La Comisión Nacional Bancaria y de Valores, con fundamento en lo dispuesto por los artículos 48, primer párrafo, 54, primer párrafo, 56, segundo párrafo y 57 de la Ley para Regular las Instituciones de Tecnología Financiera, así como 4, fracciones XXXVI y XXXVIII; 16, fracción I y 19 de la Ley de la Comisión Nacional Bancaria y de Valores, y

**C O N S I D E R A N D O**

Que en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de las presentes disposiciones, la Comisión Nacional Bancaria y de Valores mediante resolución publicada en el Diario Oficial de la Federación el 24 de julio de 2017, reformó las Disposiciones de carácter general aplicables a las casas de bolsa para ampliar el plazo con el que cuentan las casas de bolsa para vender o reclasificar sus títulos conservados a vencimiento de 28 a 90 días;

Que a fin de estar en condiciones de hacer frente a riesgos y ataques que pudieran ocasionar afectaciones a las instituciones de financiamiento colectivo y a la realización de operaciones con sus clientes, resulta conveniente establecer el marco normativo sobre seguridad de sus sistemas e infraestructura tecnológica, así como determinar los controles internos que deberán tener, contando con un régimen que procure garantizar la seguridad de la infraestructura tecnológica en que se soportan sus operaciones y la confidencialidad, integridad y disponibilidad de la información, teniendo medidas específicas para proteger su información, otorgar certeza en su operación y continuidad de los servicios;

Que por otra parte, una de las características fundamentales de las instituciones de financiamiento colectivo es que precisamente operan a través de medios remotos de comunicación electrónica o digital, esto es, dispositivos tecnológicos para efectuar la transmisión de datos, aplicaciones informáticas, interfaces, páginas de Internet y similares, por lo que resulta indispensable a la luz del artículo 56 de la Ley para Regular las Instituciones de Tecnología Financiera, regular el funcionamiento y el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, incluyendo las normas atinentes a las formas de autenticar tanto a las propias instituciones como a sus clientes, cumpliendo con los principios de neutralidad tecnológica y protección al consumidor establecidos en la Ley;

Que en términos de la Ley para Regular las Instituciones de Tecnología Financiera, las instituciones de financiamiento colectivo podrán pactar con terceros la prestación de servicios necesarios para su operación, de conformidad con las disposiciones que para tal efecto dicte la Comisión Nacional Bancaria y de Valores, por lo que se establecen las normas atinentes a dicha contratación, así como aquellos servicios que requerirán de la autorización de la propia Comisión tomando en cuenta para ello la debida protección de la información sensible de los clientes de estas entidades financieras;

Que con el objeto de que los clientes cuenten con información necesaria para identificar los riesgos en que incurren por la celebración de operaciones y la toma de decisiones de inversión, es indispensable incorporar el régimen aplicable a las instituciones de financiamiento colectivo para la revelación de información sobre los solicitantes de financiamiento, acorde con la facultad con la que cuenta la Comisión Nacional Bancaria y de Valores sobre normas en materia de transparencia de los servicios de dichas entidades financieras;

Que, a la par, en términos de la Ley para Regular las Instituciones de Tecnología Financiera, una vez que se haya efectuado alguna operación en las instituciones de financiamiento colectivo, las propias instituciones deberán tener a disposición de los inversionistas que estén participando en dicha operación, la información acerca del comportamiento de pago del solicitante, de su desempeño o cualquier otra que sea relevante en términos de las disposiciones que para tal efecto dicte la Comisión Nacional Bancaria y de Valores;

Que en ese tenor, resulta indispensable establecer el contenido de la información, la forma y periodicidad de esta a fin de que los inversionistas cuenten en todo momento con aquella información que les permita dar continuidad a la operación en la que hayan participado, en congruencia con los principios establecidos en la propia Ley relativos a la protección al consumidor e inclusión financiera, y

Que a fin de que la Comisión Nacional Bancaria y de Valores cuente con la información correspondiente a las actividades y operaciones de las instituciones de tecnología financiera, se establece la obligación de presentar los reportes correspondientes, el responsable de su envío y de la calidad de su contenido, así como los plazos y medios para su presentación, ha resuelto expedir la siguiente:

**RESOLUCIÓN QUE MODIFICA LAS DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA**

**ARTÍCULO PRIMERO.-** Se **REFORMAN** los artículos 2, 50, fracción V, último párrafo y 51, segundo párrafo; se **ADICIONAN** al Título Tercero, el Capítulo VI a denominarse “De la seguridad de la información” que comprende los artículos 63 a 68; el Capítulo VII a denominarse “Del uso de medios electrónicos” que comprende los artículos 69 a 84; el Capítulo VIII a denominarse “De la contratación de servicios con terceros” que comprende los artículos 85 a 88; el Capítulo IX a denominarse “De la revelación de información” que comprende las Secciones Primera denominada “De la revelación de información en la publicación de solicitudes y proyectos” con los artículos 90 a 94, Segunda a denominarse “De la revelación de información del comportamiento de pago y desempeño del Solicitante o proyecto” con los artículos 95 a 97 y Tercera a denominarse “De la revelación de información al público en general” con el artículo 98; el Título Cuarto a denominarse “Reportes Regulatorios” con el Capítulo I a denominarse “Reportes en general” con los artículos 99 a 103 y el Capítulo II a denominarse “Medios de entrega” con el artículo 104; así como los Anexos 11, 12, 13, 14, 15, 16, 17, 18, 19 y 20; se **DEROGA** el artículo 48; y se **SUSTITUYEN** los Anexos 8 y 9 de las Disposiciones de carácter general aplicables a las instituciones de tecnología financiera, publicadas en el Diario de la Federación el 10 de septiembre de 2018, para quedar como sigue:

