecto se utiliza el citado por Romero y es la que establece el Departamento de Defensa de Estados Unidos: "*la prevención de daños para la protección y restauración de computadoras, sistemas electrónicos de comunicación, servicios de comunicación electrónica, comunicaciones alámbricas y comunicación electrónica, incluyendo información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio*" (Romero Galicia, 2018).

La información puede estar en 3 estados de acuerdo con Zajeganović (2023), quien cita a McCumber, esta se puede encontrar siendo transmitida, almacenada o procesada. John McCumber desarrolló una herramienta de administración de seguridad llamado el cubo de la seguridad. Como cualquier cubo tiene tres dimensiones, cada una representa una de las herramientas para abordar de manera integral la seguridad de los sistemas de información. La primera dimensión del cubo incluye los tres principios de seguridad de la información (tríada de la CIA: confidencialidad, integridad y disponibilidad). La segunda dimensión identifica tres estados de datos. La tercera dimensión del cubo

representa medidas de protección (Tecnología, Políticas y Prácticas, y Personas). (Zajeganović, y otros, 2023).

Figura 1.

Cubo de McCumber



Nota. En la cara principal se pueden apreciar los principios de la seguridad o la Triada CIA, en la cara derecha se pueden apreciar las medidas de protección y en la cara superior el estado de la información. Tomada de (Zajeganović, y otros, 2023).

Desde la perspectiva de este cubo, es importante tener medidas de protección en cualquier estado de la información para salvaguardar los principios de la seguridad. Es decir que un dato puede estar en un estado de almacenamiento y pudiera tener un ataque de un malware tipo ransomware o “secuestro de datos”, lo que estaría vulnerando la disponibilidad. Una medida de protección tecnológica puede ser un software instalado en punto final de detección y respuesta, el cual puede contener el ataque o responder de acuerdo con las reglas configuradas.

Cuando se le exige a una empresa FinTech cumplir con la Ley, es una medida de protección política por parte del gobierno que deriva en medidas tecnológicas y de personas por parte de las empresas a quienes aplique la Ley.

Dentro de la Ley FinTech en México se encuentran diversos artículos que aplican a la exigencia por parte del gobierno sobre las empresas para ser reguladas. En el artículo 4, fracción XVI se entiende por Institución de Tecnología Financiera (ITF)

a las a las instituciones de tecnología financiera reguladas en esta Ley, las cuales son las instituciones de financiamiento colectivo y las instituciones de fondos de pago electrónico. De aquí se deriva, que esta Ley solo aplica para estos dos tipos de Fintech. La Ley también exige en su artículo 34, fracción IV que las IFT que operen con activos virtuales divulguen los riesgos tecnológicos, cibernéticos y de fraude inherentes. Por lo tanto, aquí se está exigiendo hacer conscientes a los usuarios de los riesgos. Esto conlleva a que las ITF mejoren su postura de ciberseguridad. Más adelante en el artículo 39 de la Ley para Regular las Instituciones de Tecnología Financiera. (2018), fracciones V y VI se exige que para tener autorización por parte de la Comisión Nacional Bancaria y de Valores (CNBV), las solicitudes por parte de las empresas FinTech deben de demostrar primero lo relacionado con políticas de divulgación de riesgos y responsabilidades por la realización de las Operaciones en la empresa FinTech, y en segundo lugar las medidas y políticas en materia de controles de riesgos operativos, así como de la seguridad de la información, incluyendo las políticas de la triada de la ciberseguridad como confidencialidad, con la evidencia de que cuentan con un soporte tecnológico seguro, confiable y preciso para la atención de sus Clientes y con los estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información, así como la prevención de fraudes y ataques cibernéticos.

Los conceptos antes mencionados sirven para entender que el objetivo es proteger a las FinTech de los diferentes riesgos cibernéticos que existen y que además den cumplimiento a la Ley con el apoyo del Marco de Ciberseguridad del NIST.

Metodología

La intención de este proyecto es dar recomendaciones a las empresas FinTech de reciente creación o que son incipientes en el ámbito de la ciberseguridad. Estas recomendaciones están alineadas con la legislación mexicana. Se propone una estrategia de seguridad básica para las Fintech basada en los vectores de ataque

más comunes y que además de proteger las partes más vulnerables haga cumplir a las empresas con la Ley. Por lo tanto, se opta por una metodología cualitativa. De acuerdo con Cadena-Iñiguez (2020), esta metodología es inductiva y sigue un diseño de investigación flexible, además que, dentro de sus ventajas ofrece una realidad dinámica, lo que se requiere para el análisis de los cambios tecnológicos y la evolución de los riesgos cibernéticos.

Se exploraron los diferentes marcos de ciberseguridad existentes y más aceptados. Posteriormente se entendió lo que marca la Ley, por lo tanto, esta investigación es exploratoria, inductiva y descriptiva.

Como se hacen recomendaciones alineadas a marcos de ciberseguridad y se empatan con el cumplimiento mexicano se lleva a cabo un método sistemático, de acuerdo con Ponce de León (2009), este método puede combinarse entre método inductivo y deductivo cuando se separan las partes de un todo en orden jerárquico siguiendo determinados criterios de clasificación. Además, el conocimiento adquirido se organiza en un sistema coherente que funcione para las empresas Fintech. Se estudiaron casos particulares de empresas que han sido vulneradas y se recomiendan mecanismos para incrementar la seguridad y de esta manera disminuir los riesgos.

