Universidad Autónoma del Estado de México

Centro Universitario UAEM Valle de Chalco

REGULACIÓN A LA NORMA FINTECH EN UN CASO DE ESTUDIO: PARA UNA INSTITUCIÓN DE FONDO DE PAGO ELECTRÓNICO EN TEMAS DE SEGURIDAD DE LA INFORMACIÓN

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

Cesar Gonzalez Garcia

ASESORA:

DRA. EN C. DE LA COMP. MARÍA DE LOURDES LÓPEZ GARCÍA

Revisor:

DR. EN C. MANUEL ÁVILA AOKI

Revisor:

M. EN C.C. FRANCISCO RAUL SALVADOR GINEZ

VALLE DE CHALCO SOLIDARIDAD, MÉXICO MARZO 2022.

CENTRO UNIVERSITARIO UAEM VALLE DE CHALCO

CUVCH

REGULACIÓN A LA NORMA FINTECH EN UN CASO DE ESTUDIO: PARA UNA INSTITUCION DE FONDO DE PAGO ELECTRÓNICO EN TEMAS DE SEGURIDAD DE LA INFORMAICIÓN.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1.
INTRODUCCIÓN

1. Antecedentes

Las empresas Fintech pueden ser concebidas como entidades que ofrecen productos y servicios financieros mediante el uso de tecnologías de la información y la comunicación, como páginas de internet, redes sociales y aplicaciones para celulares, lo cual brinda un servicio menos costoso que el ofrecido por la banca tradicional (Velázquez,2020).

Es importante mencionar que la **Ley Fintech** regula las Instituciones de Tecnología Financiera (ITFs) con el objetivo de ofrecer una mayor certeza jurídica a usuarios de servicios financieros a través de plataformas digitales (SHCP, 2018ª, párr. 3). En la tabla 1 se observan las verticales más importantes de estas empresas, según la Asociación de Fintech en México:

Tabla 1. Servicios de empresas Fintech [Elaboración propia]

Servicios	Particularidades
Medios de pago y transferencias	Plataformas de pago, comercio electrónico y transferencias internacionales.
Infraestructura para servicios financieros	Evaluación de riesgo, perfiles de clientes y de riesgo, prevención de fraudes, verificación de identidades API6 bancarias, agregadores de medios de pago, inteligencia de negocios, ciberseguridad y contratación electrónica.
Contratación digital de créditos	Empresas que ofrecen productos de crédito a través de plataformas electrónicas.
Soluciones financieras para empresas	Software para contabilidad e infraestructuras de facturación y gestión financiera.

Finanzas personales y asesorías financieras	Administración de finanzas personales, comparadores y distribuidores de productos financieros, educación financiera, asesores automatizados y planeación financiera.
Mercados financieros	Servicios digitales de intermediación de valores, instrumentos financieros y divisas.
Crowdfunding	Modelo de financiamiento colectivo donde diferentes personas de diversas partes del mundo realizan pequeñas o grandes aportaciones financieras a un determinado proyecto.
Insurtech	Tecnología aplicada a la prestación de servicios en el sector asegurador
Criptomonedas y blockchain	Desarrolladores de soluciones basados en blockchain, intermediarios digitales y mercados de activos tangibles
Entidades financieras disruptivas	Bancos u otras entidades financieras 100% digitales.

Ante la necesidad de normar el marco operacional de las denominadas empresas Fintech, el primero de marzo de 2018 entró en vigor la ley para regular a las instituciones de tecnología financiera (denominada **Ley Fintech**), así como la emisión de las Disposiciones de Carácter General (DCG) aplicables a estas empresas, publicadas en el Diario Oficial de la Federación (DOF) el 10 de septiembre de 2018 y modificadas mediante una resolución con fecha 25 de marzo de 2019 (Velázquez,2020).

Las instituciones que contemplan para la regulación y supervisión de la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores se mencionan en la tabla 2.

Tabla 2. Instituciones Fintech supervisadas por la CNBV [Elaboración propia]

Institución	Operaciones
Instituciones de Fondos de Pago Electrónico (IFPE)	- Emisión, administración y redención de saldos de dinero registrados electrónicamente para hacer pagos o transferencias. - Pueden realizar operaciones en moneda nacional y virtuales. - Pueden actuar como transmisor de dinero. - Podrán comercializar, emitir o administrar medios de disposición
Instituciones de Financiamiento Colectivo (IFC) (Crowfunding financiero)	-Autorización para realizar operaciones de financiamiento (deuda, capital o copropiedad). - Régimen de divulgación de riesgos. - Un proyecto no puede ser financiado por más de una IFC. - No está permitido ofrecer rendimientos garantizados.
Activos virtuales (criptomonedas)	- Las IFPE e IFC podrán operar con los activos virtuales autorizados por Banxico. - Banxico definirá los activos virtuales con los que podrá operar y las condiciones y restricciones de las operaciones realizadas con activos virtuales. - Cualquier institución que maneje activos virtuales deberá sujetarse a la regulación aplicable en materia de PLD.

1.2 Justificación

Las empresas que administran recursos económicos deben operar bajo la supervisión y administración de las autoridades financieras mexicanas para asegurar su buen funcionamiento, cubrir la seguridad de la información, proteger

el interés público y prevenir el lavado de activos, así como, el financiamiento del terrorismo.

Uno de los puntos más importantes en la formulación de la legislación de empresas de tecnología es enfatizar la transparencia y seguridad de todo el sistema financiero mexicano. Por su parte, los usuarios pueden monitorear, informar y solicitar directamente mejores servicios financieros digitales.

Es importante que las empresas que apliquen para operar como instituciones tecnológicas financieras deben cumplir con la **Ley Fintech**, pues de no ser así, las multas por incumplimiento de los requisitos de seguridad y/o continuidad del negocio se fijarán en 30.000 a 150.000 UMA, y el rango equivalente en 2019 será de 2,534,700.00 a 12,673,500.00 pesos.

1.3 Planteamiento del problema o pregunta de investigación

Las empresas que no cuentan con una regulación o certificación de seguridad están más expuestas a posibles ataques o incidentes de seguridad por lo que podrían perjudicar a la empresa y a sus clientes. Para minimizar los riesgos o incidentes se generan las siguientes preguntas de investigación. ¿Cuál es el proceso para obtener la regulación ante la Comisión Nacional Bancaria y de Valores?, ¿Cuáles son las acciones que debe realizar una empresa para garantizar la seguridad de la información de un cliente?, ¿Qué normas o estándares de seguridad podrían ayudar a robustecer la seguridad de la información de las Fintech?, ¿Cuáles son los riesgos a los que se enfrentan las instituciones tecnológicas financieras?

Por lo cual, el desarrollo de esta investigación es de gran importancia para las empresas próximas a ser autorizadas como Fintech.

1.4 Objetivos

El objetivo general de este trabajo es desarrollar un instrumento guía basado en la **Ley Fintech** para obtener la regulación de la Comisión Nacional Bancaria y de Valores en una empresa tecnológica y financiera.

Mientras que los objetivos específicos son los que siguen:

1. Seleccionar los parámetros relacionados con temas de seguridad de la información que se considera en el titulo 3, sección V indicados en la **Ley Fintech**.
2. Desarrollar los documentos base en tema de seguridad de la información que se requieren para solicitar la autorización a la Comisión Nacional Bancaria y de Valores.
3. Realizar recomendaciones sobre los puntos mínimos que se deben considerar en los documentos relacionados en temas de seguridad de la información.
4. Identificar los estándares de seguridad para robustecer la seguridad de información de las Instituciones de Fondos de Pago Electrónico (IFPE).
5. Describir como las mejores prácticas o los estándares de seguridad apoyarían a proteger los datos de los clientes de las Instituciones de Fondos de Pago Electrónico (IFPE).

1.6 Hipótesis

Si una empresa tecnológico-financiera utiliza un instrumento guía que le permita cubrir todos los puntos requeridos para ofrecer a sus clientes el buen funcionamiento en la seguridad de la información, la protección de los intereses públicos y la prevención del lavado de dinero entonces adquirirá el estatus de una empresa regulada Fintech.

1.7 Metodología

Para el alcance de los objetivos de esta tesis se realizará lo siguiente:

Investigación documental para el desarrollo del documento guía, ya que se hará una selección y recopilación de información sobre las normas de seguridad de la información y protección de datos personales, además de las consultas de tipo bibliográfico tales como libros, trabajos de tesis, artículos científicos, memorias, revistas, bases de datos especializados, páginas web, videos y otros recursos especializados.

CAPITULO 2.
EMPRESAS FINTECH

Fintech es una industria naciente en la que las empresas usan la tecnología para brindar servicios financieros de manera eficiente, ágil, cómoda y confiable. La palabra se forma a partir de la contracción de los términos *finance* y *technology* en inglés: FINANZAS + TECNOLOGÍA = FINTECH (Fintech México, (s. f.)).

Las empresas Fintech o de tecnología financiera son un fenómeno mundial que crece exponencialmente en diferentes áreas del sector financiero mundial, tan solo en México se tienen más de 300 empresas de esta naturaleza. El 82% de éstas están concentradas en Ciudad de México, Guadalajara, Monterrey, Mérida y Puebla, donde la Ciudad de México es la ciudad con mayor inclusión financiera (Canales TI, 2019, párr.1).

Su relevancia e impacto es de tal magnitud que numerosos países han elaborado leyes específicas para este sector. Nuestro país no es la excepción y promulgó la Ley para la Regular a las Instituciones de Tecnología Financiera (**Ley Fintech**). Uno de sus objetivos es prevenir riesgos, especialmente burbujas financieras y fraudes, así como sentar las bases para la creación de un ecosistema que fomente la innovación y el desarrollo (Canales TI, 2019, párr.2).

Ante la necesidad de normar el marco operacional de las denominadas empresas Fintech, el 1. ° de marzo de 2018 entró en vigor la ley para regular a las instituciones de tecnología financiera (denominada **Ley Fintech**), así como la emisión de las Disposiciones de Carácter General (DCG) aplicables a estas empresas, publicadas en el Diario Oficial de la Federación (DOF) el 10 de

septiembre de 2018 y modificadas mediante una resolución con fecha 25 de marzo de 2019 (Velázquez,2020).

La Comisión Nacional Bancaria y de Valores (CNBV) emitió lo siguiente:

> Bajo los principios de inclusión e innovación financiera, promoción de la competencia, protección al consumidor, preservación de la estabilidad financiera y neutralidad tecnológica y que dichas disposiciones incluyen requisitos para actuar como institución de tecnología financiera, capitales mínimos, contabilidad, excepciones para recibir recursos en efectivo o efectuar y recibir transferencias nacionales o internacionales (…) a fin de destinar los recursos a los esquemas para la alineación de incentivos de las instituciones de financiamiento colectivo, constancias sobre riesgos, metodologías sobre la asignación del grado de riesgo a los solicitantes de recursos en instituciones de financiamiento colectivo y plan de continuidad de negocios entre otras (CNBV, 2019a, párr. 3).

La Secretaría de Hacienda y Crédito Público declaro que México avanzó en la modernidad del sistema financiero ocupando el séptimo lugar a nivel mundial en la regulación del sector Fintech y señala que en México existen alrededor de 330 empresas Fintech (SHCP, 2018b).

Esta Comisión estableció que a las personas que realizaban actividades de financiamiento colectivo o de fondos de pago electrónico con anterioridad a la entrada en vigor de la **Ley Fintech** y que presentaron su solicitud de autorización ante la CNBV en el periodo establecido, podrán continuar realizando dichas actividades hasta en tanto se resuelva su solicitud (CNBV, 2019, párr.4). Mientras que, las personas que realizaban actividades señaladas en la **Ley Fintech** que no presentaron su solicitud de autorización al 25 de septiembre, deberán abstenerse de continuar realizando dichas actividades o celebrando nuevas operaciones, y deberán realizar únicamente los actos tendientes a la conclusión

o cesión de las operaciones existentes; de lo contrario, serán sujetas a las sanciones penales y administrativas que marca la Ley (CNBV, 2019, párr.4).

Por otro lado, la Comisión Nacional Bancaria y de Valores (CNBV), es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público (SHCP), con facultades en materia de autorización, regulación, supervisión y sanción sobre los diversos sectores y entidades que integran el sistema financiero en México, así como sobre aquellas personas físicas y morales que realicen actividades previstas en las leyes relativas al sistema financiero. La Comisión se rige por la Ley de la CNBV (CNBV, s. f., párr.1).

El proceso de autorización de Instituciones de Tecnología Financiera (ITF) avanza de acuerdo con los plazos previstos en la Ley para Regular a las Instituciones de Tecnología Financiera (**Ley Fintech**). Al día de hoy, se encuentran en trámite ante la CNBV, 93 solicitudes de autorización para organizarse y operar como ITF, con el siguiente detalle:

- 59 solicitudes para operar Instituciones de Fondos de Pago Electrónico (IFPE), y 34 solicitudes son de Instituciones de Financiamiento Colectivo (IFC).
- 69 empresas solicitantes se encuentran operando actualmente. Lo anterior con base en la Disposición Octava Transitoria de la **Ley Fintech**, ya que realizaban actividades financieras con anterioridad a la entrada en vigor de dicha ley y con oportunidad formalizaron su solicitud para operar como ITF.
- 1 una empresa formalmente autorizada y en operación, NVIO PAGOS MÉXICO, S.A.P.I. de C.V., Institución de Fondos de Pago Electrónico, a la que se le irán sumando las demás que, en su caso, se vayan autorizando (CNBV, 2021).

El informe **Fintech 100** de 2019, realizado por KPMG, Fintech Innovators y la firma de inversión Fintech H2 Ventures, presentó a las 100 compañías Fintech líderes en todo el mundo, Las compañías de pagos y transacciones forman el grupo más grande en la lista **Fintech100 de 2019,** en la tabla 3 se describen las

empresas, la ubicación de las mismas y una breve descripción de las operaciones que brindan las 10 mejores empresas de Fintech del 2019. (KPMG, 2020).

El informe de KPMG se puede encontrar lo siguiente:

- 42 empresas de Asia Pacífico (incluidas Australia y Nueva Zelanda).
- 36 empresas del Reino Unido y EMEA (Europa, Oriente Medio y África).
- 22 empresas de las Américas (Norte y Sudamérica).

Tabla 3. Las 10 mejores empresas del Fintech 100 del 2019 [Elaboración propia]

Compañía	Ubicación	Descripción de operaciones
Ant Financial	China	Plataforma de pagos para fiestas.
Grab	Singapur	Utiliza datos y tecnología para mejorar todo, desde el transporte hasta pagos en una región de más de 620 un millón de personas.
JD Digits	China	Es una empresa de tecnología digital, dedicada a brindar servicios digitales, en línea y servicios fuera de línea para todos los escenarios alrededor de tres puntos clave: datos, usuario y conectividad, utilizando tecnologías emergentes como big data, inteligencia artificial, computación en la nube, blockchain e IoT.
GoJek	Indonesia	Una plataforma de servicios múltiples con más de 20 servicios que incluyen Gopay, Gobills, Gopoints, Paylater y Gopulsa prestan servicios a millones de usuarios en el sudeste asiático.
Paytm	India	Es el pago digital más grande, empresa en India con más de 380 millones usuarios registrados y 12 millones de comerciantes en aborde su plataforma Paytm.

Du Xiaoman Financial	China	Ofrece servicios de préstamos e inversiones a plazo.
Compass	Estados Unidos	Es una empresa de tecnología inmobiliaria con una potente plataforma de extremo a extremo que admite todo el flujo de trabajo de compra y venta.
Ola	India	Desde la parte posterior de su base de usuarios de viajes compartidos Ola Money está facilitando y simplificando los pagos de sus usuarios.
Opendoor	Estados Unidos	Permite recibir una oferta sobre una vivienda en unos pocos clics y vender en cuestión de días, eliminando los dolores de cabeza, las incertidumbres y los riesgos de la transacción.
OakNorth	Reino Unido	Se especializa en préstamos para pequeñas y medianas empresas utilizando su plataforma de tecnología y datos patentada

Las compañías de pagos y transacciones forman el grupo más grande en la lista Fintech100 de 2019, representando a las 27 firmas clasificadas. Las empresas de los sectores de riqueza, seguros y préstamos han aumentado en importancia este año. Cuatro de las siete empresas australianas clasificadas son empresas de pagos (KPMG, 2020).