**TÍTULOS PRIMERO** y **SEGUNDO** . . .

**TÍTULO TERCERO** . . .

**Capítulos** **I** a **V** . . .

**Capítulo VI**

De la seguridad de la información

**Capítulo VII**

Del uso de medios electrónicos

**Capítulo VIII**

De la contratación de servicios con terceros

**Capítulo IX**

De la revelación de información

**Sección Primera**

De la revelación de información en la publicación de solicitudes y proyectos

**Sección Segunda** De la revelación del comportamiento de pago y desempeño del Solicitante o proyecto

**Sección Tercera** De la revelación de información al público en general

**TÍTULO CUARTO**

Reportes regulatorios

**Capítulo I**

Reportes en general

**Capítulo II**

Medios de entrega

**Anexos** **1** a **7** . . .

**Anexo 8** Instructivo para la obtención de las constancias electrónicas de conocimiento de riesgos.

**Anexo 9** Formato de manifestaciones respecto del cumplimiento de los requisitos para ser considerado como Inversionista Experimentado.

**Anexo 10** . . .

**Anexo 11** Incidentes de afectación en materia de seguridad de la información.

**Anexo 12** Informe de incidentes de seguridad de la información.

**Anexo 13** Indicadores de seguridad de la información.

**Anexo 14** Formato de información de sistemas y aplicativos.

**Anexo 15** Lineamientos para la revelación de información de Financiamientos Colectivos de Deuda de Préstamos Empresariales entre Personas y para el Desarrollo Inmobiliario.

**Anexo 16** Lineamientos para la revelación de información para Financiamientos Colectivos de Capital.

**Anexo 17** Información agregada de las instituciones de financiamiento colectivo para su revelación al público en general.

**Anexo 18** Reportes regulatorios que deberán presentar las instituciones de financiamiento colectivo.

**Anexo 19** Reportes regulatorios que deberán presentar las instituciones de fondos de pago electrónico.

**Anexo 20** Designación de responsables para el envío y calidad de la información.

“**Artículo 2.-** En adición a las definiciones contenidas en la Ley, para efectos de las presentes disposiciones se entenderá, en singular o plural, por:

I. Autenticación, al conjunto de técnicas y procedimientos utilizados para verificar la identidad de:

a) Un Cliente y su facultad para realizar operaciones a través del Medio Electrónico de que se trate, o de un Usuario de Infraestructura Tecnológica para acceder, utilizar u operar algún componente de la Infraestructura Tecnológica.

b) Una institución de financiamiento colectivo y su facultad para recibir instrucciones a través de un Medio Electrónico.

II. Bloqueo, al proceso mediante el cual la institución de financiamiento colectivo inhabilita el uso de un Factor de Autenticación o Identificador de Cliente de forma temporal o definitiva.

III. Cifrado, al mecanismo que deben utilizar las instituciones de financiamiento colectivo para proteger la confidencialidad de la información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.

IV. Compromisos de Inversión, a las aportaciones que los Inversionistas se hayan comprometido a realizar en favor de los Solicitantes durante el Plazo de Solicitud de Financiamiento Colectivo, con independencia de que las aportaciones correspondientes sean entregadas a las instituciones de financiamiento colectivo durante dicho plazo o a los Solicitantes con posterioridad a su término.

V. Cómputo en la Nube, al modelo de provisión externa de servicios de cómputo bajo demanda y en infraestructura compartida, independientemente de la ubicación física de la infraestructura tecnológica del tercero que provea el servicio, pudiendo ser entre otros uno o más de los siguientes esquemas de servicios digitales: de infraestructura como servicio, de plataforma como servicio o de software como servicio.

VI. Contingencia Operativa, a cualquier evento que dificulte, limite o impida a una institución de financiamiento colectivo prestar sus servicios o realizar aquellos procesos que pudieran tener una afectación a sus Clientes.

VII. Contraseña, a la cadena de caracteres alfanuméricos y especiales que autentica a un Cliente en el Medio Electrónico de la institución de financiamiento colectivo.

VIII. Cuentas Destino, a las cuentas receptoras de recursos dinerarios que los Clientes de la institución de financiamiento colectivo registren en el Medio Electrónico que corresponda para realizar Operaciones.

IX. Desbloqueo, al proceso mediante el cual la institución de financiamiento colectivo habilita el uso de un Factor de Autenticación o Identificador de Cliente que se encontraba bloqueado.

X. Dispositivo de Acceso, al equipo que permite a un Cliente acceder al Medio Electrónico que corresponda de la institución de financiamiento colectivo.