La principal técnica utilizada en este proyecto es la técnica de investigación bibliográfica, ya que no se tienen casos de primera mano y el tiempo es reducido para aplicar la observación. De acuerdo con Ponce de León (2009), esta técnica tiene como finalidad captar los adelantos científicos en el menor tiempo posible y con los más satisfactorios resultados. En consecuencia, se hicieron diversas lecturas y se aceleró la comprensión.

Las principales técnicas utilizadas en este proyecto serán las técnicas de observación científica. Para la observación de los ataques más comunes dirigidos a las Fintech se ocupará la técnica de la observación no estructurada y estructurada.

Los instrumentos que se utilizarán para esta investigación son las fichas de trabajo, de esta manera se destacan conceptos importantes para la comprensión y relación de la ciberseguridad y las Fintech.

Debido a todas las fuentes bibliográficas existentes y a los diversos conceptos alrededor de la seguridad de la información, se utiliza la técnica de búsqueda bibliográfica. Se analiza el marco normativo nacional. Se entiende la seguridad solicitada en la Ley Fintech y se traslada a la tecnología que haga cumplir la ley buscando optimización de costos y tratando de aumentar la protección.

Los instrumentos para la recolección de información están basados en las fuentes confiables relacionadas con la seguridad de la información, la seguridad informática y la ciberseguridad, como artículos, noticias, libros y revistas. Además de que se elaboraron los resúmenes necesarios. En cada fuente bibliográfica se aplicaron las citas textuales requeridas.

El método para la interpretación de la información que se cite en este proyecto está basado en la descripción de las principales recomendaciones internacionales, además de que se trasladó lo solicitado por la Ley para la ciberseguridad, a las mejores prácticas que prometen incrementar el nivel de seguridad y madurez y por lo tanto cumplir con la regulación. Basado en esto, se propone una seguridad base para aumentar la protección a las FinTech de reciente creación.

Con el objetivo de dar cumplimiento a la investigación, se siguen las siguientes fases:

Propuesta de atención al problema

Alrededor de cada organización existen diferentes tipos de riesgos. Cómo se ha venido mencionando, este trabajo está enfocado en hacer recomendaciones para

cumplir con la Ley Fintech y para aumentar el nivel de madurez de una organización en ciberseguridad con apoyo del Marco de Referencia del NIST orientado a las Infraestructuras Críticas. Con este Marco se puede tener un mejor entendimiento y gestión de los riesgos de la ciberseguridad. Se han tomado las definiciones de Infraestructuras Críticas de Romero Galicia, 2018 y del propio NIST (Marco para la mejora de la seguridad cibernética en infraestructuras críticas, 2018), las cuales definen a las funciones económicas como vitales.

Las empresas Fintech pueden hacer uso del Marco de Ciberseguridad del NIST sin importar su grado de madurez, además de que lo pueden utilizar para para identificar riesgos, evaluar su estado actual de ciberseguridad y administrar los riesgos de ciberseguridad. De acuerdo con el Marco de Ciberseguridad más actual (The NIST Cybersecurity Framework (CSF) 2.0, 2024) publicado el 26 de febrero de 2024, el Núcleo del Marco está compuesto por:

Funciones: Son las funciones básicas de ciberseguridad, las cuales incluyen en la versión 2.0 Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.

Categorías: Son las subdivisiones de una Función que resultan en actividades particulares, estás pueden ser divisibles para hacer más específicas las tareas.

Subcategorías: Las actividades son divididas para tareas más específicas y muestran los avances en cada categoría.

Referencias: La versión 2.0 del Marco ha actualizado algunas referencias, sin embargo, en el Marco para la mejora de la seguridad cibernética en infraestructuras críticas, se han dejado las referencias que aplican en este trabajo y son básicamente normas, directrices y prácticas comunes que ilustran como llegar al resultado deseado. Estas referencias no son exhaustivas. Un ejemplo de ellas para la función Gobernar sería la siguiente:

Subcategoría: Contexto Organizacional (GV.OC)

Ejemplo de Referencia para GV.OC-01: SP 800-221A: GV.CT-5

El Núcleo del Marco establece actividades que las empresas o instituciones pueden realizar para lograr los resultados deseados. A pesar de que existe un

gran número de actividades se pueden priorizar de acuerdo con la importancia y/o necesidad. A continuación, se deja un ejemplo de lo que es el Núcleo del Marco de Seguridad del NIST en la Tabla1.

Tabla 1

Nombres e identificadores de funciones básicas y categorías del Marco de Ciberseguridad 2.0 del NIST

Función	Categoría	Identificador
Gobernar	Contexto Organizacional	GV.OC
	Estrategia de Gestión del Riesgo	GV.RM
	Roles, responsabilidades y autoridades	GV.RR
	Política	GV.PO
	Vigilancia	GV.OV
	Gestión de riesgos de la cadena de suministro en materia de ciberseguridad	GV.SC
Identificar	Gestión de activos	ID.AM
	Evaluación del riesgo	ID.RA
	Mejora	ID.IM
Proteger	Gestión de identidades, autenticación y control de accesos	PR.AA
	Concientización y entrenamiento	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de plataforma	PR.PS
	Resiliencia en infraestructuras tecnológicas	PR.IR
Detectar	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder	Administración de incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Reporte de respuesta y comunicación de incidentes	RS.CO
	Mitigación de incidentes	RS.MI
Recuperación	Ejecución del plan de recuperación de incidentes	RC.RP
	Comunicación de recuperación de incidentes	RC.CO

Nota. Se muestran las 6 funciones básicas del Marco, las categorías y como se nombran los identificadores (The NIST Cybersecurity Framework (CSF) 2.0, 2024).