CAPITULO 3.
INSTRUMENTO GUÍA

Las empresas que quieren operar como Fintech necesitan realizar una solicitud a la CNBV, dicha solicitud debe de contar con una serie de documentos, en este capítulo se describirán cuáles son los documentos necesarios en temas de seguridad de la información:

La CNBV publicó la GUÍA PARA LA SOLICITUD DE AUTORIZACIÓN PARA LA ORGANIZACIÓN Y OPERACIÓN DE INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO en marzo del 2021, en la SECCIÓN IV “Inicio de Operaciones”, página 77, se enlista de manera enunciativa y no limitativa la documentación e información que la CNBV solicitará a la Institución para su revisión, previo al inicio de operaciones. A continuación, se describirán los documentos y las características anteriormente mencionados:

- Diagrama de red: en este documento se tienen que identificar las topologías de la red, así como las instancias en la nube e interconexión con otras redes (ya sea de la misma ITF o de proveedores). Deberá incluir descripción de la segregación física y lógica de las redes de comunicaciones, así como los equipos de seguridad perimetral (dispositivos o mecanismos automatizados para detectar eventos inusuales y prevenir incidentes de seguridad de la información, así como aquellos que eviten conexiones y flujos de datos entrantes o salientes no autorizados y fuga de datos), incluyendo esquemas de redundancia y otras medidas de seguridad dispuestas.

- Descripción de los controles implementados para proteger la integridad de las transacciones (tokens, certificados, passwords, nips, uso de hsm, etc.).

- Reporte de resultados de las pruebas de vulnerabilidades y de penetración llevados a cabo sobre la infraestructura tecnológica, como parte de las pruebas en la etapa final del proceso de desarrollo e implementación de los componentes de esta, previo a su liberación, así como los planes de remediación aplicados para mitigar las vulnerabilidades identificadas dentro de las pruebas.

- Descripción de las medidas para almacenar los registros de auditoría y los controles para mantener la integridad y disponibilidad de estos, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuadas por los clientes de la Infraestructura Tecnológica.

- Datos del Oficial en Jefe de Seguridad de la Información (CISO) de la IFPE, así como los de la figura del supervisor de este y de un suplente del CISO, al igual que el organigrama, la descripción puesto y funciones que consideren al menos las siguientes:

    - Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad de la información.

    - Validar el contenido y aprobar el Plan Director de Seguridad. Se entenderá por Plan Director de Seguridad al documento que establece la estrategia de seguridad a corto, mediano y largo plazo de una IFPE para garantizar una correcta gestión de la seguridad de la información y evitar la materialización de incidentes de seguridad de la información que podrían afectar de forma negativa a la IFPE.

    - Autorizar y vigilar la asignación de los accesos a la Infraestructura Tecnológica de la IFPE, incluyendo aquellos de los usuarios con mayores privilegios.

    - Verificar que, al menos trimestralmente o antes en caso de eventos inusuales o incidentes de seguridad de la información, se revisen las

actividades y asignación de perfiles y permisos de acceso en los diferentes componentes de la Infraestructura Tecnológica de la IFPE, incluyendo aquellas del personal técnico que cuente con altos privilegios, tales como administrador de sistemas operativos y de bases de datos.

- Mantener un control específico, para las autorizaciones de accesos por excepción, tales como clientes de ambientes de desarrollo con acceso a ambientes de producción y con accesos por eventos de contingencia, entre otros.
- Validar la gestión de incidentes de seguridad de la información, considerando las etapas de identificación, protección, detección, respuesta y recuperación, así como los aspectos de gobierno, preparación, pruebas, concientización y evaluación-aprendizaje, y asegurarse de la integración del equipo para la detección y respuesta de incidentes de seguridad de la información.
- Verificar la realización y efectividad de los programas de capacitación y concientización en materia de seguridad de la información dentro de la IFPE y hacia los clientes.
- Participar en los grupos que las autoridades establezcan para el intercambio de información y recursos en materia de seguridad de la información, y asegurarse de que los comunicados de seguridad por parte de las autoridades se atienden en forma oportuna.
- Ser el principal canal de comunicación, contacto y referencia, como máximo responsable de los aspectos relacionados con seguridad de la información al interior de la IFPE, ante entidades externas en el ámbito de sus responsabilidades.

- Manuales de políticas y procedimientos respecto de la seguridad de la información, que al menos consideren lo siguiente:
    - Controles de acceso y perfiles de usuario, los cuales deberán incluir la definición y características de credenciales de acceso (composición, tiempo de vigencia, entre otros) así como la descripción de los mecanismos para autenticar entre si a los componentes de la infraestructura tecnológica (certificados, usuarios aplicativos, etc.).
    - Controles de seguridad dentro del proceso de ciclo de vida de aplicaciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones pruebas de vulnerabilidades, análisis de código y destrucción de información, entre otros.
    - Clasificación de la Información de acuerdo con su nivel de criticidad evaluado por el dueño de la información.
    - Descripción de los controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de cliente de la Infraestructura Tecnológica.
    - Descripción de los protocolos y equipos de cifrado de la información de la ITF usados cuando la información sea transmitida, almacenada, procesada o se acceda de forma remota a dicha información.
    - Descripción de los procesos de gestión de incidentes de seguridad de la información, así como el proceso mediante el cual se harán del conocimiento de la CNBV que aseguren la detección, clasificación, atención y contención, diagnóstico, reporte a niveles jerárquicos competentes, solución, investigación (incluyendo en su caso análisis forenses), seguimiento y comunicación a autoridades, clientes y contrapartes, así como el proceso para llevar a cabo una investigación inmediata sobre las causas que generaron el incidente de seguridad de

la información y establecer un plan de trabajo que describa las acciones a implementar para eliminar o mitigar los riesgos y vulnerabilidades que propiciaron el incidente.

LA GUÍA PARA LA SOLICITUD DE AUTORIZACIÓN PARA LA ORGANIZACIÓN Y OPERACIÓN DE INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO solo menciona 12 documentos en temas de seguridad de la información, a continuación, se resumirán dichos documentos:

1. Diagrama de red.
2. Controles para proteger la integridad de la información (tokens, certificados, passwords, nips, uso de hsm, etc.).
3. Reporte de resultado de pruebas de vulnerabilidades y de Pentest.
4. Registros de auditorías.
5. Responsabilidades del CISO.
6. Control de acceso y perfiles de usuarios.
7. Ciclo de vida de aplicaciones, metodología de desarrollo o adquisición.
8. Clasificación de la información.
9. Gestión de sesiones de usuarios.
10. Cifrado
11. Gestión a Incidentes
12. Metodología de evaluación de riesgos

Como se estableció en “La guía para la solicitud de autorización para la organización y operación de instituciones de fondos de pago electrónico”, los documentos que se describieron no contemplan todos los controles que indica la **Ley Fintech**, por lo cual, a continuación, se describirán el total de documentos

necesarios para tener todos los controles de la **Ley Fintech** en un documento oficial.

1. **Plan de continuidad del negocio**: En la tabla 4 se mencionarán algunos de los controles de la **Ley Fintech** que se deberán contemplar en el documento "**Plan de continuidad del negocio**".

Tabla 4.. Principales artículos el plan de continuidad del negocio [Elaboración propia]

ID Control	Descripción
59	Las instituciones deberán contar con un Plan de Continuidad de Negocio que permita, ante Contingencias Operativas, la continuidad en la prestación de sus servicios y en la realización de sus procesos, su restablecimiento oportuno, así como la mitigación de las afectaciones producto de dichas contingencias.
60	Para desarrollar el Plan de Continuidad de Negocio, las instituciones de financiamiento colectivo deberán cumplir con los requerimientos mínimos establecidos en el Anexo 10 de las presentes disposiciones.
61	El Órgano de Administración de las instituciones de financiamiento colectivo, respecto del Plan de Continuidad de Negocio, deberá realizar al menos las funciones siguientes:
61 - II	El Órgano de Administración de las instituciones de financiamiento colectivo, deberá aprobar el Plan de Continuidad de Negocio, así como sus modificaciones.

En el anexo 1 se encuentra el total de los artículos que se deberán contemplar para alinear en el documento oficial.

2. **Evaluación de riesgos**: Este documento deberá ser el primero en realizarse ya que al identificar los riesgos se pueden planear las

actividades que mitigarán los riesgos identificados, en la tabla 5 se describirán los artículos de la **Ley Fintech** que se deberán alinear a esta actividad.

Tabla 5. Artículo que contempla la evaluación de riesgos [Elaboración propia]

ID Control	Descripción
61 - I	El Órgano de Administración de las instituciones de financiamiento colectivo, deberá designar y, en su caso, remover a la persona que funja como responsable de la administración de riesgos. Dicha persona deberá tener conocimientos en materia de riesgos operacionales y podrá ser empleado de la propia institución de financiamiento colectivo, o bien, un tercero contratado para tal efecto.

Aunque en la **Ley Fintech** solo se contempla un control para el tema de evaluación de riesgos, es un tema muy importante ya que es la base para la gestión en temas de seguridad de la información.

3. **Política de seguridad de la información**: La política de seguridad es uno de los documentos más importantes para la gestión de seguridad de la información, en la tabla 6 se mencionan algunos controles que se deberían alinear en este documento.

Tabla 6. Artículo que contempla política de seguridad de la información [Elaboración propia]

ID Control	Descripción
61 - III	El Órgano de Administración de las instituciones de financiamiento colectivo, deberá diseñar y establecer la política de comunicación para la notificación oportuna de las Contingencias Operativas a los Clientes y al interior de la institución de financiamiento colectivo, así como con la CNBV y demás Autoridades Financieras competentes en atención de la naturaleza de la Contingencia Operativa de que se trate.

61 - IV	El Órgano de Administración de las instituciones de financiamiento colectivo, deberá hacer del conocimiento de la CNBV las Contingencias Operativas que se presenten en cualquiera de los canales de atención al público o al interior de la propia institución de financiamiento colectivo. Lo anterior, siempre que estas interrupciones tengan una duración de, al menos, 30 minutos.
61 - V	El Órgano de Administración de las instituciones de financiamiento colectivo, deberá aprobar las metodologías para estimar los impactos cuantitativos y cualitativos de las posibles Contingencias Operativas que le presente, en términos de estas disposiciones, el responsable de la administración de riesgos, para su utilización en el análisis de impacto a que hace referencia el Anexo 10.
	Cuando la administración de la institución de financiamiento colectivo esté a cargo de un consejo de administración y un director general, este último será el responsable de llevar a cabo lo previsto en las fracciones III y IV anteriores.
63 - III - b	Configuración segura de acuerdo con el tipo de componente, considerando al menos, puertos y servicios, permisos otorgados bajo el principio de mínimo privilegio, uso de medios extraíbles de almacenamiento, listas de acceso, actualizaciones del fabricante y reconfiguración de parámetros de fábrica. Se entenderá como principio de mínimo privilegio a la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias de cada Usuario de la Infraestructura Tecnológica.
63 - X	Que sea sometida a la realización de ejercicios de planeación y revisión anuales que permitan medir su capacidad para soportar su operación, garantizando que se atiendan oportunamente las necesidades de incremento de capacidad detectadas como resultado de dichos ejercicios.

63 - X párrafo 2	Asimismo, la institución de financiamiento colectivo deberá evaluar la obsolescencia de los componentes de la Infraestructura Tecnológica, debiendo contar con un plan para su actualización.
63 - XII	Que tenga controles que permitan detectar la alteración o falsificación de libros, registros y documentos digitales relativos a las Operaciones.
83-II	Delimitar las funciones de los operadores, a fin de que sean independientes respecto de otras funciones operativas.

4. **Política de responsabilidades del director general:** Dentro de este documento se tendrán que definir las responsabilidades del director general las cuales se establecen en la **Ley Fintech,** además de las responsabilidades que sean establecidas por la misma empresa. En la tabla 7 se describirán algunos de los controles que establece la **Ley Fintech** para esta política.

Tabla 7. Artículo que contempla para las responsabilidades del director [Elaboración propia]

ID Control	Descripción
63	El director general o, en su caso, el administrador único de la institución de financiamiento colectivo, será responsable de la implementación de los controles internos en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad. El marco de gestión a que se refiere este párrafo, deberá asegurar que la Infraestructura Tecnológica de dicha institución, ya sea propia o provista por terceros, se apegue a los requerimientos siguientes:
63 párrafo 2	El director general o, en su caso, el administrador único de la institución de financiamiento colectivo será responsable de

	documentar en manuales las políticas y procedimientos previstas en este artículo.
64	El director general o, en su caso, el administrador único de la institución de financiamiento colectivo, será responsable del cumplimiento de las siguientes obligaciones en relación con la Infraestructura Tecnológica:
64 - I	Aprobar el Plan Director de Seguridad, así como sus actualizaciones, el cual debe estar alineado con la estrategia de negocio de la institución de financiamiento colectivo, así como definir y priorizar los proyectos en materia de seguridad de la información, con el objetivo de reducir la exposición a los riesgos tecnológicos y la materialización de Incidentes de Seguridad de la Información hasta niveles aceptables en los términos que defina, en su caso, el consejo de administración o el propio administrador único, según se trate, a partir de un análisis de la situación actual.

5. **Política de aplicaciones**: En este documento se deberá alinear los procedimientos para la gestión de la aplicaciones ya se para cambios, actualizaciones o desarrollo de las mismas, en la tabla 8 se describirán alguno de los controles que establece la **Ley Fintech** para este documento.

Tabla 8. Artículo que contempla la política de aplicaciones [Elaboración propia]

ID Control	Descripción
63 - II	Que sus procesos, funcionalidades y configuraciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones y el inventario detallado de cada componente de la Infraestructura Tecnológica, estén documentados.

63 - III	Que se hayan considerado aspectos de seguridad de la información en la definición de proyectos para adquirir o desarrollar cada uno de sus componentes, debiendo incluirlos durante las diversas etapas del ciclo de vida. Este comprenderá la elaboración de requerimientos, diseño, desarrollo o adquisición, pruebas de implementación, pruebas de aceptación por parte de los Usuarios de la Infraestructura Tecnológica, procesos de liberación incluyendo pruebas de vulnerabilidades y análisis de código previos a su puesta en producción, pruebas periódicas, gestión de cambios, reemplazo y destrucción de información.
63 - III - c	Mecanismos de seguridad en las aplicaciones que procuren que, durante su ejecución se protejan de ataques o intrusiones, tales como inyección de código, manipulación de la sesión, fuga de información, alteración de privilegios de acceso, entre otros. Dichos mecanismos deberán de ser implementados tanto para las aplicaciones proporcionadas por terceros como para las aplicaciones desarrolladas, implementadas y mantenidas por la propia institución de financiamiento colectivo.
63 - IV	Que cada uno de sus componentes sea probado antes de ser implementado o modificado, utilizando mecanismos de control de calidad que eviten que en dichas pruebas se utilicen datos reales del ambiente de producción, se revele información confidencial o de seguridad o se introduzca cualquier funcionalidad no reconocida para dicho componente.
63 - V	Que cuente con las licencias o autorizaciones de uso

6. **Política de componentes de Red:** En este documento se deberá alinear con los requerimientos sobre los componentes de red, en la tabla 9 se

describirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 9. Artículo que contempla la política de componentes de red [Elaboración propia]

ID Control	Descripción
63 - III - a	Tratándose de componentes de comunicaciones y de cómputo, los aspectos de seguridad deberán incluir, la segregación lógica, o lógica y física de las diferentes redes en distintos dominios y subredes, dependiendo de la función que desarrollen o el tipo de datos que se transmitan, incluyendo segregación de los ambientes productivos de los de desarrollo y pruebas, así como componentes de seguridad perimetral y de redes que aseguren que solamente el tráfico autorizado es permitido.
64 -II- e	Dispositivos, redes de comunicaciones, sistemas y procesos asociados a los Medios Electrónicos y canales de atención al Cliente, a fin de verificar que no existan vulnerabilidades o se cuente con herramientas o procedimientos que permitan conocer las credenciales de Autenticación de los Usuarios de la Infraestructura Tecnológica, así como cualquier información que, de manera directa o indirecta, pudiera dar acceso a la Infraestructura Tecnológica en nombre del Usuario de la Infraestructura Tecnológica.