XI. Evento de Seguridad de la Información, a cualquier suceso, interno o externo, relacionado con Clientes, terceros contratados por la propia institución de financiamiento colectivo, personas y procesos operativos, así como con componentes de la Infraestructura Tecnológica, dispositivos, medios físicos, u otros elementos que almacenen información, entre otros, que pueda suponer una afectación en la confidencialidad, integridad o disponibilidad de la información que dicha institución gestione o conozca o en la propia Infraestructura Tecnológica.

XII. Factor de Autenticación, al mecanismo de Autenticación, tangible o intangible, basado en las características físicas del Cliente, dispositivos, o información que solo el Cliente posea o conozca.

XIII. Financiamiento Colectivo de Capital, a la operación de financiamiento colectivo mediante la cual los Solicitantes obtienen recursos por parte de los Inversionistas a cambio de títulos representativos de su capital social.

XIV. Financiamiento Colectivo de Copropiedad o Regalías, a la operación de financiamiento colectivo mediante la cual los Inversionistas y Solicitantes celebran entre ellos asociaciones en participación o cualquier otro tipo de convenio por el cual los Inversionistas adquieren una parte alícuota o participación en un bien presente o futuro, o en los ingresos, utilidades, regalías o pérdidas que se obtengan de la realización de una o más actividades o de los proyectos de los Solicitantes.

XV. Financiamiento Colectivo de Deuda de Préstamos Empresariales entre Personas, a la operación de financiamiento colectivo, en la que los Solicitantes son personas morales o personas físicas con actividad empresarial y los Inversionistas realizan aportaciones:

a) Con el fin de que los Solicitantes reciban un préstamo o crédito para financiar sus actividades, quedando obligados al pago del principal y, en su caso, accesorios a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación.

b) Con el objeto de efectuar una operación de arrendamiento financiero, en la que se adquiere un activo a nombre de los Inversionistas o de las instituciones de financiamiento colectivo a nombre propio, pero en representación de estos, y se da en arrendamiento financiero al Solicitante. Para efectos de la operación de arrendamiento financiero, se estará a lo dispuesto por la Ley General de Títulos y Operaciones de Crédito.

c) Con el fin de celebrar una operación de factoraje financiero, en la que adquieren parte de algún derecho de crédito que el Solicitante tenga a su favor, quedando el Solicitante como obligado solidario de su deudor, sin que dicho derecho derive de préstamos, créditos o mutuos que el Solicitante previamente haya otorgado. Para efectos de la operación de factoraje financiero, se estará a lo dispuesto por la Ley General de Títulos y Operaciones de Crédito.

XVI. Financiamiento Colectivo de Deuda de Préstamos Personales entre Personas, a la operación de financiamiento colectivo en la que el Solicitante es una persona física que obtiene en préstamo los recursos aportados por los Inversionistas, quedando obligado al pago del principal, y en su caso accesorios, a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación.

XVII. Financiamiento Colectivo de Deuda para el Desarrollo Inmobiliario, a la operación de financiamiento colectivo que tiene por objeto que los Inversionistas otorguen un préstamo o crédito a los Solicitantes destinado al financiamiento de actividades de desarrollo inmobiliario quedando obligados al pago del principal y, en su caso, accesorios a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación.

XVIII. Fondo de Capital Privado, al vehículo de inversión, fideicomiso, mandato, comisión o figuras similares constituidos bajo las leyes mexicanas o extranjeras, cuyo fin sea invertir en el capital de sociedades no listadas en las bolsas de valores al momento de la inversión para promover su desarrollo y otorgarles financiamiento.

XIX. Identificador de Cliente, a la cadena de caracteres alfanuméricos o especiales, información de un dispositivo o cualquier otra información que conozca tanto la institución de financiamiento colectivo como el Cliente, que permita identificar al propio Cliente en el Medio Electrónico de la institución de financiamiento colectivo.

XX. Incidente de Seguridad de la Información, a aquel Evento de Seguridad de la Información en la institución de financiamiento colectivo cuando actualice alguno de los siguientes supuestos:

a) Haya comprometido la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la Infraestructura Tecnológica con un efecto adverso para la institución de financiamiento colectivo, sus Clientes, terceros, proveedores o contrapartes, entre otros.

b) Vulnere la Infraestructura Tecnológica comprometiendo la información que procesa, almacena o transmite.

c) Constituya una violación de las políticas y procedimientos de seguridad de la información.

d) Represente la materialización de una pérdida, ya sea por extracción, alteración o extravío de la información; por fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información; por accesos no autorizados que deriven en el uso indebido de la información o de los sistemas; por fraude, robo, o en interrupción de los servicios, atentados contra las infraestructuras interconectadas, conocidos como ciberataques, entre otros.

XXI. Información Sensible, a la información personal de los Clientes que contenga nombres, domicilios, teléfonos, direcciones de correo electrónico o cualquier otro dato que identifique al Cliente, en conjunto con números de cuenta, números de tarjetas y demás datos de naturaleza financiera, así como Identificadores de Clientes o información de Autenticación.

XXII. Inversionista, a la persona física o moral que aporta recursos o activos virtuales a los Solicitantes para la celebración de operaciones de financiamiento colectivo.