Las subcategorías deben de ser atendidas con forme las necesidades y posibilidades de cada empresa. Enseguida, se describe cada función y categoría, posteriormente, se hacen las recomendaciones de tecnologías o servicios para dar

cumplimiento al NIST y se señalan los puntos con los que se da cumplimiento a la Ley Fintech.

1. **Gobernar (GV)**: En esta función se establece la estrategia de gestión del riesgo de ciberseguridad de la organización, las expectativas y las políticas son establecidas, comunicadas y monitoreadas. Dependiendo de la organización y sus necesidades, esta información se hace llegar a áreas internas y/o externas.

    1.1 **Contexto Organizacional (GV.OC)**: Las organizaciones deben de comprender las circunstancias (misión, expectativas de las partes interesadas, dependencias y requisitos legales, normativos y requisitos contractuales) que rodean las decisiones de gestión de riesgos de ciberseguridad de la empresa. La mayoría de las empresas cuenta ya con una misión y visión claras. Es importante ocupar los medios oficiales de comunicación de la organización para comunicar la gestión de riesgos de la seguridad cibernética. Esta información tiene que llegar a las partes internas y externas. Se debe tener ya una postura sobre la ciberseguridad.

    1.2 **Estrategia de Gestión del Riesgo (GV.RM)**: Las prioridades, restricciones, declaraciones de tolerancia y apetito de riesgo y suposiciones de la organización se establecen, comunican y utilizan para dar soporte a las decisiones sobre riesgos operativos. Los objetivos sobre la gestión de riesgos deben de ser establecidos por las partes interesadas. Es importante el desarrollo de un plan de gestión de riesgos, además de estar informados de las estrategias de ciberseguridad de entes reguladores como Banxico (Estrategia de Ciberseguridad del Banco de México, 2024), quien pueden marcar una tendencia de las principales estrategias a seguir para instituciones financieras.

    1.3 **Roles, responsabilidades y autoridades (GV.RR)**: En este apartado se deben de establecer y comunicar a los responsables los roles,

responsabilidades y autoridades en materia de ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.

1.4 **Política (GV.PO)**: Al igual que las otras actividades, la política de ciberseguridad de la empresa es establecida, comunicada y aplicada.

1.5 **Vigilancia (GV.OV)**: Una vez que se tienen los resultados o salidas de las actividades de gestión del riesgo de ciberseguridad de toda la organización, estos se utilizan para informar, ajustar y mejorar la estrategia de gestión de riesgos.

1.6 **Gestión de riesgos de la cadena de suministro en materia de ciberseguridad (GV.SC)**: Los procesos de administración de los riesgos cibernéticos de la cadena de suministro son identificados, establecidos, gestionados, vigilados, y mejorados por los interesados de la empresa.

2. **Identificar (ID)**: Los riesgos actuales de ciberseguridad de la empresa son entendidos y reconocidos.

2.1 **Gestión de activos (ID.AM)**: Los activos de la empresa Fintech que le permiten alcanzar sus propósitos de negocio son identificados y administrados consistentemente con la importancia de los objetivos de la empresa y la estrategia del riesgo. Estos activos pueden ser: datos, infraestructura tecnológica, softwares, sistemas, instalaciones, servicios, personas, entre otros. Estos activos pueden ser inventariados para mayor control.

2.2 **Evaluación de riesgos (ID.RA):** Los riesgos de ciberseguridad alrededor de los activos y las personas deben de ser comprendidos por la organización. Para ello se pueden contratar servicios de un tercero que ofrezca un análisis de vulnerabilidades, además de participar en foros para enterarse de las amenazas cibernéticas actuales. Es importante que la organización entienda el impacto que podría tener un riesgo que se materialice.

2.3 **Mejora (ID.IM)**: Las organizaciones deben de identificar las mejoras a los procesos de administración de riesgos de ciberseguridad, los procedimientos y las actividades aplicadas en todo el Marco de Ciberseguridad. Estas mejoras parten de las evaluaciones de riesgos.

3. **Proteger (PR)**: Para la protección de la organización se ocupan diferentes medidas de seguridad y se gestionan los riesgos de ciberseguridad. Estas medidas van desde la autenticación hasta la capacitación de personal. En esta función también se evalúa el aprovechamiento de los riesgos.

   3.1 **Gestión de identidades, autenticación y control de accesos (PR.AA)**: El acceso físico y lógico a activos de la organización debe ser limitado a usuarios con autorización. Para esta funcionalidad se puede ocupar hardware de propósito específico como un Gestor de Acceso Privilegiado (PAM por sus siglas en inglés). El responsable de seguridad debe crear los perfiles de acuerdo con las necesidades del negocio y a las políticas internas.