7. **Política de control de acceso:** En este documento deberá alinear los requerimientos sobre el control de acceso que tienen que implementar las

empresas para acceder a la información sensible y de igual forma para los accesos físicos y lógicos de las instalaciones. En la tabla 10 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 10. Artículo que contempla la política de control de acceso [Elaboración propia]

ID Control	Descripción
63 - VI	Que cuente con medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada en la propia Infraestructura Tecnológica
63 - VI - a	Mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio.
64 - VI - a	Para lo anterior, se deberán incluir controles pertinentes para aquellos Usuarios de la Infraestructura Tecnológica con mayores privilegios, derivados de sus funciones, tales como la de administración de bases de datos, sistemas operativos y aplicativos.
63 - VI - a	Asimismo, se deberán prever en manuales las políticas y procedimientos para las autorizaciones de accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con accesos por eventos de contingencia, entre otros. Dichas políticas y procedimientos deberán ser aprobados por el oficial en jefe de seguridad de la información
63 - VI - c	Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el Usuario de la Infraestructura Tecnológica sea quien las

	conozca, así como medidas de seguridad, cifrado en su almacenamiento y mecanismos para solicitar el cambio de claves de acceso cada noventa días o menos. Tratándose de Clientes, el plazo referido será el definido por las propias instituciones de financiamiento colectivo en los manuales a que alude el último párrafo de este artículo. En el caso de los Usuarios de la Infraestructura Tecnológica asignados a aplicativos o componentes para autenticarse entre ellos, el cambio a que alude este inciso deberá realizarse, al menos, una vez al año. En el evento de que algún Usuario de la Infraestructura Tecnológica tenga conocimiento de las claves de acceso y deje de prestar sus servicios a la institución de financiamiento colectivo, estas deberán inhabilitarse de manera inmediata.
63 - VI - d	Controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de Usuario de la Infraestructura Tecnológica.
75	Las instituciones de financiamiento colectivo deberán prever lo necesario para que, una vez autenticado el Cliente en el Medio Electrónico que corresponda, la sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las instituciones de financiamiento colectivo establecerán, al menos, los mecanismos siguientes
75-I	Dar por terminada inmediatamente la Sesión en forma automática e informar al Cliente del motivo en cualquiera de los casos siguientes:
I - a	Cuando exista inactividad por más de cinco minutos.
I - b	Cuando en el curso de una Sesión, la institución de financiamiento colectivo identifique cambios relevantes en los parámetros de comunicación, tales como identificación del Dispositivo de Acceso, rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros.

75-II	Impedir el acceso de forma simultánea en un mismo Medio Electrónico, mediante la utilización de un mismo Identificador de Cliente y hacerlo del conocimiento del Cliente.
75-III	En el evento de que las instituciones de financiamiento colectivo ofrezcan servicios de terceros mediante enlaces, deberán comunicar a sus Clientes que, al momento de ingresar a dichos servicios, se ingresará a otro enlace cuya seguridad no depende ni es responsabilidad de dicha institución de financiamiento colectivo

8. **Política de cifrado:** Este documento deberá alinear los requerimientos sobre el cifrado considerando el grado de sensibilidad de la información, en la tabla 11 se escribirán algunos de los controles que establece la **Ley Fintech** para este punto.

Tabla 11. Artículo que contempla la política de cifrado[Elaboración propia]

ID Control	Descripción
63 - VI - b	Cifrado de la información conforme al grado de sensibilidad o clasificación de la información que la institución de financiamiento colectivo determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes o almacenada en la Infraestructura Tecnológica o se acceda de forma remota.
64 - VI - b	Las instituciones de financiamiento colectivo deberán cifrar al menos, la información que hayan clasificado como crítica en términos de estas disposiciones.

9. **Política de seguridad física:** En este documento se deberán considerar los requerimientos sobre la seguridad física de la empresa, en la tabla 12 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 12. Artículo que contempla la política de seguridad física [Elaboración propia]

ID Control	Descripción
63 - VI - e	Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la Infraestructura Tecnológica y permitan la operación conforme a las especificaciones del proveedor, fabricante o desarrollador.
83-I	Mantener controles de seguridad física o lógica o ambas según sea el caso en la Infraestructura Tecnológica de los canales remotos, incluyendo los dispositivos de grabación de las comunicaciones y los medios de almacenamiento y respaldo de estas, que protejan en todo momento la confidencialidad e integridad de la información proporcionada por sus Clientes.

10. **Política de trasmisión de datos:** En este documento se deberán considerar los requerimientos para asegurar la seguridad de la información al momento que se trasmite por los diferentes componentes de la infraestructura tecnología, en la tabla 13 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 13. Artículo que contempla la política de trasmisión de datos [Elaboración propia]

ID Control	Descripción
63 - VI - f	Medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la Infraestructura Tecnológica considerando, al menos, lo siguiente:

63 - VI - f-1	La veracidad e integridad de la información.
63 - VI - f-2	La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan solo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro.
63 - VI - f-3	Los protocolos de mensajería, comunicaciones y Cifrado, los cuales deben procurar la integridad y confidencialidad de la información.
63 - VI - f-4	La identificación de transacciones atípicas, previendo que se cuenten con herramientas de monitoreo o medidas de alerta automática para su atención por las áreas operativas correspondientes.
63 - VI - f-5	La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones.
63 - VI - f párrafo 2	Las medidas a que alude este inciso deberán establecerse acorde con el grado de riesgo que las instituciones de financiamiento colectivo definan para cada tipo de transacción.
63 - VI - párrafo 2	Las instituciones de financiamiento colectivo, en la clasificación de la información a que alude el inciso b) de esta fracción, dicho inciso se contempla dentro de la Política de Cifrado, deberán considerar al menos una categoría referente a la información crítica. En dicha categoría deberán incluir como mínimo la Información sensible y las imágenes de identificaciones oficiales e información biométrica de los Clientes, así como cualquier otra que determinen de acuerdo con sus políticas.

11. **Política de respaldos (Rolback):** En este documento se deberán alinear los requerimientos de respaldo de información o proceso de recuperación de la

información, en la tabla 14 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 14. Artículo que contempla la política de respaldos [Elaboración propia]

ID Control	Descripción
63 - VII	Que cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, en concordancia con lo estipulado en su Plan de Continuidad de Negocio a que alude el Capítulo V del Título Tercero de las presentes disposiciones.

12. **Política de protección de pistas de auditoría:** En este documento se deberán alinear los requerimientos sobre los registros de auditoría, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por los Usuarios de la Infraestructura Tecnológica, en la tabla 15 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 15. Artículo que contempla la política de pistas de auditoria [Elaboración propia]

ID Control	Descripción
63 - VIII	Que mantenga registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por los Usuarios de la Infraestructura Tecnológica, lo anterior con independencia del nivel de privilegios con el que estos cuenten para el acceso, generación o modificación de la información que reciban, generen, almacenen o transmitan en cada componente de la Infraestructura Tecnológica, incluyendo actividad

	de procesos automatizados, así como los procedimientos para la revisión periódica de dichos registros.
63 - VIII	Las instituciones de financiamiento colectivo deberán conservar los registros de auditoría a que se refiere esta fracción, por un periodo de tres años cuando dichos registros se refieran a actividades realizadas sobre componentes que procesen o almacenen información considerada como crítica de conformidad con la clasificación que determine la institución de financiamiento colectivo. En caso contrario, el periodo de conservación de los registros será mínimo de seis meses.

13. **Políticas de seguridad para la atención y respuesta a incidentes:** En este documento se deberán considerar los requerimientos sobre el procedimiento que se debe seguir en caso de que ocurra un incidente de seguridad, en la tabla 16 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 16. Artículo que contempla la política de atención de incidentes [Elaboración propia]

ID Control	Descripción
63 - IX	Que para la atención de los Eventos de Seguridad de la Información e Incidentes de Seguridad de la Información se cuente con procesos de gestión que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a áreas competentes, solución, seguimiento y comunicación a autoridades, Clientes y contrapartes.
63 - IX párrafo 2	Para la detección y respuesta de Incidentes de Seguridad de la Información a que hace referencia el párrafo anterior, el director general o, en su caso, el administrador único deberá designar un

	equipo que incorpore al personal de las diferentes áreas de la institución de financiamiento colectivo para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con el artículo 66 de las presentes disposiciones.
63 - IX párrafo 3	En caso de que se detecte la existencia de vulnerabilidades y deficiencias en la Infraestructura Tecnológica, deberán tomarse las acciones correctivas o controles compensatorios de acuerdo con el nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la institución de financiamiento colectivo puedan verse afectados.
63 - XIV	Que cuente con dispositivos o mecanismos automatizados para detectar y prevenir Eventos de Seguridad de la Información e Incidentes de Seguridad de la Información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información considerando, entre otros, medios de almacenamiento removibles.
63 - XIV párrafo 2	Las instituciones de financiamiento colectivo deberán correlacionar los datos obtenidos de los dispositivos o mecanismos automatizados a que alude el párrafo anterior con los datos de otras fuentes, tales como registros de actividad de Eventos de Seguridad de la Información o de Incidentes de Seguridad de la Información.
67	Cuando se presente un Evento de Seguridad de la Información o Incidente de Seguridad de la Información en: (i) los componentes de la Infraestructura Tecnológica de la institución de financiamiento colectivo; (ii) los canales de atención a los Clientes, tales como Medios Electrónicos, o (iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la

	institución de financiamiento colectivo, el director general o, en su caso, el administrador único, deberá:
67-I	Prever lo necesario para hacer del conocimiento de la CNBV, de forma inmediata los Incidentes de Seguridad de la Información, mediante correo electrónico remitido a la cuenta Ciberseguridad-CNBV@cnbv.gob.mx o a través de otros medios que la propia CNBV señale. En dicha notificación se deberá indicar, al menos, la fecha y hora de inicio del Incidente de Seguridad de la Información de que se trate y, en su caso, la indicación de si continúa o ha concluido y su duración; una descripción de dicho evento o incidente, así como una evaluación inicial del impacto o gravedad.
67-I	Adicionalmente, las instituciones de financiamiento colectivo deberán enviar mediante correo electrónico a la CNBV, a la cuenta Ciberseguridad-CNBV@cnbv.gob.mx o a través de otros medios que la propia CNBV señale, dentro de los cinco días hábiles siguientes a la identificación del Incidente de Seguridad de la Información de que se trate, la información que se contiene en los Anexos 11 y 12 de las presentes disposiciones.
67-I	En el caso de Eventos de Seguridad de la Información, deberán reportarse a través de los medios señalados en el primer párrafo de esta fracción solo aquellos que, de acuerdo con las políticas y procedimientos establecidos por la propia institución de financiamiento colectivo, se califiquen como relevantes por tener potencial afectación para la institución de financiamiento colectivo, sus Clientes, contrapartes, proveedores u otras entidades del sistema financiero, además de los relacionados con Información Sensible, imágenes de identificaciones oficiales e información biométrica de los Clientes. Este reporte únicamente deberá contener la fecha y hora de inicio, así como la descripción del evento de que se trate.

67-II	Llevar a cabo una investigación inmediata sobre las causas que generaron el Incidente de Seguridad de la Información y establecer un plan de trabajo que describa las acciones a implementar para eliminar o mitigar los riesgos y vulnerabilidades que propiciaron el mencionado incidente. Dicho plan deberá indicar, al menos, el personal responsable de su diseño, implementación, ejecución y seguimiento, plazos para su ejecución, así como los recursos técnicos, materiales y humanos, y enviarse a la CNBV en un plazo no mayor a quince días hábiles posteriores a que concluyó el Incidente de Seguridad de la Información.
68	La información de los Eventos de Seguridad de la Información calificados como relevantes e Incidentes de Seguridad de la Información a que se refiere el presente artículo deberá estar respaldada en los medios que las instituciones de financiamiento colectivo determinen y conservarse por, al menos, diez años.

14. **Políticas de seguridad para escaneos de vulnerabilidades:** En este documento se deberá alinear los requerimientos que se contemplan para realizar los escaneos de vulnerabilidad, en la tabla 17 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 17. Artículo que contempla la política de escaneo de vulnerabilidades [Elaboración propia]

ID Control	Descripción
64 -III	Elaborar un calendario anual para la realización de pruebas de escaneo de vulnerabilidades de los componentes de la Infraestructura Tecnológica que almacenen, procesen o transmitan información, priorizándolos de acuerdo con el resultado del ejercicio de

	clasificación de información que determine la institución de financiamiento colectivo. El calendario deberá prever la revisión bimestral de los componentes de la Infraestructura Tecnológica de manera que, a la conclusión del año, se hayan revisado la totalidad de los componentes que almacenen, procesen o transmitan información catalogada por la institución de financiamiento colectivo como crítica, además de los que esta considere necesarios. El director general o, en su caso, el administrador único, será responsable de vigilar que dichas pruebas se lleven a cabo, ya sea a través de la propia institución de financiamiento colectivo o de un tercero contratado al efecto. Adicionalmente, cuando se incorporen nuevos componentes de la Infraestructura Tecnológica, el director general o, en su caso, el administrador único, será el responsable de vigilar que se realice la prueba de escaneo de vulnerabilidades, previo a su puesta en producción.

15. **Políticas de seguridad para pruebas de intrusión:** En este documento se deberán alinear los requerimientos para el proceso de pruebas de intrusión, en la tabla 18 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 18. Artículo que contempla la política de pruebas de intrusión [Elaboración propia]

ID Control	Descripción
64 -V	Clasificar las vulnerabilidades detectadas de acuerdo con la metodología aprobada por el responsable de la administración de riesgos de la institución de financiamiento colectivo.
64 -VI	Elaborar planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren las fracciones II, III y IV anteriores, considerando la clasificación de la fracción V del presente

	artículo, así como implementar mecanismos de defensa que prevengan el acceso y uso no autorizado de la Infraestructura Tecnológica.
64 -VI-1	Los planes de remediación a que se refiere el párrafo anterior deberán ser validados por el oficial en jefe de seguridad de la información. Asimismo, dichos planes deberán contener, al menos, la indicación del personal responsable de su implementación y ejecución, así como plazos para esta, detalle de las actividades realizadas y por realizar, al igual que los recursos técnicos, materiales y humanos empleados. Los referidos planes de remediación deben ser elaborados una vez que se identifiquen las vulnerabilidades y ser enviados a la CNBV en un plazo de diez días hábiles.
64 -VI-2	En adición a lo señalado en el párrafo anterior, en caso de tratarse de proyectos a corto, mediano o largo plazo en los planes de remediación, deberán incorporarse al Plan director de Seguridad.
64 -VII	Implementar procesos de seguimiento al cumplimiento de los planes de remediación referidos, lo que deberá ser verificado por el oficial en jefe de seguridad de la información, quien adicionalmente deberá corroborar que los referidos planes han logrado corregir las vulnerabilidades encontradas.

16. Plan de capacitación y concientización: En este documento se deberán indicar los requerimientos que se solicitan para dar cumplimiento a los temas de capacitación, en la tabla 19 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 19. Artículo que contempla la política de capacitación [Elaboración propia]

ID Control	Descripción

64 -VIII	Implementar programas anuales de capacitación dirigidos a todo el personal, así como de concientización en materia de seguridad de la información hacia los Clientes incluyendo, en su caso, a terceros que les presten servicios, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de Infraestructura Tecnológica tengan al respecto.