XXIII. Inversionista Experimentado, a cualquiera de los siguientes:

a) Entidades financieras a que alude el artículo 21, tercer párrafo de la Ley, así como las demás entidades financieras que conforme a su régimen legal puedan actuar como Inversionistas en las Operaciones de que se trate.

b) Entidades financieras del exterior, siempre que la institución de financiamiento colectivo haya obtenido autorización de la CNBV para recibir o realizar transferencias en términos del artículo 10 de las presentes disposiciones.

c) Dependencias y entidades de la Administración Pública Federal.

d) Personas que manifiesten encontrarse en el supuesto señalado en el Anexo 9 de las presentes disposiciones.

XXIV. Inversionista Relacionado, aquel que manifieste ante las instituciones de financiamiento colectivo tener parentesco con el Solicitante por consanguinidad, afinidad o civil hasta el cuarto grado, o ser su cónyuge, concubino o concubinaria.

XXV. Ley, a la Ley para Regular las Instituciones de Tecnología Financiera.

XXVI. Medios Electrónicos, a los equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados, incluyendo la Plataforma, que las instituciones de financiamiento colectivo utilizan para prestar sus servicios.

XXVII. Número de Identificación Personal (NIP), a la Contraseña que autentica a un Cliente en el Medio Electrónico de la institución de financiamiento colectivo mediante una cadena de caracteres numéricos.

XXVIII. Órgano de Administración, al administrador único o al consejo de administración de una ITF.

XXIX. Plan de Continuidad de Negocio, al conjunto de estrategias, procedimientos y acciones que permitan, ante la verificación de Contingencias Operativas, la continuidad en las Operaciones, actividades o en la realización de los procesos críticos de las instituciones de financiamiento colectivo, o bien su restablecimiento oportuno, así como la mitigación de las afectaciones producto de dichas Contingencias Operativas.

XXX. Plan Director de Seguridad, al documento que establece la estrategia de seguridad de una institución de financiamiento colectivo a corto, mediano y largo plazo para procurar una correcta gestión de la seguridad de la información y evitar que los Eventos de Seguridad de la Información se materialicen en Incidentes de Seguridad de la Información.

XXXI. Plataforma, a las aplicaciones informáticas, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital que las ITF utilicen para operar con sus Clientes.

XXXII. Plazo de Solicitud de Financiamiento Colectivo, al período en que una solicitud de financiamiento colectivo puede mantenerse publicada en la Plataforma de una institución de financiamiento colectivo con el fin de ofrecer a los Inversionistas la celebración de una Operación con los Solicitantes.

XXXIII. Reporte de Información Crediticia, a cualquiera de los reportes de crédito emitidos por sociedades de información crediticia a que se refiere el artículo 36 Bis de la Ley para Regular las Sociedades de Información Crediticia, a saber:

a) El emitido por una sociedad de información crediticia en el que se incluya la información contenida en las bases de datos de las demás sociedades de información crediticia.

b) Los emitidos por cada una de las sociedades de información crediticia.

XXXIV. Restablecimiento de Contraseñas, al procedimiento mediante el cual el Cliente puede definir una nueva Contraseña o Número de Identificación Personal (NIP).

XXXV. Sesión, al periodo en el cual los Clientes podrán llevar a cabo consultas y Operaciones, una vez que hayan ingresado a la Plataforma de la institución de financiamiento colectivo con su Identificador de Cliente.

XXXVI. SITI: al Sistema Interinstitucional de Transferencia de Información, el cual forma parte de la oficialía de partes de la CNBV.

XXXVII. Solicitante, a la persona física o moral que hubiere requerido recursos o activos virtuales a los Inversionistas, a través de instituciones de financiamiento colectivo.

XXXVIII. UDI, a las unidades de cuenta llamadas “Unidades de Inversión” establecidas en el “Decreto por el que se establecen las obligaciones que podrán denominarse en Unidades de Inversión y reforma y adiciona diversas disposiciones del Código Fiscal de la Federación y de la Ley del Impuesto sobre la Renta”, publicado en el Diario Oficial de la Federación el 1 de abril de 1995, tal como ese sea modificado o adicionado de tiempo en tiempo.

XXXIX. Usuario de la Infraestructura Tecnológica, a la persona, Cliente o componente físico o lógico que acceda, utilice u opere algún componente de la Infraestructura Tecnológica de las instituciones de financiamiento colectivo.”

“**Artículo 48.-** Derogado.”

“**Artículo 50.-** . . .

I. a IV. . . .

V. . . .

. . .

En el caso de los Inversionistas Experimentados a que se refiere el inciso d) de la fracción XXIII del artículo 2 de las presentes disposiciones, las instituciones de financiamiento colectivo obtendrán la manifestación contenida en el Anexo 9 de estas disposiciones, así como la documentación comprobatoria, al inicio de su relación contractual o en el momento en que los Inversionistas soliciten obtener el carácter de Inversionista Experimentado conforme a las presentes disposiciones.

. . .