   3.2 **Concientización y entrenamiento (PR.AT)**: Probablemente de las actividades más importantes está la de proveer al personal de la empresa con concientización y entrenamiento en ciberseguridad, esto les permitirá realizar sus tareas con una mejor preparación.

   3.3 **Seguridad de datos (PR.DS)**: Los datos deben de ser gestionados de acuerdo con la estrategia de riesgos de la organización y deben de proteger la triada de la seguridad: confidencialidad, integridad y disponibilidad. Además, se debe de proteger la información en cualquier estado que se encuentre: reposo, en tránsito o procesada. Es importante tener una política encargada de hacer copias de seguridad periódicamente.

   3.4 **Seguridad de plataforma (PR.PS)**: El hardware y el software; (como los firmwares, los sistemas operativos o los aplicativos), así como los servicios de plataformas físicas o virtuales deben de ser gestionadas consistentemente con la estrategia de riesgos de la empresa para

mantener la confidencialidad, integridad y disponibilidad de la información. Las actividades para esta seguridad incluyen el establecer prácticas para la administración de las configuraciones de los diferentes mecanismos de seguridad, así como mantener prácticas para el software utilizado, este puede ser conservado, sustituido, eliminado o inclusive actualizado. Algo similar se debe utilizar para el hardware, el cual de la misma manera que el software se puede mantener, sustituir, eliminar o actualizar. Es recomendable llevar una bitácora con los registros de las configuraciones y del personal que tiene acceso a estos equipos. Es importante que las instalaciones, ejecuciones y actualizaciones del software no autorizado sea restringido y se cree una política que aplique a estas actividades. Para el desarrollo de software es necesario adoptar prácticas de desarrollo seguro y estar haciendo análisis de vulnerabilidades al código para encontrar brechas de seguridad.

3.5 **Resiliencia en infraestructuras tecnológicas (PR.IR)**: Es importante que las empresas Fintech mantengan una cultura de resiliencia en todas sus infraestructuras relacionadas con la tecnología y de la cual depende su operación y sus servicios. La arquitectura de seguridad es gestionada con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos. Esto puede incluir mantener redes de telecomunicaciones protegidas y actuales, proteger bases de datos y aplicativos. Para ellos la seguridad perimetral de firewall de siguiente generación pueden ofrecer una mejor protección, además de agregar un firewall de base de datos y uno firewall de aplicaciones. De igual manera, se tiene que contar con recursos suficientes que puedan dar facilidad para contar con las herramientas adecuadas.

4. **Detectar (DE)**: Es importante que las empresas Fintech se adelanten a posibles amenazas y situaciones que pueden comprometer su información, detectando a tiempo posibles amenazas o ataques. Para ello es importante

que construyan capacidades para monitorear continuamente sus activos y entender lo que pasa por ahí, además de apoyarse con tecnologías como un Administrador de Eventos y Seguridad de la Información (SIEM por sus siglas en inglés) y un equipo de Orquestación, Automatización y Respuesta de Seguridad (SOAR por sus siglas en inglés). Los indicadores de las herramientas serán clave para la detección de un riesgo.

4.1 **Monitoreo continuo (DE.CM)**: Los responsables de los activos tecnológicos deben tener la práctica de monitorear continuamente toda la infraestructura tecnológica para encontrar anomalías, indicadores de compromiso o cualquier otro evento adverso potencial. Las redes y los servicios deben estar vigilados, así como los equipos de puntos finales. Para ello se pueden ocupar tecnologías como EDR, XDR, MDR y NDR.

4.2 **Análisis de eventos adversos (DE.AE)**: Las organizaciones deben de estar preparadas para analizar anomalías, indicadores de compromiso y acontecimientos adversos potenciales para clasificarlos y reconocer incidentes de ciberseguridad. Algunas soluciones tecnológicas que pueden ayudar a la detección y al análisis son los EDR, XDR, MDR o NDR, además de complementarse con una solución SIEM y/o SOAR.

5. **Responder (RS)**: En caso de tener un incidente de seguridad, es importante que la organización esté preparada para responder y tomar acciones sobre lo que está pasando o ya pasó. Para ello se recomienda tener un equipo de respuesta a incidentes. Este equipo puede ser costoso y probablemente muchas empresas no puedan costearlo, por lo tanto, se puede contratar un servicio que ayude en estas tareas o tener una póliza que pueda cubrir estas funciones.

5.1 **Administración de incidentes (RS.MA)**: Se toman acciones para detectar incidentes de ciberseguridad y ser administrados conforme a las políticas de la empresa. Es importante contar con un plan de respuesta a incidentes para ejecutarlo. Los incidentes deben de ser clasificados de acuerdo con su impacto.

5.2 **Análisis de incidentes (RS.AN)**: Se deben de iniciar las investigaciones y enfocarlas en asegurar la efectividad de las actividades forenses y de recuperación. Se puede contratar un servicio forense digital para dar con la causa raíz del problema. Es importante tener un registro de las acciones realizadas para recopilar los datos con mayor facilidad. En este punto se debe conocer la magnitud del incidente.

5.3 **Reporte de respuesta y comunicación de incidentes (RS.CO)**: De acuerdo con las políticas de cada organización, es importante que las actividades de respuesta sean coordinadas entre los equipos y los interesados.