17. Política de responsabilidades del CISO: En este documento se deberán alinear todas las responsabilidades que están asignadas para el CISO, en la tabla 20 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 20. Artículo que contempla la política de responsabilidades del CISO [Elaboración propia]

ID Control	Descripción
65	Las instituciones de financiamiento colectivo deberán contar con una persona que, entre sus funciones, se desempeñe como oficial en jefe de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer).
65	El oficial en jefe de seguridad de la información deberá ser designado por el director general o, en su caso, por el administrador único, debiendo reportarles, y no deberá tener conflictos de interés respecto del responsable de las funciones de auditoría y tecnologías de la información que existan dentro de la institución de financiamiento colectivo.
65	Las funciones del oficial en jefe de seguridad de la información podrán ser realizadas por un tercero, siempre que se ajuste a lo señalado en el presente artículo.

66-I	Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad señalados en el artículo 63 de las presentes disposiciones.
66-II	Elaborar el Plan director de Seguridad, el cual deberá contener, por cada proyecto que se defina, nombre del proyecto, objetivo, alcance, fechas de inicio y fin, áreas involucradas y la inversión proyectada. Dicho plan deberá revisarse y actualizarse, al menos, anualmente.

18. Política de autenticación: En este documento de deberá alinear los todas las características de autenticación, así como los procedimientos para autenticar a los clientes, en la tabla 21 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 21. Artículo que contempla la política de autenticación [Elaboración propia]

ID Control	Descripción
70	Las instituciones de financiamiento colectivo, para permitir el inicio de una Sesión, solicitarán y validarán al menos lo siguiente: I El identificador de Cliente II Un factor de autenticación de los referidos en el artículo 72 de las presentes disposiciones. El Identificador de Cliente deberá ser único para cada Cliente y permitirá a las instituciones de financiamiento colectivo identificar todas las Operaciones realizadas por el propio Cliente.
71	Las instituciones de financiamiento colectivo, en el uso del Identificador de Cliente y los Factores de Autenticación, se ajustarán, cuando menos, a lo siguiente (numerales 71-I al 71-V):

71-I	Contar con los mecanismos necesarios para impedir la lectura en la pantalla del Dispositivo de Acceso, de la información de identificación y Autenticación proporcionada por el Cliente.
71-II	Contar con procedimientos que aseguren que, en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Cliente quien los reciba, active, conozca, desbloquee y restablezca.
71-III	Asegurar que cuando exista más de un Factor de Autenticación estos sean independientes, es decir, que la vulneración de uno no comprometa la fiabilidad de los demás.
71-IV	Contar con procedimientos para restablecer una Contraseña bloqueada, en los cuales se identifique la identidad del Cliente sin comprometer su Información sensible.
71-V	Contar con procedimientos para invalidar los Factores de Autenticación y el Identificador de Cliente para impedir su uso en el Medio Electrónico que corresponda, cuando un Cliente deje de serlo.
72	Las instituciones de financiamiento colectivo deberán utilizar Factores de Autenticación para verificar la identidad de sus Clientes y la facultad de estos para realizar Operaciones a través del Medio Electrónico de que se trate. Dichos Factores de Autenticación, deberán de utilizar cualquiera de los siguientes:
72-I	Información como Contraseñas y Números de Identificación Personal (NIP), que las instituciones de financiamiento colectivo proporcionen al Cliente o permiten a este generar y que solamente este último conozca para ingresar a la Plataforma e iniciar la Sesión de que se trate y que deberá tener las características siguientes:

72-I - a	Su longitud deberá ser de al menos seis caracteres e incluir caracteres alfanuméricos y especiales, cuando el Dispositivo de Acceso lo permita.
72-I - b	En ningún caso se podrán utilizar como tales, la información siguiente:
72-I - b - i	El Identificador de Cliente
72-I - b - ii	El nombre de la institución de financiamiento colectivo.
72-I - b - iii	Más de tres caracteres idénticos en forma consecutiva.
72-I - b - iv	Más de tres caracteres numéricos y alfabéticos en forma secuencial.
72-II-a	Contar con propiedades que impidan su duplicación o alteración.
72-II-b	Ser información dinámica que no podrá ser utilizada en más de una ocasión.
72-II-c	Tener una vigencia que no podrá exceder de dos minutos.
72-II-d	No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes de la institución de financiamiento colectivo o por terceros.

19. **Política de atención a clientes:** En este documento se deberán colocar todos los procesos que se deben seguir para atender las solicitudes de los clientes en cambio o actualizaciones, en la tabla 22 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 22. Artículo que contempla la política de atención a clientes [Elaboración propia]

ID Control	Descripción

76	Las instituciones de financiamiento colectivo, para la celebración de Operaciones, solicitarán a sus Clientes un segundo Factor de Autenticación de los que se establecen en el artículo 72 de estas disposiciones, adicional y diferente al utilizado para iniciar la Sesión y en cada ocasión en que se pretenda realizar una de las operaciones siguientes (numerales (76-1 al 76V):
76-I	Instrucciones para realizar compromisos de inversión o retirar sus recursos.
76-II	Registro o modificación de Cuentas Destino para el servicio de que se trate.
76-III	Cambio y Desbloqueo de Contraseñas o Números de Identificación Personal (NIP).
76-IV	Alta y modificación del medio de notificación a que se refiere el artículo 79 de estas disposiciones.
76-V	Consultas de estados de cuenta de uno o más periodos que permitan conocer información relacionada con el Cliente y sus Operaciones. No será necesario el referido segundo factor, para el caso de la consulta de estados de cuenta, siempre que el Cliente haya iniciado su Sesión con un Factor de Autenticación a los que se refieren las fracciones II y III del artículo 72 de estas disposiciones.
77	Las instituciones de financiamiento colectivo que ofrezcan servicios a sus Clientes a través de centros de atención telefónica, canales electrónicos de mensajería o por agentes automatizados, podrán realizar la identificación de sus Clientes y verificar su identidad mediante cuestionarios, en cuyo caso deberán observar lo siguiente (numerales 77-I al 77-III):

77-I	Deberán requerir datos que el Cliente conozca y que las instituciones de financiamiento colectivo puedan validar, manteniendo la debida confidencialidad de dicha información.
77-II	Contar con procedimientos para practicar cuestionarios aleatorios de forma automatizada o vía remota por los operadores, en este último caso, impidiendo que sean utilizados de forma discrecional.
77-III	Definir un conjunto de preguntas abiertas en cuestionarios de al menos tres preguntas y, en el evento de que la respuesta a una de ellas sea incorrecta, se podrá formular una pregunta adicional.

20. **Política de seguridad para gestión de proveedores:** En este documento se indican las responsabilidades que tendrán que cumplir los proveedores que sean contratados En la tabla 23 se escribirán algunos de los controles que establece la **Ley Fintech** para este documento.

Tabla 23. Artículo que contempla la política de atención a clientes [Elaboración propia]

ID Control	Descripción
85	Las instituciones de financiamiento colectivo solamente requerirán autorización de la CNBV, para contratar con terceros la prestación de servicios que tengan las siguientes características (numerales 85-I y 85-II) :
85-I	Que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de Información Sensible, imágenes de identificaciones oficiales o información biométrica de los Clientes, siempre y cuando el tercero contratado tenga privilegios de acceso para conocer dicha información o a la información de configuración de seguridad, o bien, a la administración de control de accesos.

85-II	Que realicen procesos en el extranjero relacionados con la contabilidad o tesorería, así como con el registro de movimientos transaccionales de los Clientes.
86	Asimismo, deberá quedar constancia, dentro del contrato, de la aceptación expresa por parte del tercero de las obligaciones siguientes (numerales 86-II-a, 86-II-f y 86-II-g):
86-II-a	Apegarse a lo previsto en el artículo 54 de la Ley
86-II-f	Cumplir con los términos, condiciones y procesos para que el tercero garantice a la institución de financiamiento colectivo la transferencia, devolución y eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.
86-II-g	Mantener registros de auditoría íntegros que incluyan la información detallada de los accesos o intentos de acceso y la operación o actividad efectuadas por los Usuarios de la Infraestructura Tecnológica. Dichos registros deberán estar a disposición del personal autorizado de la institución de financiamiento colectivo.

En el anexo 1 **"CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE LA LEY FINTECH"** se indican los controles en temas de seguridad de la información que establece la **Ley Fintech**, en la última columna de la tablas se colocó el nombre del documento donde se deberá contemplar para su alineación.

Aunque la **Ley Fintech** contempla los temas de seguridad de la información, existen estándares, normas o leyes de seguridad que complementan y robustecen la seguridad en las empresas, como lo es la norma **ISO 27001** y la **Ley federal de protección de datos personales en posesión de los particulares**.

La norma ISO 27001:

> Es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI debe estar implementado en la empresa como mínimo con tres meses de antelación. Cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos del SGSI. El SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estas expectativas (Ladino, 2011, pág. 335).

En la figura 1 se muestra la aplicabilidad, duración aproximada de implementación, entre otras características de la norma ISO 27001.

Un SGSI tiene como base un conjunto de controles, procesos, políticas, manuales, guías, etc. A fin de gestionar eficientemente confidencialidad, integridad y disponibilidad de la información, minimizando a la vez los riesgos de seguridad de la información de la compañía, un SGSI tiene 3 principios los cuales son:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran (ISO27000.ES, 2005, párr.19).

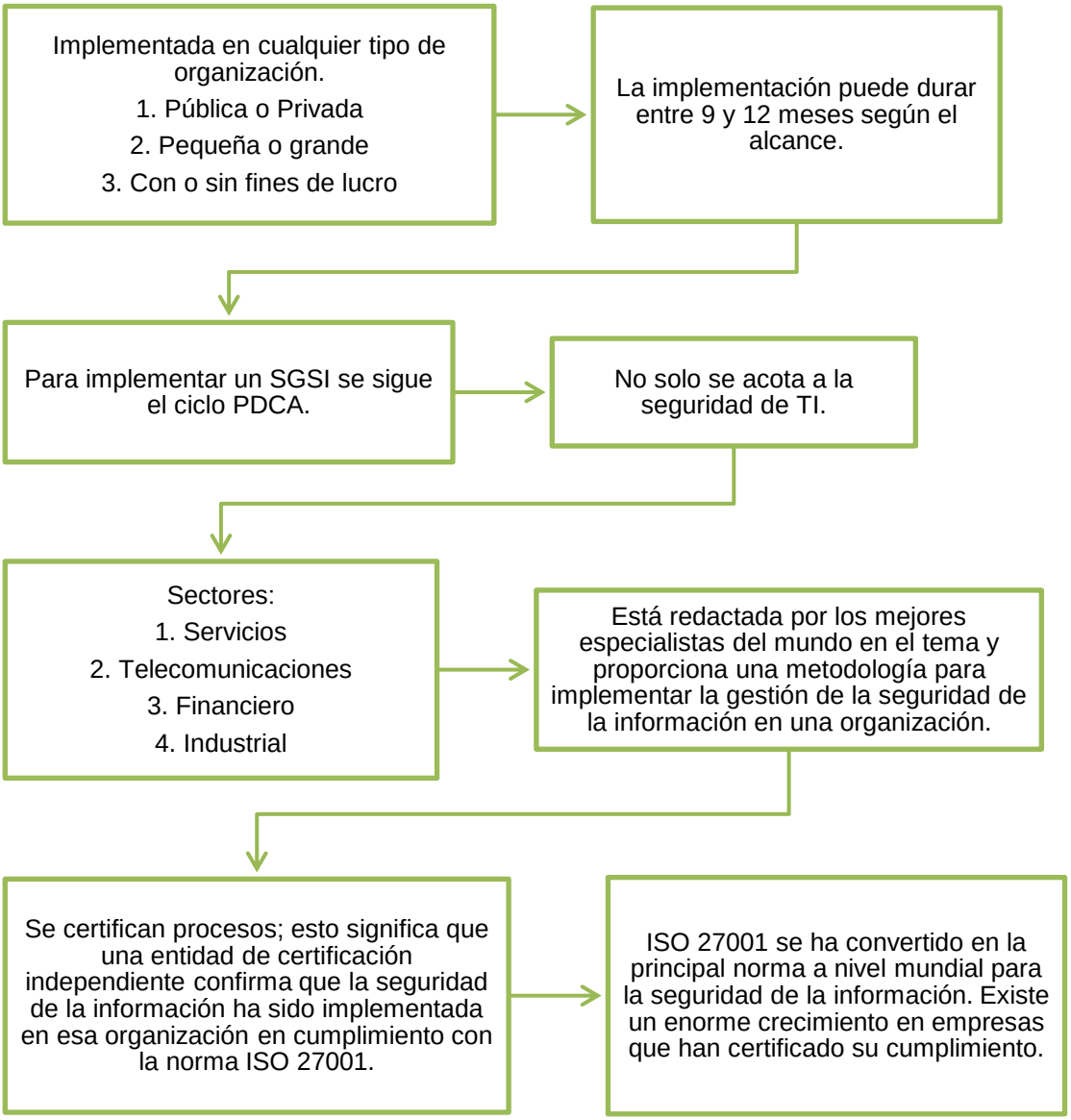

Figura 1: Introducción de ISO 27001 [Elaboración propia].

El SGSI está compuesto por un ciclo de 4 pasos Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar) tal y como se muestra en la figura 2, esta es la sistemática más usada para implantar un sistema de mejora continua, a continuación, se presentarán 4 diagramas donde se mostrarán algunas de las

actividades que se tienen que realizar en cada uno de los pasos que contempla la implementación de un SGSI:

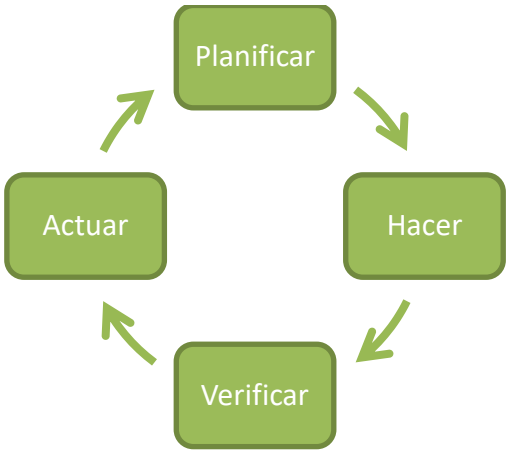

Figura 2: Fases del modelo PDCA [Elaboración propia]

Planificar (Plan): Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, en la figura 3 se muestran las actividades que se tendrían que desarrollar en esta fase (Bernal, 2013, párr. 3).

Algunos ejemplos de activos de las empresas que se tienen que identificar en el primer paso de la implementación del SGSI son:

- Procesos.
- Aplicaciones críticas.
- Servidores.
- Bases de datos.
- Dispositivos de red.
- Centros de Datos.
- Personas.

Figura 3: Actividades de la fase “Plan” [Elaboración propia].

Dentro de la fase “Plan” es necesario realizar algunas acciones para la implementación del SGSI, dichas acciones son las siguientes:

- Identificación de documentación a generar.
- Diseño de metodología de riesgos.
- Análisis y evaluación de riesgos.
- Desarrollo del SoA (La Declaración de Aplicabilidad/ por sus siglas en inglés, Statement of Applicability).
- Seguridad relativa a los recursos humanos.
- Seguridad física y del entorno.

- Protección de áreas físicas que contienen información.
- Control de acceso.

Dentro de esta fase se debe realizar una evaluación de riesgo ya que esto ayudara a identificar donde existen vulnerabilidades dentro de la empresa, en la figura 4 se explica el ciclo de vida de un riesgo.

Figura 4: Ciclo de vida de un riesgo, Fuente: (ISO27001.ES, 2005).

Hacer (Do): Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala, en la figura 5 se muestran las actividades que se tendrían que desarrollar en esta fase. (Bernal, 2013, párr. 4).