**Artículo 51.-** . . .

I. y II. . . .

La CNBV otorgará la autorización correspondiente siempre que la institución de financiamiento colectivo acredite que los términos de los préstamos o créditos que pretenda celebrar no pondrán en riesgo su solvencia y estabilidad financiera.

. . .”

“**Capítulo VI**

De la seguridad de la información

**Artículo 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 la institución de financiamiento colectivo, ya sea propia o provista por terceros, se apegue a los requerimientos siguientes:

I. Que cada uno de sus componentes realice las funciones para las que fue diseñado, desarrollado o adquirido.

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.

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.

Tratándose de componentes de comunicaciones y de cómputo, los aspectos de seguridad deberán incluir, al menos, lo siguiente:

a) 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. En particular, en aquellos segmentos con enlaces al exterior, tales como Internet, proveedores, autoridades, otras redes de la institución de financiamiento colectivo o matriz y otros terceros, todo ello referido a aquellos servicios definidos como críticos por la propia institución, ya sean sistemas de pagos, equipos de cifrado, autorizadores de Operaciones, entre otros, deberán considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (DMZ por sus siglas en inglés).

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.

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.

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.

1. Que cuente con las licencias o autorizaciones de uso, en su caso.

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 contando, al menos, con lo siguiente:

1. 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.

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.

Asimismo, se deberán prever 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.

b) Cifrado de la información conforme al grado de sensibilidad o clasificación 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.

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 las políticas y procedimientos 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.

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.

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.

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:

1. La veracidad e integridad de la información.

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.

3. Los protocolos de mensajería, comunicaciones y cifrado, los cuales deben procurar la integridad y confidencialidad de la información.

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.

5. La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones.

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.

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.

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.

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.

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.

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 a 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.

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 al nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la institución de financiamiento colectivo puedan verse afectados.

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.

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.

XI. Que cuente con controles automatizados o, en ausencia de estos, que se realicen controles compensatorios, tales como doble verificación y conciliación que, previo o posteriormente a la realización de la Operación de que se trate, minimicen el riesgo de eliminación, exposición, alteración o modificación de información, que se deriven de procesos manuales o semi-automatizados realizados por el personal de la institución de financiamiento colectivo, con el objetivo de prevenir errores, omisiones, sustracción o manipulación de información.

XII. Que tenga controles que permitan detectar la alteración o falsificación de libros, registros y documentos digitales relativos a las Operaciones.

XIII. Que cuente con procesos para medir y asegurar los niveles de disponibilidad y tiempos de respuesta, que garanticen la ejecución de las Operaciones realizadas; lo anterior, incluyendo los supuestos en que las instituciones de financiamiento colectivo contraten la prestación de servicios por parte de terceros para el procesamiento y almacenamiento de información.

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.

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.

Adicionalmente, las instituciones de financiamiento colectivo deberán mantener controles que eviten la filtración de la información correspondiente a la configuración de la Infraestructura Tecnológica, tales como direcciones IP, reglas de los cortafuegos, así como versiones de hardware y software.

XV. Que para la prestación de servicios de tecnologías de información a los Usuarios de la Infraestructura Tecnológica, en sus fases de estrategia, diseño, transición, operación y mejora continua, se proteja la integridad de la Infraestructura Tecnológica, así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por esta.

El director general o, en su caso, el administrador único será responsable de documentar en políticas y procedimientos lo previsto en este artículo.

**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:

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.

Para la aprobación de dicho plan, el director general o, en su caso, el administrador único deberá verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes y podrá contemplar los controles requeridos conforme a las disposiciones aplicables.

Tratándose de instituciones de financiamiento colectivo que cuenten con director general y consejo de administración, el primero deberá informar a dicho consejo el contenido del Plan Director de Seguridad, y contar con evidencia de su aprobación e implementación.

II. Llevar a cabo revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la Infraestructura Tecnológica. Estas revisiones deberán comprender, al menos, lo siguiente:

a) Mecanismos de Autenticación de los Usuarios de la Infraestructura Tecnológica.

b) Configuración y controles de acceso a la Infraestructura Tecnológica.

c) Actualizaciones requeridas para los sistemas operativos y software en general, previo a su implementación y una vez implementados.

d) Identificación de posibles modificaciones no autorizadas al software original.

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.

Las revisiones a que se refiere esta fracción deberán realizarse, por lo menos, una vez al año o antes si se presentan cambios significativos en la Infraestructura Tecnológica. Para determinar si se trata de un cambio significativo deberá obtenerse, al efecto, la opinión del oficial en jefe de seguridad de la información.

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 al resultado del ejercicio de clasificación de información que determine la institución de financiamiento colectivo. El calendario deberá prever la revisión trimestral 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 responsable de vigilar que se realice la prueba de escaneo de vulnerabilidades, previo a su puesta en producción.