5.4 **Mitigación de incidentes (RS.MI)**: Independientemente de la criticidad del incidente, es importante mitigarlo y erradicarlo. Se deben de tomar las medidas para monitorear los equipos y cerciorarse de que el incidente quedó erradicado. Por lo tanto, los incidentes se deben de contener y erradicar.

6. **Recuperación (RC)**: Ejecutar un plan de recuperación a los activos y operaciones afectadas es esencial para cualquier organización ante un ciberataque, además de mantener comunicación con la organización y entidades externas que puedan ayudar.

6.1 **Ejecución del plan de recuperación de incidentes (RC.RP)**: Dentro del plan de recuperación de incidentes deben de establecerse las actividades a realizar para recuperar la operación de sistemas y servicios que se vean afectados. Es importante contar con copias de seguridad y verificar el estado de la operación de los equipos para garantizar la correcta y completa restauración.

6.2 **Comunicación de recuperación de incidentes (RC.CO)**: Es importante mantener en todo momento una buena comunicación con partes internas y externas. Se debe de informar el estado de la recuperación y avisar cuando se esté completamente recuperado.

Cumplimiento contra la Ley para Regular las Instituciones de Tecnología Financiera

Con las recomendaciones anteriores se cumple con lo que marca la Ley Fintech de México. Para el caso del artículo 34, fracción IV, artículo 39, fracciones V y VI, artículo y 48 se está dando cumplimiento al contar con actividades claras de la función de Gobernar del Marco. Para la parte de contar con un soporte tecnológico seguro, confiable y preciso, es importante que las organizaciones realicen las actividades que marca la función Proteger, además de complementarlo con las funciones de Detectar y Responder. De igual forma para el artículo 48, donde se establece cumplir con los requerimientos de seguridad y continuidad operativa, se pueden aplicar las actividades de la función Recuperación del Marco. Para el artículo 76, párrafo 6, en donde se solicita interrumpir el acceso de información si se detecta alguna vulnerabilidad que ponga en riesgo la información, se debe hacer uso de la función Detectar y complementar con la función Responder.

El Marco de Ciberseguridad del NIST es una referencia muy importante para que las empresas Fintech den cumplimiento a la Ley para Regular las Instituciones de Tecnología Financiera.

Discusión de la Propuesta

Existen diferentes Marcos de Ciberseguridad, todos orientados a incrementar el nivel de seguridad en infraestructuras tecnológicas por medio de una gestión de riesgos. El Marco de Ciberseguridad del NIST es uno de los más utilizados por gobiernos y empresas privadas. Se ha utilizado este Marco como una referencia para dar recomendaciones de ciberseguridad a las empresas FinTech y que estas cumplan con la regulación mexicana, sin embargo, se podrían ocupar otros dependiendo de la necesidad y el grado de madurez de cada organización.

Otra de las razones por las que se utilizó este Marco es que en su versión 1.1 hacía referencia a las infraestructuras críticas y lo actualiza en su versión 2.0. Un Marco de Ciberseguridad sirve como guía para que las empresas u

organizaciones realicen actividades dependiendo de las necesidades de ciberseguridad que tengan y estas a su vez tomen una postura de seguridad cibernética. Las recomendaciones no solo van enfocadas a la parte tecnológica, sino que también a las partes estructurales de una organización y al entrenamiento que cada persona recibe.

Las funciones del Marco de Ciberseguridad son importantes para que las empresas FinTech aumenten su seguridad, por otra parte, se entiende que no siempre se cuenta con un presupuesto ni experiencia del cual una empresa u organización pueda pasar de un nivel 1 a nivel 4. La madurez de cada empresa se irá incrementando de acuerdo con sus necesidades y su postura de ciberseguridad.

Otro de los aspectos a resaltar es que el Marco del NIST da claridad de un Perfil Actual, es decir, de los resultados que se están obteniendo después de aplicar las acciones. Además, las organizaciones pueden tener claro el Perfil Objetivo, esto es, los resultados que desean obtener al aplicar las acciones derivadas del estudio del Marco.

Una función más que ayuda al cumplimiento de la Ley sería la de Identificar (ID). Con la subcategoría Evaluación del riesgo ID.RA-02 se puede desarrollar la capacidad para recibir información sobre amenazas cibernéticas en foros y fuentes de intercambio de información. Adicionalmente, la subcategoría ID.RA.03 puede aplicar para la identificación de amenazas internas y externas y la ID.RA.04 para entender el impacto de las amenazas y su probabilidad de ocurrir. El resto de las categorías de las funciones no debe de dejarse de revisar, ya que puede impactar directamente en la operación del negocio.

Para el artículo 37, fracción III, en donde se requiere que se cuente con controles de seguridad necesarios para llevar a cabo las operaciones, las categorías de la función Gobernar pueden servir como guía para crear políticas de gestión de riesgos en donde se establezcan los controles de seguridad necesarios para la mitigación de riesgos.

Si bien el guiar la estrategia de seguridad con el Marco del NIST aumenta el nivel de madurez de las organizaciones, este puede ser moldeado para cada empresa dependiendo de sus necesidades, tamaños y riesgos. Es importante comprender el apetito al riesgo de cada organización, así como su nivel de tolerancia. Es prioritario tener una comunicación bien establecida con toda la organización.