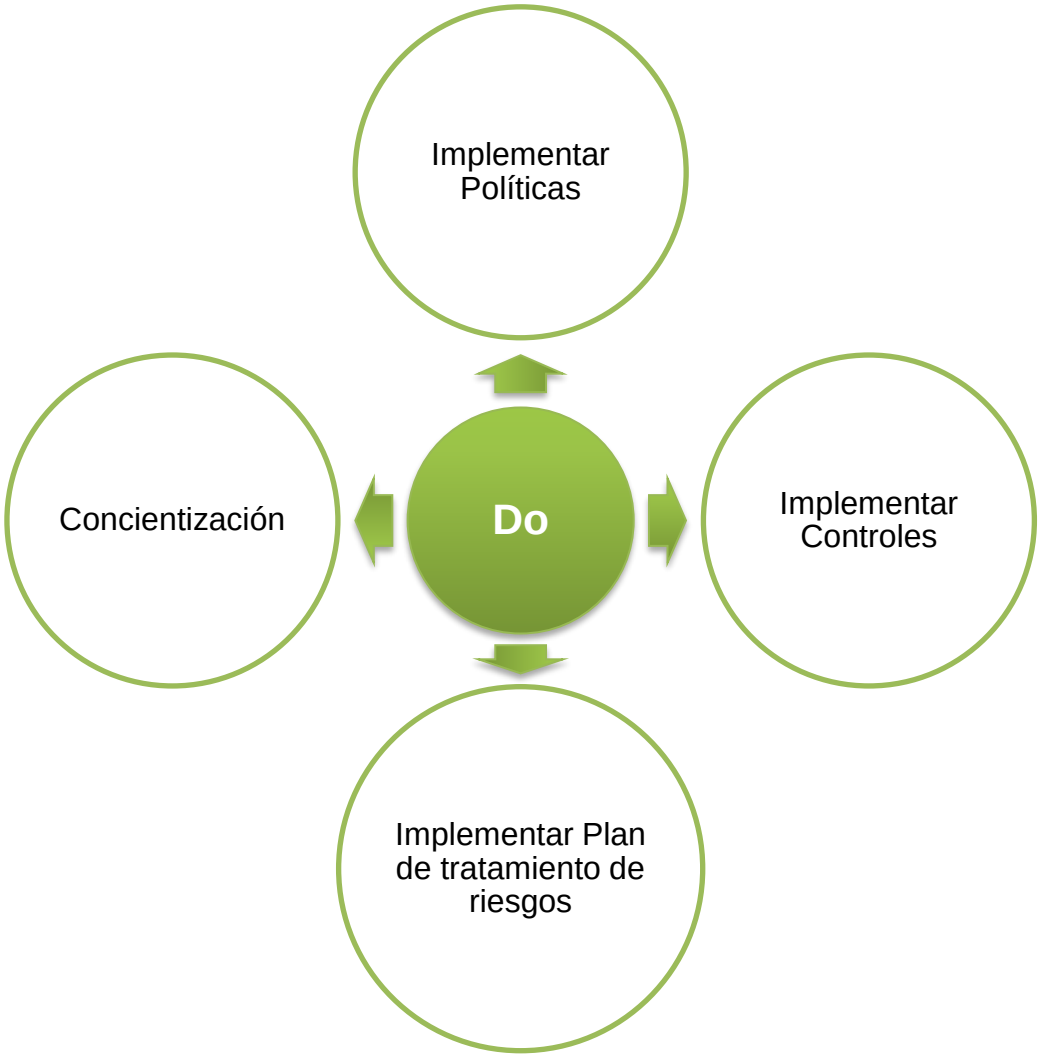

Figura 5: Actividades de la fase “Do” [Elaboración propia].

Una vez que se identificaron los riesgos existentes se tendrá que desarrollar un plan de tratamiento de riesgo, un riesgo puede tener 4 opciones que podrían tomar las empresas:

- Aplicar controles apropiados para mitigar el riesgo.
- Aceptar el riesgo identificado.
- Evitar el riesgo.
- Trasferir el riesgo.

Las documentos mínimos que se tienen que contemplar dentro del SGSI son :

Políticas Obligatorias

- Política de seguridad de la información.
- Política de control de acceso.
- Política de Clasificación de información.
- Política de seguridad para proveedores.
- Metodología de evaluación de riesgos.

Políticas no obligatorias de uso frecuente.

- Política de equipo de cómputo.
- Política de dispositivos móviles.
- Política de contraseñas.
- Política de eliminación y destrucción.
- Política de gestión del cambio.
- Política de transferencia de información.
- Política de uso de correo electrónico.

Un punto muy importante a la hora de implementar un SGSI es realizar un plan de concientización, alguno ejemplos que se pueden realizar para esta actividad son:

- Comunicados de seguridad.
- Trípticos.
- Capacitaciones.
- Encuestas.
- Auditorias.

Controlar o Verificar (Check): Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados, en la figura 6 se muestran las actividades que se tendrían que desarrollar en esta fase (Bernal, 2013, párr. 5).

Figura 6: Actividades de la fase “Check” [Elaboración propia].

Posterior a realizar la implementación de políticas y controles de seguridad se deberá llevar a cabo una revisión anual del SGSI denominada auditoría interna. Esta auditoría puede ser realizada por personal de la propia entidad. El auditor del sistema no debe haber participado en la implantación del mismo para mantener la objetividad y la independencia entre la implantación y la auditoría, las actividades que se contemplan en la auditoría interna son (Cárdenas, 2014):

- Preparación del programa de auditoría interna.
- Asignación de auditores internos.
- Otorgar independencia para el ejercicio de auditoria (segregación de funciones).
- Ejecución del ejercicio de auditoría.
- Entrega de resultados.

Una vez que se obtengan los resultados de la revisión del SGSI, se actualizarán los planes de seguridad y dicha actualización deberá realizar lo siguiente:

- Reevaluación de riesgos (Riesgo residual).
- Seguimiento a riesgos (RAP y RMP).

Para realizar el seguimiento de los riesgos se tendrán que crear 2 documentos uno para los RAP (Protocolo de aceptación de riesgos y otro para los RMP (Protocolo de mitigación de riesgos). Ejemplos de RAP y RMP son:

- Los RAP (Risk Acceptance Protocol) : La empresa no cuenta con recursos financieros para la implementar alguna herramienta de seguridad.
- RMP (Risk Mitigation Protocol) : La empresa desarrolla un proyecto de implementación de herramienta MDM para la mitigación del riesgo en dispositivos móviles.

Actuar (Act): Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas

mejoras a implantar, en la figura 7 se muestran las actividades que se tendrían que desarrollar en esta fase (Bernal, 2013, párr. 6).

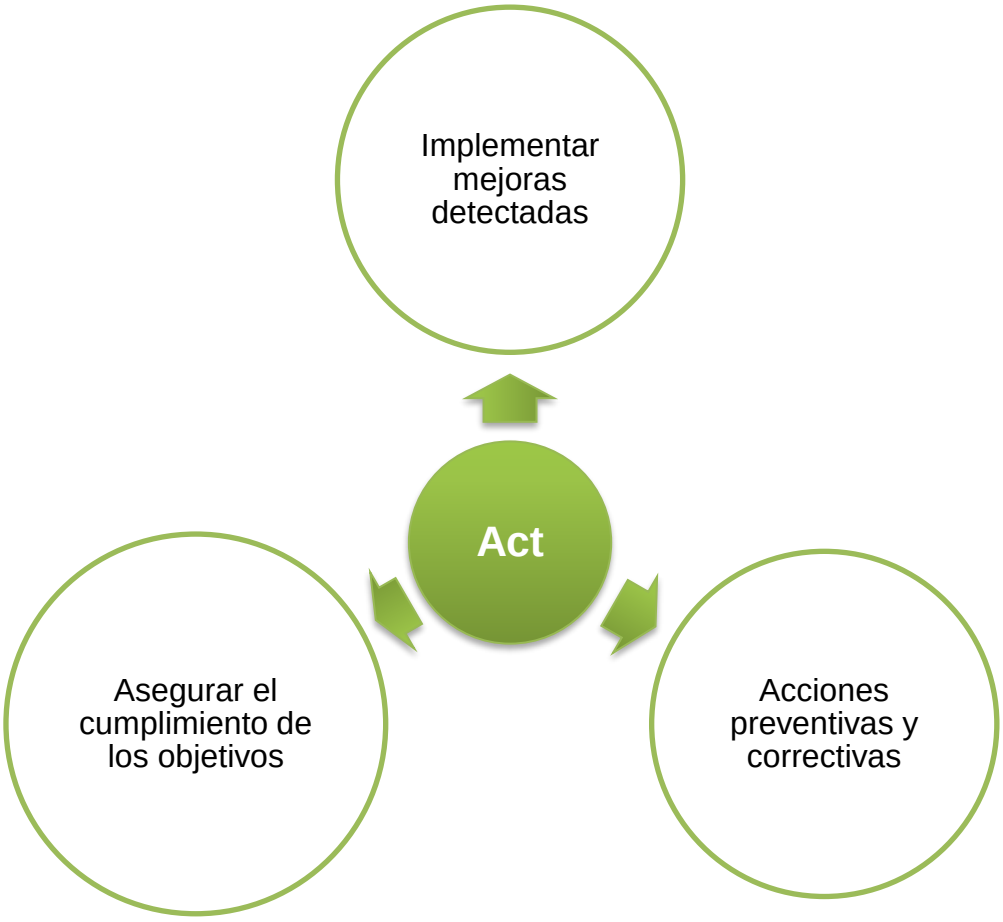

Figura 7: Actividades de la fase “Act” [Elaboración propia].

Una vez obtenidos los resultados de Auditoría, corresponde implantar las mejoras en las políticas, indicadores, procesos, etc. Se deberá establecer los tiempos de implementación de mejora continua.

La empresa debe tomar acciones para eliminar la causa de las no conformidades respecto de los requisitos del SGSI para evitar que éstas vuelvan a ocurrir, por lo cual se deberá implementar las acciones preventivas y correctivas.

El seguimiento a las no conformidades mayores, menores y observaciones y para fines de certificación de ISO 27001:2013, el plazo máximo para atender una no conformidad mayor es de tres meses.

Para finalizar se deberá asegurar el cumplimiento de los objetivos que se establecieron antes de implementar el SGSI, para esto se realizara lo siguiente:

- Validar que los controles implementados cumplan con el objetivo del Sistema de Gestión de Seguridad de la Información.
- Actualizar los objetivos del Sistema de Gestión de Seguridad de la Información.
- Actualizar los controles, políticas, procesos, etc. con la finalidad de mejora en el Sistema de Gestión de Seguridad de la Información.

Para entender de una mejor forma la relación de ciclo PDCA y el sistema de gestión de la información en la figura 8 se muestra las relación de las fase PDCA versus los dominios del SGSI.

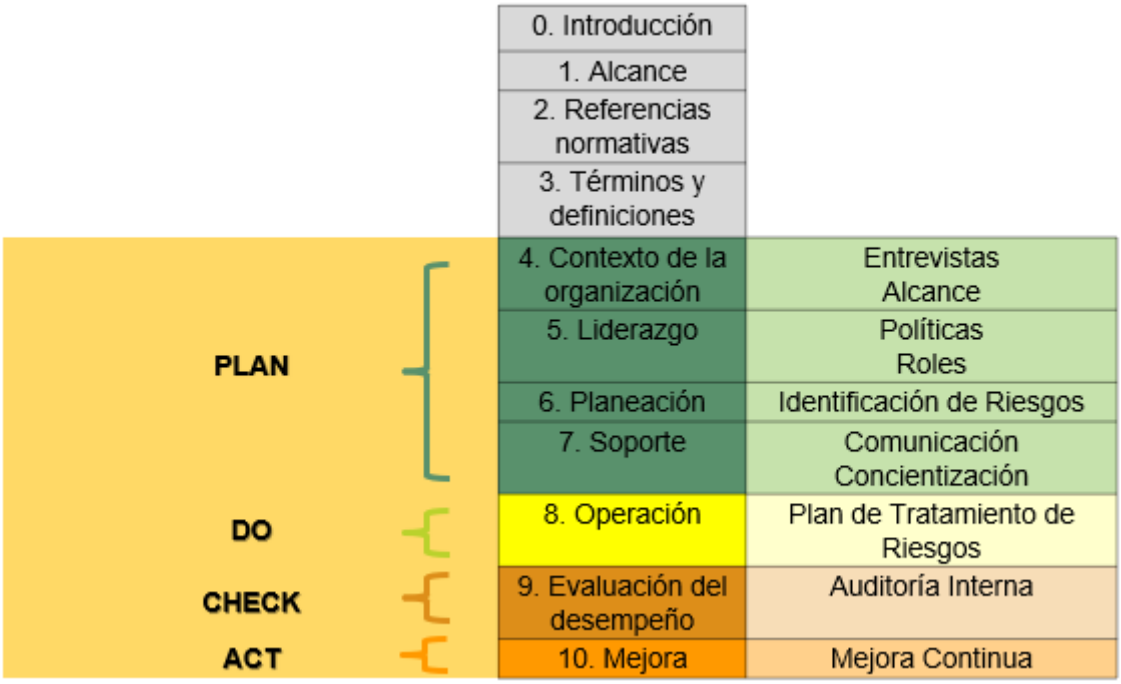

Figura 8: Relación entre el ciclo PDCA y el SGSI [Elaboración propia].

Las ventajas de implementar un Sistema de Gestión de Seguridad de la Información son:.

- Genera credibilidad y confianza a los clientes y otras partes interesadas.
- Establece un método de gestión de seguridad claro y estructurado que cumpla con las regulaciones, leyes y requisitos de la industria.
- Reduce el riesgo de pérdida, robo o daño de información luego de incidentes graves (cautela y debida diligencia) que puedan continuar con las actividades.
- Optimiza costos, la imagen de la organización, detecta y minimiza riesgos, genera mayores ingresos.

Los beneficios principales de una empresa certificada en ISO 27001:20013 son los siguientes:

- Produce una sensibilización del personal en relación con la importancia de la correcta manipulación de la información.
- Reduce los costos que se encuentran vinculados a todos los incidentes y se consiguen minimizar las primas de seguros.

A continuación, la tabla 24 presenta una comparación entre los controles de la **Ley Fintech** y los controles de ISO 27001 con la finalidad de que las empresas visualicen los controles que ayudarán a complementar la seguridad de su empresa.