IV. Contratar a un tercero independiente, con personal que cuente con capacidad técnica comprobable mediante certificaciones de la industria en la materia, para la realización de pruebas de penetración en los diferentes sistemas y aplicativos de la institución de financiamiento colectivo con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los Clientes y de la propia institución de financiamiento colectivo. Tal revisión deberá incluir la verificación de la integridad de los componentes de hardware y software que permitan detectar alteraciones de estos. Dichas pruebas deberán considerar, al menos, lo siguiente:

a) Su alcance y metodología, debiendo ser validados por el oficial en jefe de seguridad de la información.

b) Ser realizadas, al menos, dos al año sobre sistemas o aplicativos distintos, o bien, cuando lo ordene la CNBV habiendo detectado vulnerabilidades o factores que puedan los sistemas y aplicativos o la información recibida, generada, procesada, almacenada o transmitida en estos. En este último caso, la CNBV determinará el alcance de las pruebas, así como los plazos para realizarlas.

Se podrán realizar pruebas adicionales a juicio del director general o, en su caso, el administrador único, con opinión del oficial en jefe de seguridad de la información, cuando existan cambios significativos en los sistemas y aplicativos, o realizarlas sobre sistemas y aplicativos previamente llevados a cabo cuando existan vulnerabilidades críticas.

El director general o, en su caso, el administrador único de la institución de financiamiento colectivo, deberá enviar a la CNBV dentro de los veinte días hábiles de haber sido finalizadas las pruebas, un informe con las conclusiones de estas. En el envío que se realice, se deberá procurar el uso de mecanismos que impidan el acceso al contenido de este informe por personal no autorizado.

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.

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.

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.

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.

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.

VIII. Implementar programas anuales de capacitación, así como de concientización en materia de seguridad de la información, dirigidos a todo el personal y a 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.

IX. Realizar, de manera proactiva e iterativa, la búsqueda de alertas de fraude, así como de amenazas, tales como campañas de correos fraudulentos, sitios de Internet falsos, divulgación de bases de datos con información de los Clientes, aplicaciones móviles y, en su caso, alteración de los dispositivos utilizados para la realización de Operaciones, entre otros, que pudieran afectar a la seguridad de la información de los Clientes, al igual que acciones para su protección considerando, al menos, lo siguiente:

a) La continua investigación, recopilación, procesamiento y análisis de información que provenga de cualquier fuente relacionada con los productos y servicios que ofrezca la institución de financiamiento colectivo, que pueda constituir indicios o evidencias de que se han evadido los controles de seguridad, representando una amenaza para la información o recursos del Cliente.

Los indicios o evidencias a que se refiere el párrafo anterior, se mantendrán en un registro, el cual deberá contenerse en la base de datos a que se refiere el primer párrafo del artículo 68 de estas disposiciones.

b) La implementación de procesos proactivos para proteger la información o recursos de los Clientes cuando se presenten los indicios o evidencias señaladas en el inciso a) anterior, tales como bloqueo y reposición de medios de disposición, cambio de datos de autenticación y notificaciones, entre otros.

c) Que cuente con procedimientos de comunicación y recomendaciones de seguridad con los Clientes afectados, para informarles sobre los procesos de remediación que la institución de financiamiento colectivo llevará a cabo y, en su caso, las medidas que el propio Cliente debe adoptar, tales como cambio de contraseñas, verificación de saldos y movimientos, instalación de antivirus, instalación de software de detección de programas maliciosos, revisión de dispositivos y reinstalación de aplicaciones, entre otros.

Los términos y condiciones para realizar los procesos mediante los cuales se realicen las actividades señaladas en la presente fracción, deberán documentarse en los respectivos manuales de políticas y procedimientos, en los que deberá preverse que la institución de financiamiento colectivo mantendrá evidencia de la realización de dichas actividades.

X. Implementar controles que permitan a la institución de financiamiento colectivo asegurar la confidencialidad, integridad y disponibilidad de la información de los Clientes y de la propia institución de financiamiento colectivo o el acceso a la Infraestructura Tecnológica, por parte de sus empleados o personal que tengan acceso a ella, que garanticen que dicha información e Infraestructura Tecnológica no sean alterados o causen una afectación a la institución de financiamiento colectivo o a los recursos de sus Clientes. Dichos controles deberán implementarse desde la contratación respectiva y hasta su terminación.

XI. Establecer políticas y procedimientos para asegurar que el oficial en jefe de seguridad de la información obtenga de las unidades de negocio de la institución de financiamiento colectivo, la información y documentación necesarias para el cumplimiento de las funciones establecidas en las presentes disposiciones.

**Artículo 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).

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. Asimismo, no podrá realizar las funciones relacionadas con la implementación y operación de la seguridad de la información de la propia institución de financiamiento colectivo.

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.

El oficial en jefe de seguridad de la información podrá apoyarse, para el ejercicio de sus funciones en representantes de las diferentes unidades de negocio.

**Artículo 66.-** El oficial en jefe de seguridad de la información de la institución de financiamiento colectivo deberá, al menos:

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.

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. El plan a que se refiere la presente fracción deberá revisarse y actualizarse, al menos, anualmente.

III. Verificar, al menos anualmente, la definición de los perfiles de acceso a la Infraestructura Tecnológica de la institución de financiamiento colectivo, ya sea propia o provista por terceros, de acuerdo con los perfiles de puestos (segregación funcional), incluyendo aquellos con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos.

IV. Asegurarse al menos anualmente, o antes en caso de presentarse un Incidente de Seguridad de la Información, de la correcta asignación de los perfiles de acceso a los Usuarios de la Infraestructura Tecnológica. La función a que se refiere esta fracción, podrá realizarse mediante muestras representativas y aleatorias.