Una empresa puede ocupar el Marco del NIST para gestionar sus capacidades de ciberseguridad internas, así como externas. En las políticas de cada organización en donde se considera el impacto que puede tener un riesgo, se define si el riesgo es mitigado, transferido, evitado o aceptado, así como si este puede ser aprovechado. Una ventaja que tiene la versión 2.0 de este Marco es que contempla ya las cadenas de suministro.

En el artículo 39 de la Ley para Regular las Instituciones de Tecnología Financiera. (2018) se mencionan algunos de los requisitos para obtener la autorización de la CNBV. Entre los requisitos a cumplir están el de tener una política de divulgación de riesgos, que como se mencionó anteriormente el cumplimiento se puede dar con las funciones de Gobernar e Identificar. Adicionalmente se pone un requerimiento que abarca las medidas y políticas en materia de control de riesgos operativos, seguridad de la información, políticas de confidencialidad, evidencia de contar con un soporte tecnológico seguro y confiable, y de estándares de mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información. Con apoyo del Marco del NIST con la función de Gobernar se pueden establecer medidas y políticas para el control de riesgos y confidencialidad. El soporte tecnológico va ligado a la función de Proteger. Esta función, a diferencia de las otras cinco, puede demandar un presupuesto mayor debido a la implementación de infraestructura tecnológica para proteger los activos de la organización.

Es importante que para hacer eficientes los recursos se tenga muy bien desarrollado las funciones de Gobernar e Identificar, ya que de aquí podrán visualizarse las tecnologías necesarias para cumplir con las políticas y la protección de los activos identificados. En esta función de Proteger también esta

una parte medular en la gestión de riesgos que es la categoría de Concientización y entrenamiento (PR.AT).

Una organización puede invertir muchos recursos económicos y técnicos en infraestructura de seguridad, como lo pueden ser controles de acceso, administración de privilegios, seguridad perimetral, seguridad de bases de datos, protección a plataformas críticas, etcéteras, pero bastara un error humano para vulnerar estas barreras. Por lo tanto, es de suma importancia desarrollar al personal de la organización. La subcategoría PR.AT-01 puede servir a las organizaciones a sensibilizar y capacitar al personal para que desarrolle su trabajo con las habilidades suficientes para detectar algún tipo de riesgo alrededor de su labor cotidiana.

Con apoyo de la subcategoría PR.AT-02 es posible incrementar la sensibilización y capacitación del personal especializado en funciones de ciberseguridad. Estas dos secciones del Marco cumplen con una de las tareas fundamentales en la operación de las empresas FinTech, tener personal capacitado para poder identificar un riesgo y bajar la probabilidad de que estos se materialicen. Además, si se llegarán a materializar el personal contaría con el adiestramiento suficiente para saber actuar y minimizar el posible impacto.

Al hablar de la triada de la seguridad, todo el Marco del NIST tiene como objetivo reforzar la confidencialidad, garantizar la integridad y disponibilidad. Se insiste en seguir las recomendaciones de cada Función y con esto se estará cumpliendo con la Ley.

Más adelante en el artículo 39 de la Ley para Regular las Instituciones de Tecnología Financiera. (2018), fracción X, se solicita la relación de los convenios con otras Instituciones de Tecnologías Financieras o proveedores de servicios tecnológicos necesarios para realizar los procesos del negocio. Esta necesidad puede empatar con las cadenas de suministro de la versión 2.0 del Marco de Ciberseguridad del NIST. Dentro de la función Gobernar pueden desarrollarse controles de riesgo para terceros. Donde se establezcan estrategias para

gestionar riesgos sobre los proveedores de diferentes servicios, evaluar su posible impacto y fomentar a una supervisión constante de los riesgos de seguridad cibernética. Además de crear una práctica de buena comunicación con las partes interesadas a lo largo de toda la cadena de suministro.

Una función adicional importante para las organizaciones FinTech, es la de Detectar. Con esta función se pueden adelantar a posibles amenazas que existen alrededor del negocio, evitando un impacto mayor. Entre más temprano se detecte un riesgo es posible disminuir su impacto. La función Detectar se apoya de categorías como Monitoreo continuo (DE.CM), en donde se puede hacer tan amplio como se pueda. Monitoreo de activos como las redes y servicios de internet, el entorno alrededor del negocio, los proveedores, el hardware y el software. Esta función refuerza lo solicitado en el artículo 39 al demostrar que se cuenta con un soporte tecnológico seguro.

En el artículo 76 de la Ley FinTech, se solicita las organizaciones que tengan la capacidad de interrumpir el acceso de información cuando existan vulnerabilidades que pongan en riesgo la información de sus clientes. Por lo tanto, se habla ya de una respuesta ante un incidente. Dentro del Marco la función de Responder es una buena guía para tener acciones que detonen una respuesta. Además de clasificar la información que se tenga del incidente y poder priorizar acciones de contención. En esta sección del Marco también existen acciones de mitigación.

En caso de que una organización haya tenido un incidente es importante contar con un plan para recuperarse. El Marco ofrece una guía muy completa con su función Recuperar. Esta comprende la Ejecución del Plan de Recuperación de Incidentes (RC.RP) y la Comunicación de la recuperación del incidente (RC.CO).