Tabla 24. Controles ISO VS Controles **Ley Fintech** [Elaboración propia]

ID control ISO27001	Descripción de los controles de ISO 27001	Controles Ley Fintech
A.5.1.1	Políticas de seguridad de la información	63 párrafo 2
A.5.1.2	Revisión de las políticas de seguridad de la información	Sin control

A.6.1.1	Roles y responsabilidad de seguridad de la información	64, 64 - I, 64 - I párrafo 2, 64 - I párrafo 3, 65, 66-I - 66 -XII, 66 Segundo párrafo, 66 Tercer párrafo
A.6.1.2	Segregación de deberes	Sin control
A.6.1.3	Contacto con autoridades	Sin control
A.6.1.4	Contacto con grupos de interés especial	Sin control
A.6.1.5	Seguridad de la información en la gestión de proyectos	Sin control
A.6.2.1	Política de dispositivos móviles	Sin control
A.6.2.2	Teletrabajo	Sin control
A.7.1.1	Verificación de antecedentes	Sin control
A.7.1.2	Términos y condiciones del empleo	Sin control
A.7.2.1	Responsabilidades de la Alta Gerencia	Sin control
A.7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	Sin control
A.7.2.3	Proceso disciplinario	Sin control
A.7.3.1	Termino de responsabilidades o cambio de empleo	Sin control
A.8.1.1	Inventario de activos	63-II
A.8.1.2	Propiedad de activos	Sin control
A.8.1.3	Uso aceptable de los activos	Sin control
A.8.1.4	Devolución de activos	Sin control
A.8.2.1	Clasificación de la información	Sin control
A.8.2.2	Etiquetado de la información	Sin control
A.8.3	Manejo de los medios	63 III b, 63 - XIV párrafo 2
A.8.3.1	Gestión de medios removibles	63 III
A.8.3.2	Eliminación de medios	63 III
A.8.3.3	Transporte de medios físicos	Sin control

A.9.1	Requisitos de negocio para el control de acceso	63 - VI, 63 - XIV párrafo 3
A.9.1.1	Política de control de acceso	Sin control
A.9.1.2	Acceso a redes y servicios de red	Sin control
A.9.2	Gestión de acceso del usuario	63 III b, 63 - VI, 63 - VI - a
A.9.2.1	Registro y baja del usuario	Sin control
A.9.2.2	Provisión de acceso a usuarios	63 - VI - a
A.9.2.3	Gestión de derechos de acceso privilegiados	63 - VI - a
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Sin control
A.9.2.5	Revisión de derechos de acceso de usuarios	Sin control
A.9.2.6	Eliminación o ajuste de derechos de acceso	Sin control
A.9.3	Responsabilidades del usuario	63 - VI, 63 - VI - a
A.9.3.1	Uso de información de autenticación secreta	Sin control
A.9.4	Control de acceso al sistema y aplicaciones	63 - VI, 63 - VI - a, 63 – XI
A.9.4.1	Restricción de acceso a la información	Sin control
A.9.4.2	Procedimientos de inicio de sesión seguro	63 - VI - d
A.9.4.3	Sistema de gestión de contraseñas	Sin control
A.9.4.4	Uso de programas utilitarios privilegiado	Sin control
A.9.4.5	Control de acceso al código fuente de los programas	Sin control
A.10.1.1	Política para el uso de controles criptográficos	63 - VI - b, 63 - VI - c, 63 - XIV párrafo 3
A.10.1.2	Gestión de llaves	Sin control
A.11	Seguridad física y del ambiente	63 - VI - e
A.11.1.1	Perímetro de seguridad físico	Sin control
A.11.1.2	Controles físicos de entrada	Sin control
A.11.1.3	Seguridad de oficinas, habitaciones y facilidades	Sin control

A.11.1.4	Protección contra amenazas externas y del ambiente	Sin control
A.11.1.5	Trabajo en áreas seguras	Sin control
A.11.1.6	Áreas de entrega y carga	Sin control
A.11.2.1	Instalación y protección de equipo	Sin control
A.11.2.2	Servicios de soporte	Sin control
A.11.2.3	Seguridad en el cableado	Sin control
A.11.2.4	Mantenimiento de equipos	Sin control
A.11.2.5	Retiro de activos	Sin control
A.11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Sin control
A.11.2.7	Eliminación segura o reusó del equipo	Sin control
A.11.2.8	Equipo de usuario desatendido	Sin control
A.11.2.9	Política de escritorio limpio y pantalla limpia	Sin control
A.12.1.1	Documentación de procedimientos operacionales	Sin control
A.12.1.2	Gestión de cambios	63 III
A.12.1.3	Gestión de la capacidad	63 - X
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Sin control
A.12.2.1	Controles contra software malicioso	Sin control
A.12.3.1	Respaldo de información	63 - VII, 63 - XIV párrafo 3
A.12.4.1	Bitácoras de eventos	63 - VIII, 63 - XIV párrafo 2, 63 - XIV párrafo 3
A.12.4.2	Protección de información en bitácoras	63 - VIII
A.12.4.3	Bitácoras de administrador y operador	63 - VIII
A.12.4.4	Sincronización de relojes	Sin control
A.12.5.1	Instalación de software en sistemas operacionales	63 III, 63 V

A.12.6.1	Gestión de vulnerabilidades técnicas	63 III, 63 - IX párrafo 3, 64 - III, 64 -IV, 64 - IV - a, 64 -IV-b, 64 -IV-último párrafo, 64 -V, 64 -VI, 64 -VII
A.12.6.2	Restricciones en la instalación de software	Sin control
A.12.7.1	Controles de auditoría de sistemas de información	Sin control
A.13.1.1	Controles de red	63 III a
A.13.1.2	Seguridad de los servicios de red	63 III a
A.13.1.3	Separación en las redes	63 III a
A.13.2.1	Políticas y procedimientos para la transferencia de información	Sin control
A.13.2.2	Acuerdos en la transferencia de información	Sin control
A.13.2.3	Mensajería electrónica	63 - VI - f-3
A.13.2.4	Acuerdos de confidencialidad o no-revelación	Sin control
A.14.1	Requisitos de seguridad de los sistemas de información	63 IV
A.14.1.1	Análisis y especificación de requerimientos de seguridad	63 III
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Sin control
A.14.1.3	Protección de transacciones en servicios de aplicación	Sin control
A.14.2.1	Política de desarrollo seguro	63 III
A.14.2.2	Procedimientos de control de cambios del sistema	Sin control
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	63 III
A.14.2.4	Restricción de cambios en paquetes de software	Sin control
A.14.2.5	Principios de seguridad en la ingeniería de sistemas	Sin control

A.14.2.6	Entorno de desarrollo seguro	Sin control
A.14.2.7	Desarrollo tercerizado	Sin control
A.14.2.8	Pruebas de seguridad del sistema	Sin control
A.14.2.9	Pruebas de aceptación del sistema	Sin control
A.14.3.1	Protección de datos de prueba	Sin control
A.15.1.1	Política de seguridad de la información en las relaciones con el proveedor	Sin control
A.15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	63 - VI - f-5
A.15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	Sin control
A.15.2.1	Monitoreo y revisión de servicios del proveedor	63 - XIII
A.15.2.2	Gestión de cambios a los servicios del proveedor	63 - XIII
A.16	Gestión de incidentes de seguridad de la información	63 - IX, 63 - IX párrafo 2, 63 - XIV, 67, 67-I, 67-II, 68
A.16.1.1	Responsabilidades y procedimientos	63 - IX, 63 - IX párrafo 2
A.16.1.2	Reporte de eventos de seguridad de la información	63 - IX, 63 - IX párrafo 2
A.16.1.3	Reporte de debilidades de seguridad de la información	Sin control
A.16.1.4	Valoración y decisión de eventos de seguridad de la información	Sin control
A.16.1.5	Respuesta a incidentes de seguridad de la información	Sin control
A.16.1.6	Aprendizaje de incidentes de seguridad de la información	Sin control
A.16.1.7	Colección de evidencia	Sin control
A.17.1.1	Planeación de la continuidad de la seguridad de la información	Sin control
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Sin control

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Sin control
A.17.2.1	Disponibilidad de facilidades de procesamiento de información	Sin control
A.18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Sin control
A.18.1.2	Derechos de propiedad intelectual (IPR)	Sin control
A.18.1.3	Protección de registros	Sin control
A.18.1.4	Privacidad y protección de información personal identificable (PIR)	Sin control
A.18.1.5	Regulación de controles criptográficos	Sin control
A.18.2.1	Revisión independiente de seguridad de la información	64 -II, 64 -II- a,64 -II- b, 64 -II- c, 64 -II- d, 64 -II- e
A.18.2.2	Cumplimiento con políticas y estándares de seguridad	Sin control
A.18.2.3	Revisión del cumplimiento técnico	Sin control

Nota: En las celdas que aparece "**Sin control**" indica que esos controles no se contemplan dentro de la **Ley Fintech** ya que está solo contempla algunos temas de seguridad de la información de forma general a diferencia de ISO 27001 que abarca más temas y de forma más específica.

Si alguna empresa cuenta con la certificación de ISO27001 o de algún otro estándar es muy importante hacer una revisión a Fintech ya que al tener una certificación se podría dar cumplimiento a muchos de los controles de **Ley Fintech**, por lo cual el trabajo seria reduciría considerablemente y se contemplaría una mejor seguridad de la información. Para mantener el cumplimiento al estándar y a la **Ley Fintech** se necesitan realizar estas pruebas de forma periódica, así como la actualización de los documentos de forma periódica o ante cambios significativos en la empresa, las actividades que se mencionan se detallan a continuación en la figura 9:

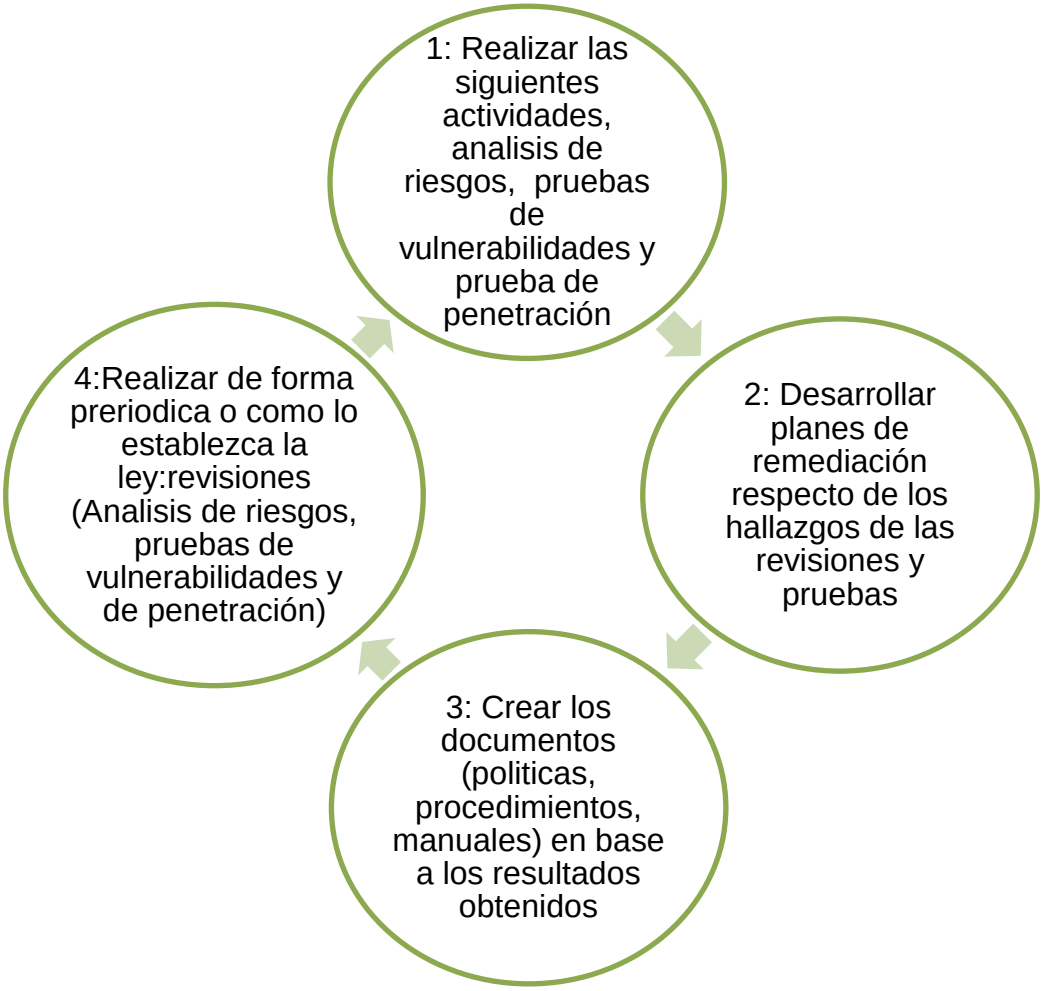

Figura 9: Pasos para implementar el estándar ISO27001 [Elaboración propia].

Para tener una mayor eficiencia en la implementación la **Ley Fintech** y apoyándonos con el estándar ISO27001, se recomienda que primero se conozca el estado de la empresa, para esto se necesita realizar como primeros pasos un análisis de riesgos y las pruebas de presentación y vulnerabilidades, ya que con los resultados que se obtengan se podrá realizar los documentos (políticas, procedimientos, manuales) en base a los resultados obtenidos de las pruebas, además de mitigar los riesgos identificados, en caso de que no se cuente con alguna persona con conocimientos previos a ISO27001 se recomienda revisar el estándar 27002 ya que en este se encuentra el cómo se pueden implementar cada uno de los controles de seguridad

CAPITULO 4.
VALIDACIÓN DEL INSTRUMENTO GUÍA APLICANDO UN CASO DE ESTUDIO

La empresa **TRASFER-TEC** realiza actividades de Institución de Fondos de Pago Electrónico, la cual hace emisiones de monederos electrónicos y soluciones financieras para empresas públicas y privadas, los tipos de tarjeta que genera son las siguientes:

- Emisión de tarjetas de vales de despensa
- Emisión de tarjetas para consumo de combustible
- Emisión de tarjetas de debito

Esta empresa cuenta con una aplicación en la cual los usuarios pueden gestionar o controlar sus tarjetas, las operaciones que pueden realizar son:

- Consultas de saldo y movimientos
- Pago de servicios (Luz, agua, internet, cable y teléfono)
- Solicitud de anticipos
- Retiro de dinero sin tarjeta

TRASFER-TEC requiere hacer una solicitud ante la CNBV para poder operar como una empresa Tecnología Financiera (**FINTECH**)**,** sin embargo, no conoce los requerimientos en temas de seguridad de la información que son necesarios para realizar la solicitud. Por este motivo el jefe de seguridad de la información de **TRASFER-TEC**, el cual cuenta con experiencia en implementación de ISO 27001 y 27002, utilizara el instrumento guía para poder cumplir con todos los requerimientos necesarios en temas de seguridad de la información.

Revisando el instrumento guía el jefe de seguridad se percató que como primer paso es necesario tener una serie de documentos en los cuales tienen que alinearse los controles que se mencionan en la **Ley Fintech**.

En base a su experiencia el jefe de seguridad de la información realizo un Assessment (Evaluación) para validar el nivel de cumplimiento que se tiene hasta el momento con la **Ley Fintech**, revisando la misma detecto que **TRASFER-TEC** solo cuenta con la política de seguridad de la información, política de atención a clientes, política de cifrado, Política de componentes de Red, Política de trasmisión de datos, Política de respaldos, Política de aplicaciones, Política de seguridad para gestión de proveedores, Política de autenticación y el área de seguridad de la información. Estaba trabajando en la creación del plan de continuidad de negocios, sin embargo, no se había realizado ningún análisis de riesgos previamente.

Basándose en el Instrumento Guía, obtuvieron el total de los documentos que se tienen que realizar previo a la solicitud, son un total de 10 documentos que hacen falta para dar cumplimiento a la **Ley Fintech** y 7 documentos que se recomiendan basados en el estándar ISO27001, esto basándose en las recomendaciones de del Instrumento Guía, se determina que primero se tiene que realizar un análisis de riegos y con base en los resultados se desarrollaran los documentos faltantes.

Como primeros pasos **TRASFER-TEC** realizo el análisis de riesgo en el cual se detectaron los siguientes riesgos, indicados en la tabla 25:

Tabla 25. Resultados del Análisis de Riesgos [Elaboración propia]

Riesgo	Descripción	Vulnerabilidad	Nivel de riesgo	Acciones
Robo de información	No se tiene un control de supervisión al personal que realiza mantenimientos.	Falta de proceso(s) de mantenimiento programado (preventivo) y correctivo	Medio	Generar una bitácora de acceso y generar las políticas para el acceso al SAIT

Denegación de servicios	No se contempla un proceso de supervisión a personal que realice actividades dentro del SITE, lo anterior puede materializar un daño de hardware o cableado	Falta de procesos de supervisión a personal, en caso de realizar actividades en SITE	Alto	Generar una bitácora de acceso y hacer un curso de concientización a las personas de mantenimiento
Robo y/o pérdida de información en dispositivos móviles	Políticas y procedimientos deficientes que regulen el uso de dispositivos móviles.	Políticas y procedimientos deficientes a dispositivos móviles	Medio	Generar una política de uso de dispositivos móviles, así como actualizar la responsiva.
Acceso no autorizado	No se tiene definido los criterios para el acceso a zonas de trabajo, lo anterior es realizado por una sola persona	Control de acceso sin criterios definidos	Alto	Generar una política de solicitud de accesos, así como la correcta generación de responsabilida-des
Pérdida de información	Colaboradores con deficiencia en conocimiento en materia de seguridad de la	Falta de cultura y concientización en materia de seguridad de la información.	Alto	Crear campañas y cursos de concientización

	información (capacitaciones débiles)			
Fuga y/o Robo de información	Falta de apoyo en las direcciones para la aceptación de todas las políticas de seguridad.	Falta de cultura y concientización en materia de seguridad de la información.	Medio	Crear campañas y políticas más especificas
Incontinuidad de la operación	Faltan controles de seguridad física en SITE (sensor de humedad, ubicación vulnerable)	Controles físicos deficientes en SITE	Medio	Aplicar los controles de seguridad física y documentar dichos controles.