Asimismo, será responsable de la autorización temporal de los accesos por excepción, tales como los de usuarios de ambientes de desarrollo con accesos a ambientes de producción, accesos por eventos de contingencia o cualquier otro acceso privilegiado que no corresponda con la política determinada por la institución de financiamiento colectivo. Igualmente, deberá contar con un registro que contenga el nombre del Usuario de la Infraestructura Tecnológica, aplicación asociada, ambiente, motivo de la excepción y fecha de inicio y de fin de la asignación.

V. Aprobar y verificar el cumplimiento de las medidas que se hayan adoptado para subsanar deficiencias detectadas con motivo de las funciones a que se refieren las fracciones III y IV de este artículo, así como de los hallazgos, tanto de auditoría interna como externa relacionada con la Infraestructura Tecnológica y de seguridad de la información.

VI. Gestionar las alertas de seguridad de la información comunicadas por la CNBV u otros medios, así como los Incidentes de Seguridad de la Información, considerando las etapas de identificación, protección, detección, respuesta y recuperación.

VII. Coordinar y presidir en la institución de financiamiento colectivo, el equipo para la detección y respuesta de Incidentes de Seguridad de la Información.

VIII. Informar al Órgano de Administración o, en caso de contar con un comité de auditoría y un comité de riesgos a estos, en la sesión inmediata siguiente, según resulte aplicable, a la verificación del Incidente de Seguridad de la Información, respecto de las acciones tomadas y del seguimiento a las medidas para prevenir o evitar que se presenten nuevamente los mencionados incidentes.

IX. Proponer y coordinar los programas de capacitación y concientización en materia de seguridad de la información dentro de la institución de financiamiento colectivo y hacia los Clientes, y verificar su efectividad.

X. Presentar mensualmente al director general o, en su caso, al administrador único, el informe de gestión en materia de seguridad de la información. Este reporte deberá efectuarse al comité de auditoría y al comité de riesgos o, en ausencia de estos, al consejo de administración de la institución de financiamiento colectivo.

XI. Considerar, al menos, los indicadores de riesgo en materia de seguridad de la información establecidos en el Anexo 13 de estas disposiciones, e informar del resultado de la evaluación de dichos indicadores al Órgano de Administración, y en su caso, al comité de auditoría o comité de riesgos.

XII. Ser el responsable de la implementación de la regulación que en materia de seguridad de la información emitan otras autoridades financieras.

XIII. Responder a los requerimientos formulados por las autoridades y al interior de la institución de financiamiento colectivo en materia de seguridad de la información.

Las instituciones de financiamiento colectivo deberán asegurarse de que el oficial en jefe de seguridad de la información tenga a su disposición los registros de las personas que cuenten con acceso a la información relacionada con las operaciones en las que interviene la propia institución de financiamiento colectivo, incluyendo aquellas que se encuentren en el extranjero y de los Usuarios de la Infraestructura Tecnológica que cuenten con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos, así como de sus prestadores de servicios.

Las instituciones de financiamiento colectivo que pertenezcan a un grupo financiero sujeto a la supervisión de la CNBV, o bien, que formen parte de Consorcios o Grupos Empresariales que cuenten con una entidad financiera sujeta a la supervisión de la propia CNBV, podrán asignar las funciones del oficial en jefe de seguridad de la información, a la persona que desempeñe dichas actividades en la entidad financiera supervisada por la CNBV, siempre y cuando dicha persona cumpla con lo establecido en el artículo 65 de estas disposiciones.

**Artículo 67.-** En caso de que se presente un Evento de Seguridad de la Información o Incidente de Seguridad de la Información a que alude la fracción I de este artículo 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:

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.

Adicionalmente, las instituciones de financiamiento colectivo deberán enviar mediante correo electrónico a la CNBV, a la cuenta [Ciberseguridad-CNBV@cnbv.gob.mx](mailto: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.

Para el caso de Eventos de Seguridad de la Información, deberán reportarse a través de los medios señalados en el primer párrafo de esta fracción y solo aquellos que, de acuerdo a las políticas establecidas 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. Este reporte únicamente deberá contener la fecha y hora de inicio, así como la descripción del evento de que se trate.

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.

Cuando el Incidente de Seguridad de la Información se refiera a que la Información Sensible que se encuentre en custodia de la institución de financiamiento colectivo o de terceros que le presten servicios, fue extraída, extraviada, eliminada, alterada, o bien, las instituciones de financiamiento colectivo sospechen de la realización de algún acto que involucre accesos no autorizados a dicha información, el director general o, en su caso, el administrador único o la persona que alguno de estos designe, deberá notificar a los Clientes la posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información, dentro de las siguientes cuarenta y ocho horas a que ocurrió el Incidente de Seguridad de la Información o a que se tuvo conocimiento de este, a través de los medios de notificación que el Cliente haya señalado para tal efecto, a fin de prevenirlo de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada, eliminada, o alterada, debiendo informarle las medidas que deberá tomar y, en su caso, efectuar la reposición de los medios de disposición que correspondan o la sustitución de Factores de Autenticación necesarios. La evidencia de esta notificación deberá incluirse en el resultado de la investigación señalada en el párrafo anterior.