El seguir las recomendaciones de cada Función del Marco puede garantizar el cumplimiento con la Ley para Regular las Instituciones de Tecnología Financiera de México, pero no puede garantizar una protección total. Todos los sistemas tienen vulnerabilidades que deben de ser atendidas conforme estos evolucionen.

Conclusiones

El Marco de Ciberseguridad del NIST es una guía para las empresas de reciente creación o que ya tienen tiempo en el mercado y quieren reforzar la ciberseguridad. Cada empresa tendrá sus riesgos particulares y podrá tolerar en mayor o menor medida los riesgos, inclusive entre las mismas empresas FinTech. Por ello es importante el atender las actividades descritas en este Marco, pues si son aplicadas adecuadamente aumenta la posibilidad de dar cumplimiento a la regulación mexicana, además de proporcionar mayor seguridad.

Existen diferentes factores que van a definir la postura de ciberseguridad de cada empresa y por lo tanto los perfiles organizativos. Los factores principales son el apetito al riesgo y el presupuesto con el que cuente la organización. Las prioridades deben de ser establecidas por los tomadores de decisión y directores.

Para las empresas FinTech es importante comenzar a priorizar las actividades enfocadas en la disminución del riesgo cibernético. Comenzar con una buena planeación de gobernanza y de identificación de riesgos da claridad de los activos a proteger y de las medidas a tomar en cuenta a la hora de hacer una estrategia de gestión de riesgos. Como lo marca el Marco de Ciberseguridad del NIST, existen acciones que las empresas deben hacer continuamente, como las que dan apoyo a Gobernar, Identificar, Proteger y Detectar. Existen otras acciones que deben estar listas en todo momento, como las que dan apoyo a Responder y Recuperar.

El apalancar la postura de ciberseguridad de una empresa FinTech a el Marco de Ciberseguridad del NIST tiene varios beneficios, como poder llevar a la organización un nivel superior de comprensión entre los riesgos cibernéticos y los objetivos de la organización. Además, lleva a la organización al cumplimiento de la regulación mexicana. Si se siguen las a acciones del Marco, se debe entender que los riesgos están en constante evolución y, por lo tanto, las prácticas de seguridad cibernética.

Bibliografía

- Adrian, T., Natalucci, F., & Wu, J. (2024). *Global Financial Stability Report.* International Monetary Fund.

- Alcalá Casillas, M. G., & Meléndez Ehrenzweig, M. Á. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: revista de tecnología y sociedad*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072023000100005&lng=es&nrm=iso&tlng=es

- Alvarado Quito, K., & Campodónico Durango, G. (2023). Análisis de las Fintech y su contribución al desarrollo de las PYMES en Guayaquil - Ecuador. *Revista Universidad y Sociedad, 15*(2), 475-483. Obtenido de http://scielo.sld.cu/pdf/rus/v15n2/2218-3620-rus-15-02-475.pdf

- AttackIQ. (2020). *The CISO's Guide to the Top Cybersecurity Frameworks.* San Diego: AttackIQ. Obtenido de https://www.attackiq.com/wp-content/uploads/2021/02/cisos-guide-to-the-top-cybersecurity-frameworks.pdf

- Banco de México. (2022). *Reporte de Estabilidad Financiera.* Obtenido de https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7BCA27B414-CC15-A42D-099B-DBAA4A38A8F2%7D.pdf

- Blum, D. (2020). *Rational Cybersecurity for Business.* Silver Spring: Apress Open.

- Cadena-Iñiguez, P., Rendón-Medel, R., Aguilar-Ávila, J., Salinas-Cruz, E., Cruz-Morales, F., & Sangerman-Jarquín, D. (2017). Métodos cuantitativos, métodos cualitativos o su combinación en la investigación: un acercamiento en las ciencias sociales. *Revista mexicana de ciencias agrícolas*. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-09342017000701603&lng=es&tlng=es

- El 38% de las ‘fintech’ se rezaga en ciberseguridad. (2024). *El Financiero*. Obtenido de https://www.elfinanciero.com.mx/opinion/de-jefes/2024/03/22/el-38-de-las-fintech-se-rezaga-en-ciberseguridad/

- (2024). *Estrategia de Ciberseguridad del Banco de México.* Banco de México, Ciudad de México. Obtenido de https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf

- Finnovating. (2023). *FinTech Global Vision 2023.* Estados Unidos.

- García Gallegos, D. (2019). Crowdfunding, transformación digital financiera y jurídica en México. *Revista chilena de derecho y tecnología*, 142. Obtenido de https://www.scielo.cl/pdf/rchdt/v8n2/0719-2584-rchdt-8-2-00139.pdf

- Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). Guide for Security-Focused Configuration Management of Information Systems. *NIST Special Publication 800-128*. Obtenido de https://doi.org/10.6028/NIST.SP.800-128

- La Universidad del Internet. (15 de 11 de 2022). *mexico.unir.net*. Obtenido de https://mexico.unir.net/noticias/economia/fintech/

- Ley para Regular las Instituciones de Tecnología Financiera. (2018). *Diario Oficial de la Federación*. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF.pdf

- Marco para la mejora de la seguridad cibernética en infraestructuras críticas. (2018). Obtenido de https://doi.org/10.6028/NIST.CSWP.04162018es

- Peñafiel Lucuy, K. A. (2021). Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 143-172. Obtenido de

http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2021000100009&lng=es&tlng=es

- Ponce de León Armenta, L. (2009). *Metodología del Derecho.* Ciudad de México, México: Porrúa.