Con base en los datos obtenidos del análisis de riesgos se obtuvieron los siguientes resultados (Figura 10):

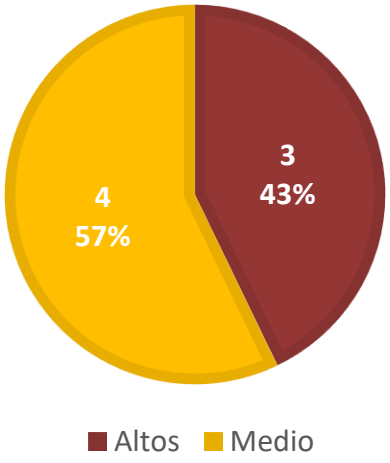

Figura 10: Resultados de análisis de riesgos [Elaboración propia].

Se detectaron 3 riesgos altos, 4 riesgos medios, de los cuales se tendrán que atender por prioridad, los documentos que se necesitan crear para dar cumplimiento a la ley Fintes son los siguientes:

- Evaluación de riesgos: Este requerimiento se deberá documentar, el cual deberá contar con la metodología que se utilizó, los planes de remediación que se aplicaran y establecer el periodo en el que se ejecutara nuevamente para validar la mitigación de los riesgos o identificar si existen nuevos.

- Política de control de acceso: Este documento se contempla para poder mitigar un riesgo detectado, en el cual se deberán implementar controles de seguridad tanto físicos como lógicos para la gestión de control de accesos.

- Política de seguridad física: Partiendo del riesgo detectado (Incontinuidad de la operación) se deberán implementar los controles de seguridad en SITE (sensor de humedad, ubicación vulnerable), así como documentar dicho controles en una política oficial.

- Política de dispositivos móviles: Debido a que **TRASFER-TEC** utiliza dispositivos móviles se identificó el riesgo (Robo y/o pérdida de información en dispositivos móviles), por lo que se deberán establecer controles de seguridad para los empleados de la institución que tengan acceso algún dispositivo móvil.

- Política de responsabilidades del director general: Dentro de las responsabilidades del director general se deberá contemplar la aprobación de los documentos (Política, procedimientos, manuales) ya que ésta es una parte fundamental para cumplir con todos los requerimientos que se solicitan en la **Ley Fintech**.

- Plan de capacitación, concientización: El tema de concientización es una parte muy importante ya que es necesario que todo el personal este consciente de los riesgos y los controles que se pueden aplicar para evitar o disminuir dichos riesgos, para llegar a esto es necesario impartir capacitaciones

periódicas ya sea con apoye de comisados vía correo, o folletos impresos en donde se hagan recomendaciones de seguridad de la información.

- Política de protección de pistas de auditoría: El registro de los eventos es fundamental en casos que existen incidentes de seguridad ya que con estos se pueden obtener las causas de dichos incidentes.

- Políticas de seguridad para la atención y respuesta a incidentes: Se deberá tener documentados los pasos que se deben de seguir en caso de que ocurra algún incidente de seguridad, ya que sin esto el impacto que pueden tener los incidentes podrían ser de gravedad.

- Políticas de seguridad para escaneos de vulnerabilidades e intrusión: Para poder tener una seguridad óptima es necesario probar regularmente los procesos y sistemas de seguridad.

- Política de responsabilidades del CISO: El Ciso es una pieza fundamental para el cumplimiento en la seguridad de la información por lo cual se deben establecer las responsabilidades que tendrá.

Una vez identificados los documentos faltantes y los riesgos, la empresa **TRASFER-TEC** deberá trabajar en la creación de dichos documentos y en los planes de remediación para realizar la solicitud ante la CNBV y poder operar como una empresa Financiera Tecnológica.

CAPITULO 5.
CONCLUSIONES

Las empresas de Tecnología Financiera (Fintech) en México ha ido incrementando con el tiempo ya que actualmente se realiza una gran cantidad de movimientos bancarios de forma digital. Las Fintech desarrollan herramientas utilizando las nuevas tecnologías para mejorar los procesos dentro del área de las finanzas, la cuales ofrecen diversas operaciones, entre ellas están las siguientes:

- Administración de finanzas,
- Préstamos,
- Remesas,
- Financiamiento colectivo o crowdfunding,
- Gestión de inversores,
- Educación financiera,
- Ahorro,
- Seguros.

El hecho de que existan estas operaciones digitales abre un mundo para posibles riesgos e incidentes de seguridad de la información para las Fintech, por este motivo los bancos o empresas se tienen que preparar para cualquier incidente que se pueda presentar.

En México la Comisión Nacional Bancaria y de Valores es la encargada de regular, supervisar, autorizar y sancionar sobre las entidades que integran el sistema financiero mexicano, esta contempla diversas leyes o normativas para las empresas bancarias como por ejemplo la **Ley Fintech** y la Circular única de Bancos (CUB), estas se aplicaran dependiendo de las operaciones que realice cada empresa.

Es necesario que se tenga un marco legal para que las empresas puedan ofrecer seguridad y efectividad en los sistemas, así como prevenir el lavado de dinero y financiamiento del terrorismo. Por ese motivo fue que el 9 de marzo del 2018 se creó la ley que regularía a las instituciones Fintech **"Ley Fintech"**. La CNBV en conjunto con la Comisión Nacional para Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) son las facultadas para regular, supervisar, autorizar y sanción a las instituciones Tecnologías Financieras.

El instrumento Guía se creó con la finalidad de orientar a las instituciones que busquen operar como Tecnología Financiera, apoyando a identificar los requerimientos mínimos que se necesitan para hacer la solicitud ante la Comisión Nacional Bancaria de Valores (CNBV), así como que las mimas empresas puedan realizar este cumplimiento sin necesidad de contratar a terceros, esto aplicaría solo si las empresas cuentan con personal con conocimientos previos en los estándares que se mencionan dentro del Instrumento Guía.

En esta guía se describieron los documentos necesarios para realizar la solicitud y aunque existe La GUÍA PARA LA SOLICITUD DE AUTORIZACIÓN PARA LA ORGANIZACIÓN Y OPERACIÓN DE INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO, en esta solo se mencionan 12 documentos, en los cuales no se contemplan el total de los requerimientos de la **Ley Fintech** por tal motivo se realizó la alineación a los requerimientos que solicita la **Ley Fintech** para brindar mayor claridad a las instituciones en como poder cumplir ante la **Ley Fintech**.

Aunque el instrumento Guía define los documentos base para dar cumplimiento a la **Ley Fintech** esto no quiere decir que si alguna empresa ya cuenta con políticas, procedimientos, manuales, con diferentes nombres a los que se definieron en este documento, esto no quiere decir que incumpla con las ley ya que cada empresa es diferente y cuenta con diferentes servicios, áreas, proceso o diferentes roles a los que se definen en la ley fintech, esta guía les

puede ayudar a validar cuales son los controles o documentos que posiblemente le falten.

El tema de seguridad de la información se reforzo con el estándar ISO27001, el cual nos proporciona los pasos que se deben seguir para la ejecución de un Sistema de gestión de seguridad de información, así como mayor profundidad en los controles de seguridad.

El instrumento guía se probó mediante la aplicación de un caso de estudio, en el que se demostró que al utilizar este instrumento guía las Instituciones Tecnológicas Financieras podrán visualizar de forma general los documentos necesarios, así como su alineación con cada uno de los requerimientos en temas de seguridad de la información que establece la **Ley Fintech**, esto le ayuda mucho a las instituciones ya que con esto no omitirán ningún requerimiento y podrán cumplir con todo los puntos de seguridad de la información.

El Instrumento guía se complementó con el estándar de seguridad ISO27001 y al momento de probar el caso de estudio este tema tuvo mucha relevancia ya que con apoyo del estándar se realizaron las etapas de la implementación de forma que mediante se iban haciendo las actividades se mitigaba o atacaban los riesgos que se detectaron en el análisis de riesgo.

Con la combinación la **Ley Fintech** y del estándar ISO27001 se generó una Guía robusta en temas de seguridad de la información y esto les proporciona a las instituciones un valor agregado para sus servicios y operaciones, ya que si implementan estos dos podrán ofrecer seguridad a sus clientes.

CAPITULO 6.

REFERENCIAS DE CONSULTA

Bernal, J. (2013) Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. Recuperado de https://www.pdcahome.com/5202/ciclo-pdca/

Cárdenas Guillen, N. (2014) Manual para la aplicación del estándar ISO/IEC27001. Recuperado de http://ri.uaemex.mx/handle/20.500.11799/99986

Canales TI (2019). Fintech, vulnerables por uso intensivo de tecnología. Recuperado de https://itcomunicacion.com.mx/Fintech-vulnerables-por-uso-intensivo-de-tecnologia/

Comisión Nacional Bancaria y de Valores [CNBV] (2015). Descripción del Sector. Recuperado de https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/PARTICIPANTES_EN_REDES_DE_MEDIOS_DE_DISPOSICI%C3%93N/Paginas/DescripcionDelSector.aspx

Comisión Nacional Bancaria y de Valores [CNBV] (2018). LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA. Publicadas en el Diario Oficial de la Federación el 3 de septiembre del 2018 Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018

Comisión Nacional Bancaria y de Valores [CNBV] (s. f.). ¿Qué hacemos? Recuperado de https://www.gob.mx/cnbv/que-hacemos

Comisión Nacional Bancaria y de Valores [CNBV] (2019). DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INTITUCIONES DE

TECNOLOGÍA FINANCIERA. Recuperado de Disposiciones Fintech (cnbv.gob.mx)

Comisión Nacional Bancaria y de Valores [CNBV] (2019b). CNBV recibió 85 solicitudes de autorización para operar como Institución de Tecnología Financiera. Recuperado de https://www.gob.mx/cnbv/articulos/cnbv-recibio-85-solicitudes-de-autorizacion-para-operar-como-institucion-de-tecnologia-financiera

Comisión Nacional Bancaria y de Valores [CNBV] (2021). CNBV informa respecto al proceso de autorización de Instituciones de Tecnología Financiera. Recuperado de https://www.gob.mx/cnbv/articulos/cnbv-informa-respecto-al-proceso-de-autorizacion-de-instituciones-de-tecnologia-financiera?idiom=es

Comisión Nacional Bancaria y de Valores [CNBV] (2021). GUÍA PARA LA SOLICITUD DE AUTORIZACIÓN PARA LA ORGANIZACIÓN Y OPERACIÓN DE INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO Recuperado de https://www.gob.mx/cms/uploads/attachment/file/622658/Guia_Autorizacion_IFPE_-_Marzo_2021.pdf

Diario Oficial de la Federación (2010)Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Fernández de Marcos, Isabel Davara (coord.), Diccionario de protección de datos personales. Conceptos fundamentales, México, INAI, 2019. Recuperado de https://archivos.eleconomista.com.mx/files/2020/02/12/diccionario_pdp_digital.pdf

Fintech México (s. f.). Qué es Fintech. Recuperado de https://www.Fintechmexico.org/qu-esFintech

ISO/IEC27001:2013, “Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos, 2013.

ISO27000.ES (2005). Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información. Recuperado de https://www.iso27000.es/sgsi.html

KPMG (2020). 2019 Fintech100: Leading Global Fintech innovators. Recuperado de https://home.kpmg/pe/es/home/insights/2020/01/2019-Fintech100.html

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 17(47), 334-339.

Secretaría de Hacienda y Crédito Público [SHCP] (2018b). El sector Fintech y su regulación en México. Recuperado de https://www.gob.mx/shcp/articulos/el-sector-Fintech-ysu-regulacion-en-mexico

Velázquez Martínez, M. D. L. Á. (2020) Empresas Fintech, activos virtuales y la era digital: retos y oportunidades en México. *Revista iberoamericana de contaduría, economía y administración*,*9*(18), pp. 47 - 73

ANEXO 1.
CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE LA LEY FINTECH

En este anexo se mostrarán los controles en temas de seguridad de la información que se establecen en la **Ley Fintech**, la cual está dividida por 4 Títulos: 1: Disposiciones generales, 2: De la información y documentación adicional para solicitar la autorización para actuar como ITF, 3: De las instituciones de financiamiento colectivo y 4: De los reportes regulatorios. Sin embargo, en este documento solo se abarcará el titulo tercero el cual contiene los temas de seguridad de la información.

Titulo Tercero	
Capítulo V Del Plan de Continuidad de Negocio	
ID Control	**Documento Recomendado para su alineación**
59	Plan de continuidad de negocio
60	Plan de continuidad de negocio
61	Plan de continuidad de negocio
61 - I	Evaluación de riesgos
61 - II	Plan de continuidad de negocio
61 - III	Política de seguridad de la información
61 - IV	Política de seguridad de la información
61 - V	Política de seguridad de la información
62	Plan de continuidad de negocio
62 - I	Plan de continuidad de negocio
62 - II	Plan de continuidad de negocio
62 - III	Plan de continuidad de negocio
63 - III	Plan de continuidad de negocio

62 - IV	Plan de continuidad de negocio
62 - V	Plan de continuidad de negocio
62 - VI	Plan de continuidad de negocio
62 - VII	Plan de continuidad de negocio
63 - VII	Plan de continuidad de negocio

El capítulo VI de la **Ley Fintech** es la que contempla la mayor parte de los temas de seguridad de la información.