- Rodríguez Ceja, V. (2024). Reporte de Estabilidad Financiera. *Banco de México*. Obtenido de https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7B6E48E53C-CE3E-9D3E-2D0D-A092213E8205%7D.pdf

- Rodríguez Parra, C. F. (junio de 210). SEGURIDAD DE LA INFORMACIÓN: ESTRATEGIA PARA FORTALECER EL GOBIERNO. *Revista de Derecho Privado*, 3-24. Obtenido de https://www.redalyc.org/articulo.oa?id=360033192006

- Romero Galicia, J. (2018). CONCEPTUALIZACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL DE MÉXICO. *Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, XXVIII*(2), 6. Obtenido de https://www.redalyc.org/articulo.oa?id=65458498003

- The NIST Cybersecurity Framework (CSF) 2.0. (Febrero de 2024). *National Institute of Standards and Technology*. Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- Zajeganović, M. B., Vugdelija, N. J., Stefanović, R. R., Kostić, S. M., Miljković, U. D., & Mach, G. G. (2023). Data security in mobile healthcare. *Vojnotehnicki glasnik, 71*(3), 748-768. Obtenido de https://www.redalyc.org/articulo.oa?id=661775012013

- Zárate Urgell, J. A., García Nieves, S., González Becerra, A., Antonio Toledo, I., & Cruz , R. A. (2022). Análisis de la ciberseguridad en el sector financiero de México con el fin de implementar la metodología Zero trust y mejorarla. *Ciencia*

Latina Revista Multidisciplinaria, *7*(1), 5. Obtenido de https://ciencialatina.org/index.php/cienciala/article/view/4661/7103

Atención a la retro alimentación del proyecto final

Comentario	Atención	# de página
Solicite el formato correcto a la coordinación del diplomado, ya que, le falta una sección inicial.	Se solicita formato y se atiende la petición.	1
Todas las figuras, tablas, gráficas o cuadros deben indicar la fuente de obtención de la información.	Se revisó el documento y se agrega referencias para el Cubo de McCumber en la página 9, y la tabla 1 página 14.	9 y 14
La numeración de páginas va al pie, no en la cabecera.	Se corrige la numeración.	Todas.
Página 3: Cite la fuente de obtención de información del texto subrayado en color morado con número "3".	Se revisó el documento y corrigió la cita.	3, 4
Página 9: Cite correctamente la fuente de obtención de información del texto subrayado en color rojo con número "1". Se cambió el texto, 7-10-2024.	Se revisó el documento y la cita, se hace la corrección.	9
Debe citar correctamente todo el texto subrayado en colores identificado como posible plagio.	Se revisa el documento y se agregan las citas correctas sobre la Ley.	24
Revisar las citas, ya que algunas no están realizadas de manera correcta, por ejemplo las citas textuales	Se revisan y corrigen las citas textuales.	1, 3 y 4
Aun cuando si se discuten las aportaciones, se recomienda profundizar en la manera en cómo la propuesta responde a los	Se entiende el punto, por ahora la intención es cubrir solo la legislación de la Ley para Regular las Instituciones de Tecnología Financiera y que las empresas Fintech se apeguen a un Marco de ciberseguridad, en	

elementos centrales de la legislación nacional relacionada con el tema.	este caso el del NIST, y cumplir con esta Ley.	
Revisar la redacción para mantener los párrafos en un rango de 8 a 10 renglones, ya que se hace uso de párrafos demasiado extensos	Se revisa el documento y se atiende la recomendación.	Todas.

Revisión 21 de octubre

Comentario	**Atención**	**# de página**
No se presenta una redacción coherente y buena ortografía	Se corrige ortografía y redacción.	Varías páginas del artículo
1. Coherencia verbal: se usan conjugaciones verbales en futuro en varias secciones, como si a penas se fuera a realizar la investigación.	Se atiende el comentario y en las secciones donde había verbos en futuro se corrigen.	Varías páginas del artículo
2. Estructura. No se distingue una cadena lógica respecto al análisis de se hace de la Ley Fintech contra el Marco de NIST, si bien el análisis es correcto, no se identifica la secuencia lógica del análisis (e.g. hay una sección donde se pasas del artículo 34, al 37 y luego al 39, ¿Por qué el autor no siguió la numeración secuencial?)	Al revisar la secuencia de los artículos que hablan de seguridad informática en la Ley, se pone esa secuencia, ya que no todos tocan el tema de ciberseguridad. Se mantiene esa secuencia.	Varías páginas del artículo
Si bien hay aportes interesantes, no se alcanza el objetivo planteado en virtud de que no es posible identificar en el documento porqué NIST es mejor que otros estándares para el cumplimiento de la Ley Fintech.	Existen diferentes marcos de ciberseguridad y ninguno es mejor que otro, todo dependerá de la utilización que se le quiera dar. En este caso se escogió NIST CSF por su versatilidad en organizaciones de reciente	7

	creación o que ya llevan tiempo. Se agrega una comparación de algunos marcos de ciberseguridad solo para contextualizar la existencia de más marcos.	