Capítulo VI	
ID Control	**Documento Recomendado para su alineación**
63	Política de responsabilidades del director general
63 - I	Política de seguridad de la información
63 - II	Política de aplicaciones
63 - III	Política de aplicaciones
63 - III - a	Política de componentes de Red
63 - III - b	Política de seguridad de la información
63 - III - c	Política de aplicaciones
63 - IV	Política de aplicaciones
63 - V	Política de aplicaciones
63 - VI	Política de control de acceso
63 - VI - a	Política de control de acceso
64 - VI - a	Política de control de acceso
63 - VI - a	Política de control de acceso
63 - VI - b	Política de cifrado
64 - VI - b	Política de cifrado
63 - VI - c	Política de control de acceso
63 - VI - d	Política de control de acceso
63 - VI - e	Política de seguridad física

63 - VI - f	Política de trasmisión de datos
63 - VI - f-1	Política de trasmisión de datos
63 - VI - f-2	Política de trasmisión de datos
63 - VI - f-3	Política de trasmisión de datos
63 - VI - f-4	Política de trasmisión de datos
63 - VI - f-5	Política de trasmisión de datos
63 - VI - f párrafo 2	Política de trasmisión de datos
63 - VI - párrafo 2	Política de trasmisión de datos
63 - VII	Política de respaldos Rollback
63 - VIII	Política de protección de pistas de auditoría
63 - VIII	Política de protección de pistas de auditoría
63 - IX	Políticas de seguridad para la atención y respuesta a incidentes.
63 - IX párrafo 2	Políticas de seguridad para la atención y respuesta a incidentes.
63 - IX párrafo 3	Políticas de seguridad para la atención y respuesta a incidentes.
63 - X	Política de seguridad de la información
63 - X párrafo 2	Política de seguridad de la información
63 - XI	Política de seguridad de la información
63 - XII	Política de seguridad de la información
63 - XIII	Política de seguridad de la información
63 - XIV	Políticas de seguridad para la atención y respuesta a incidentes.
63 - XIV párrafo 2	Políticas de seguridad para la atención y respuesta a incidentes.
63 - XIV párrafo 3	Política de seguridad de la información
63 - XV	Política de seguridad de la información
63 párrafo 2	Política de responsabilidades del director general
64	Política de responsabilidades del director general
64 - I	Política de responsabilidades del director general

64 - I párrafo 2	Política de responsabilidades del director general
64 - I párrafo 3	Política de responsabilidades del director general
64 -II	Política de responsabilidades del director general
64 -II- a	Política de responsabilidades del director general
64 -II- b	Política de responsabilidades del director general
64 -II- c	Política de responsabilidades del director general
64 -II- d	Política de responsabilidades del director general
64 -II- e	Política de responsabilidades del director general
64 -III	Políticas de seguridad para escaneos de vulnerabilidades
64 -IV	Políticas de seguridad para pruebas de intrusión
64 -IV-a	Políticas de seguridad para pruebas de intrusión
64 -IV-b	Políticas de seguridad para pruebas de intrusión
64 -IV-b	Políticas de seguridad para pruebas de intrusión
64 -IV-último párrafo	Políticas de seguridad para pruebas de intrusión
64 -V	Políticas de seguridad para escaneos de vulnerabilidades y Políticas de seguridad para pruebas de intrusión
64 -VI	Políticas de seguridad para escaneos de vulnerabilidades y Políticas de seguridad para pruebas de intrusión
64 -VII	Políticas de seguridad para escaneos de vulnerabilidades y Políticas de seguridad para pruebas de intrusión
64 -VIII	Plan de capacitación, concientización
64 -IX	Política de responsabilidades del director general
IX - a	Política de responsabilidades del director general
IX - a	Política de responsabilidades del director general
IX - b	Política de responsabilidades del director general
IX - c	Política de responsabilidades del director general
64 -X	Política de responsabilidades del director general
64 -XI	Política de responsabilidades del director general
65	Política de responsabilidades del CISO

65	Política de responsabilidades del CISO
65	Política de responsabilidades del CISO
65	Política de responsabilidades del CISO
65	Política de responsabilidades del CISO
66	Política de responsabilidades del CISO
66-I	Política de responsabilidades del CISO
66-II	Política de responsabilidades del CISO
66-III	Política de responsabilidades del CISO
66-IV	Política de responsabilidades del CISO
66-IV	Política de responsabilidades del CISO
66-V	Política de responsabilidades del CISO
66-VI	Política de responsabilidades del CISO
66-VII	Política de responsabilidades del CISO
66-VIII	Política de responsabilidades del CISO
66-IX	Política de responsabilidades del CISO
66-X	Política de responsabilidades del CISO
66-XI	Política de responsabilidades del CISO
66-XII	Política de responsabilidades del CISO
66-XIII	Política de responsabilidades del CISO
66 segundo párrafo	Política de responsabilidades del CISO
66 tercer párrafo	Política de responsabilidades del CISO
67	Políticas de seguridad para la atención y respuesta a incidentes.
67-I	Políticas de seguridad para la atención y respuesta a incidentes.
67-I	Políticas de seguridad para la atención y respuesta a incidentes.
67-I	Políticas de seguridad para la atención y respuesta a incidentes.
67-II	Políticas de seguridad para la atención y respuesta a incidentes.
67-II	Políticas de seguridad para la atención y respuesta a incidentes.

68	Políticas de seguridad para la atención y respuesta a incidentes.
68	Políticas de seguridad para la atención y respuesta a incidentes.

El capítulo VII de la **Ley Fintech** contienen los requisitos sobre como el uso de los medios electrónicos.

Capítulo VII	
ID Control	**Documento Recomendado para su alineación**
69	Política de seguridad de la información
69-I	Política de seguridad de la información
69-II	Política de seguridad de la información
69-III	Política de seguridad de la información
69-IV	Política de seguridad de la información
69-V	Política de seguridad de la información
69-VI	Política de seguridad de la información
69-VII	Política de seguridad de la información
69-VIII	Política de seguridad de la información
70	Política de autenticación
I	Política de autenticación
II	Política de autenticación
71	Política de autenticación
71-I	Política de autenticación
71-II	Política de autenticación
71-III	Política de autenticación
71-IV	Política de autenticación
71-V	Política de autenticación
72	Política de autenticación
72-I	Política de autenticación
I - a	Política de autenticación

I - b	Política de autenticación
I - b - i	Política de autenticación
I - b - ii	Política de autenticación
I - b - iii	Política de autenticación
I - b - iv	Política de autenticación
72-II	Política de autenticación
72-II-a	Política de autenticación
72-II-b	Política de autenticación
72-II-c	Política de autenticación
72-II-d	Política de autenticación
72-II-d	Política de autenticación
72-III	Política de autenticación
72-III	Política de autenticación
73	Política de autenticación
73-I	Política de autenticación
73-II	Política de autenticación
73-III	Política de autenticación
74	Política de autenticación
74-I	Política de autenticación
I - a	Política de autenticación
I - b	Política de autenticación
74-II	Política de autenticación
I - a	Política de autenticación
I - b	Política de autenticación
75	Política de control de acceso
75-I	Política de control de acceso
I - a	Política de control de acceso
I - b	Política de control de acceso
75-II	Política de control de acceso

75-III	Política de control de acceso
76	Política de atención a clientes
76-I	Política de atención a clientes
76-II	Política de atención a clientes
76-III	Política de atención a clientes
76-IV	Política de atención a clientes
76-V	Política de atención a clientes
77	Política de atención a clientes
77-I	Política de atención a clientes
77-II	Política de atención a clientes
77-III	Política de atención a clientes
77-IV	Política de atención a clientes
78	Política de atención a clientes
79	Política de atención a clientes
80	Política de atención a clientes
I	Política de atención a clientes
II	Política de atención a clientes
81	Política de atención a clientes
81-I	Política de atención a clientes
81-II	Política de atención a clientes
81-III	Política de atención a clientes
81-IV	Política de atención a clientes
82	Política de atención a clientes
82 párrafo 2	Política de atención a clientes
82 párrafo 3	Política de atención a clientes
83	Política de seguridad en la información
83-I	Política de seguridad en la información
83-II	Política de seguridad en la información
83-III	Política de seguridad en la información

83-IV	Política de seguridad en la información
84	Política de seguridad en la información

En el capítulo VIII de la **Ley Fintech** se establecen los requerimientos sobre la contratación de proveedores.

Capítulo VIII	
ID Control	**Documento Recomendado para su alineación**
85	Política de seguridad para gestión de proveedores
85-I	Política de seguridad para gestión de proveedores
85-II	Política de seguridad para gestión de proveedores
86	Política de seguridad para gestión de proveedores
86-I	Política de seguridad para gestión de proveedores
86-II	Política de seguridad para gestión de proveedores
86-II	Política de seguridad para gestión de proveedores
86-II-a	Política de seguridad para gestión de proveedores
86-II-b	Política de seguridad para gestión de proveedores
86-II-c	Política de seguridad para gestión de proveedores
86-II-d	Política de seguridad para gestión de proveedores
86-II-e	Política de seguridad para gestión de proveedores
86-II-f	Política de seguridad para gestión de proveedores
86-II-g	Política de seguridad para gestión de proveedores
86-II-h	Política de seguridad para gestión de proveedores
86-II-i	Política de seguridad para gestión de proveedores
86-III	Política de seguridad para gestión de proveedores
86-III-a	Política de seguridad para gestión de proveedores
86-III-b	Política de seguridad para gestión de proveedores
86-III-c	Política de seguridad para gestión de proveedores
86-III-d	Política de seguridad para gestión de proveedores
86-III-e	Política de seguridad para gestión de proveedores

86-IV	Política de seguridad para gestión de proveedores
86-V	Política de seguridad para gestión de proveedores
86-VI	Política de seguridad para gestión de proveedores
86-VI - a	Política de seguridad para gestión de proveedores
86-VI - b	Política de seguridad para gestión de proveedores
86-VI - c	Política de seguridad para gestión de proveedores
86-VII	Política de seguridad para gestión de proveedores
86-VIII	Política de seguridad para gestión de proveedores
86-IX	Política de seguridad para gestión de proveedores
87	Política de seguridad para gestión de proveedores
87-I	Política de seguridad para gestión de proveedores
87-II	Política de seguridad para gestión de proveedores
87-III	Política de seguridad para gestión de proveedores
87-IV	Política de seguridad para gestión de proveedores
87-V	Política de seguridad para gestión de proveedores
87-V-a	Política de seguridad para gestión de proveedores
87-V-b	Política de seguridad para gestión de proveedores
87-V-c	Política de seguridad para gestión de proveedores
87-V-d	Política de seguridad para gestión de proveedores
87-V-e	Política de seguridad para gestión de proveedores
87-VI	Política de seguridad para gestión de proveedores
88	Política de seguridad para gestión de proveedores
88-I	Política de seguridad para gestión de proveedores
88-II	Política de seguridad para gestión de proveedores
88-III	Política de seguridad para gestión de proveedores
88-IV	Política de seguridad para gestión de proveedores
88-V	Política de seguridad para gestión de proveedores
88-VI	Política de seguridad para gestión de proveedores
88-VII	Política de seguridad para gestión de proveedores

88-VIII	Política de seguridad para gestión de proveedores
88-IX	Política de seguridad para gestión de proveedores

ANEXO 2.
GLOSARIO

Amenaza: Circunstancia o evento con la capacidad de causar daño a una organización

Autenticación: Verificación de una identidad declarada, es un proceso para asegurar la autenticidad de una persona o equipo. Esto puede ser proporcionado por un código, contraseña, token, datos biométricos, técnicos u otros.

Autorización: Procesos de concesión de acceso a un recurso, ya sea completo o restringido.

Backup. Típicamente respaldo de información o datos.

Centro de datos: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Clasificación: Es el proceso de clasificación de los sistemas de información, redes, aplicaciones y datos del negocio en función de su sensibilidad y criticidad, así como la asignación de propietario de éstos.

Clasificación de información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización (Público, privado y confidencial). Tiene como objetivo asegurar que la información reciba el nivel de protección adecuado.

Criticidad: Es el impacto que la ausencia de información o sistema podría tener sobre el negocio. Por ejemplo: Información pública (como precios de mercado) es absolutamente crítica para el negocio; por el contrario, información altamente confidencial (como currículos de candidatos) no son críticos para el negocio.

Control Interno: Comprende el plan y procesos de Empresa para salvaguardar sus activos, verificar la exactitud y fiabilidad de la información, promover la eficiencia operativa y fomentar la adhesión a las políticas internas.

Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

Datos: Cualquier información, independientemente de su formato, que está contenida y/o procesada por sistemas de información de la institución, así como redes de comunicaciones y medios de almacenamiento. Estos datos pueden residir en muchos formatos incluyendo copias impresas, medios magnéticos, ópticos, microfichas, almacenamiento en línea, materiales físicos, etc.

Datos de clientes: Son todos los datos que identifican a un cliente, tales como razón social, nombre, dirección, número de teléfono, URL, RFC, etc. Los datos del cliente se clasifican como "A" y se consideran confidenciales.

Datos sensitivos de clientes: Son los datos del cliente, junto con información de su cuenta, tal como el número de cuenta, saldo, historial de crédito, etc. Los datos sensitivos de los clientes también se clasifican como "A" y se consideran altamente confidenciales.

Desarrollo seguro: Conjunto de adopción de buenas prácticas, actividades, métodos y herramientas que la empresa utiliza para desarrollar y mantener el software y sus productos, considerando la seguridad de la información.

Disponibilidad: es la propiedad para que la información sea accesible en cualquier momento que sea requerida.

Equipo desatendido: Equipo sin persona responsable del mismo.

Escritorio limpio: Se refiere a que no haya información sensible tanto en el escritorio físico digital o virtual.

Evaluación de riesgo: Proceso de ponderación de la relación costo-beneficio de asegurar un activo de información en relación con el valor de ese activo a la

organización. Hay una serie de medidas que se pueden emplear para proteger los activos de información, sin embargo, la rentabilidad de estas medidas debe ser evaluada cuidadosamente.

Gestión de riesgos:

1. Evaluación de riesgos.
2. Mitigación de riesgos.
3. Monitoreo de Riesgos.

Hacking ético. Conjunto de habilidades para detectar y explotar vulnerabilidades en un sistema hardware o software. Para ello se emplean conocimientos de redes, programación y base de datos entre otros y se ejecutan determinadas herramientas y dispositivos hardware y software.

Incidente de Seguridad: Cualquier evento que tenga o pueda tener como resultado la pérdida o daños a los activos de la organización, o una acción que viole los procedimientos de seguridad de la organización.

Infracción: Intrusión no autorizada en los activos de información de empresa que pueden o no implicar el uso no autorizado de dichos activos

Información: Conocimiento, inteligencia, hechos o datos. Esto puede incluir información electrónica, creada, procesada, almacenada, o transmisión entre computadoras, dispositivos de comunicación o en papel. La información puede guardarse físicamente en mesas, archiveros y cajones y/o residir en bases de datos, archivos de datos, unidades de disco, programas, bibliotecas, directorios, colas de transacción o ser transmitida a través de las líneas de datos.

Integridad: es la propiedad que busca proteger la información para que no sea modificada por alguien no autorizado.

Medios de almacenamiento: Dispositivos técnicos destinados a proveer espacio físico o virtual, para albergar información.

Mitigación de riesgos: Minimización de la exposición al riesgo a un nivel aceptable.

Monitoreo de riesgos: Actividad realizada con regularidad para asegurar la operación continua de las medidas de protección a los activos de información.

No-Empleado: Cualquier persona no contratada directamente por la empresa, como proveedores, consultores, personal temporal y visitantes.

Política: Es una amplia declaración de principios que presenta la posición administrativa para cada área de control definida y **debe** ser seguida (excepto cuando ha sido aprobada una excepción).

Proveedor: Persona o empresa que ofrece productos o servicios de almacenamiento de datos y procesamiento de datos, hardware, software, consultoría de negocios y personal de seguridad. Los servicios de un proveedor también incluyen aquellos que no pueden ser provistos por el mismo Banco, como los proveedores de servicios de Internet.

Procedimiento: Documenta un plan de acción o respuesta a una situación determinada. Los procedimientos están diseñados para garantizar que se cumplan los objetivos y las políticas se cumplan. Estos deben ser seguidos en todo momento, a menos que se apruebe excluirlos por una razón válida.

Relación con proveedores: interacción que la empresa tiene con las organizaciones que le suministran bienes y servicios, reportando beneficios a ambas partes.

Respaldos: es una copia de seguridad de información clasificada como confidencial y/o de uso interno.

Riesgo: La Agencia Española de Protección de Datos (AEPD)2081 establece que el riesgo se deriva de la exposición a amenazas, por lo que, para la mejor comprensión, lo define como “la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas”.

Riesgo de seguridad: La Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales (GISGSDP), publicada en junio de 2015, define al riesgo de seguridad como “potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización”

Rollback. Procedimiento para devolver la configuración al estado inmediatamente anterior.

Seguridad de la información: Es el conjunto de medidas preventivas y reactivas de la empresa y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Seguridad física: Se refiere al acceso a los activos de información tangibles que tienen un alto valor intrínseco para la empresa.

Seguridad lógica: Controles basados en software, encontrados comúnmente en sistemas de información que cumplen con las políticas y prácticas de seguridad de la empresa.

Sistemas de Información: Computadoras, instalaciones de comunicaciones y redes que almacenan, procesan, recuperan o transmiten datos e información, incluyendo programas, especificaciones y procedimientos para su operación y mantenimiento.

Usuario de la información: Es cualquier empleado, proveedor u otra persona autorizada que utilice la información durante su trabajo diario.

Violación: Queja o sospecha de excepción a la política, que se vuelve efectiva sólo después de una investigación

Vulnerabilidad: La falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas

KPMG: Es una red global de formas de servicios profesionales que ofrecen servicios de auditoría, de asesoramiento legal y fiscal, y de asesoramiento financiero y de negocio en 156 países.

IFPE: Instituciones de Fondos de Pago Electrónico

SOA: La Declaración de Aplicabilidad (SoA por sus siglas en inglés, Statement of Applicability) de la norma ISO 27001, de Sistemas de Gestión de Seguridad de la Información (SGSI), es un documento formado por la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la norma.