**Artículo 68.-** Las instituciones de financiamiento colectivo deberán llevar un registro en bases de datos de los Eventos de Seguridad de la Información calificados como relevantes, Incidentes de Seguridad de la Información, fallas o vulnerabilidades detectadas en la Infraestructura Tecnológica que incluya, al menos, la información relacionada con la detección de fallas, errores operativos, intentos de ataques informáticos y de aquellos efectivamente llevados a cabo, así como de pérdida, extracción, alteración, extravío o uso indebido de información de los Usuarios de la Infraestructura Tecnológica, en donde se contemple la fecha del suceso y una breve descripción de este, su duración, servicio o canal afectado, Clientes afectados y montos, así como las medidas correctivas implementadas.

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.

**Capítulo VII**

Del uso de Medios Electrónicos

**Artículo 69.-** Las instituciones de financiamiento colectivo para el uso de Medios Electrónicos, darán a conocer a sus Clientes, al menos lo siguiente:

I. Las Operaciones y servicios que podrán realizarse a través de Medios Electrónicos.

II. Los mecanismos y procedimientos de identificación y Autenticación del Cliente.

III. Las responsabilidades del Cliente y de la institución de financiamiento colectivo respecto del uso del Medio Electrónico que corresponda.

IV. Los mecanismos y procedimientos para la notificación de las Operaciones realizadas y servicios prestados por las instituciones de financiamiento colectivo.

V. Los límites de los montos de las Operaciones, sin que estos superen los de los artículos 49 y 50 de las presentes disposiciones.

VI. Los riesgos inherentes, términos y condiciones para el uso del Medio Electrónico de que se trate, así como las sugerencias para evitar el uso indebido de sus datos de Autenticación para prevenir la realización de operaciones irregulares o ilegales que vayan en detrimento del patrimonio de los Clientes y de las instituciones de financiamiento colectivo.

VII. Los mecanismos y procedimientos que la institución de financiamiento colectivo pondrá a disposición de los Clientes para atender las aclaraciones relacionadas con Operaciones y servicios.

VIII. Los procedimientos de notificación y términos y condiciones para la aceptación, por parte de los Clientes, de las modificaciones a las condiciones señaladas en las fracciones anteriores de este artículo.

**Artículo 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, y

II. Un Factor de Autenticación de las categorías 2, 3 o 4 a que se refiere 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, a través del Medio Electrónico que corresponda.

La longitud del Identificador de Cliente deberá ser de al menos seis caracteres alfanuméricos o especiales.

**Artículo 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:

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.

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.

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.

IV. Contar con procedimientos para restablecer una Contraseña bloqueada, en los cuales se identifique la identidad del Cliente sin comprometer su Información Sensible.

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 ser tal.

**Artículo 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 ser de cualquiera de las siguientes categorías:

I. Factor de Autenticación categoría 1: se compone de información obtenida mediante la aplicación de cuestionarios al Cliente, automatizados o por parte de operadores telefónicos o remotos, en los cuales se requieran datos que el Cliente conozca y que las instituciones de financiamiento colectivo puedan validar.

Las instituciones de financiamiento colectivo, en la utilización de este factor, para verificar la identidad de sus Clientes, deberán observar lo siguiente:

a) Contar con procedimientos automatizados para practicar cuestionarios aleatorios, de forma automatizada o vía remota por los operadores, impidiendo que sean utilizados de forma discrecional.

b) 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. En ningún caso las respuestas a estas preguntas podrán ser datos que se muestren en el Medio Electrónico ni se encuentren en comunicaciones impresas o electrónicas enviadas por las instituciones de financiamiento colectivo a sus Clientes.

c) Validar las respuestas proporcionadas por sus Clientes a través de herramientas informáticas, sin que el operador pueda consultar o acceder a los datos de autenticación de los Clientes.

II. Factor de Autenticación categoría 2: se compone de información que solo el Cliente defina, conozca e ingrese a través de un dispositivo de acceso, tales como Contraseñas y Números de Identificación Personal (NIP) y deberá cumplir con las características siguientes:

a) Su longitud deberá ser de al menos seis caracteres e incluir caracteres alfanuméricos y especiales, cuando el Dispositivo de Acceso lo permita.

b) En ningún caso se podrán utilizar como tales, la información siguiente:

i. El Identificador de Cliente.

ii. El nombre de la institución de financiamiento colectivo.

iii. Más de tres caracteres idénticos en forma consecutiva.

iv. Más de tres caracteres numéricos y alfabéticos en forma secuencial.

Las instituciones de financiamiento colectivo permitirán al Cliente cambiar sus Contraseñas, Números de Identificación Personal (NIP) y otra información de Autenticación estática, cuando este último así lo requiera, utilizando los Medios Electrónicos que correspondan y en los términos previstos en las presentes disposiciones.

Tratándose de Contraseñas definidas o generadas por las instituciones de financiamiento colectivo durante el restablecimiento de dichas contraseñas, las instituciones de financiamiento colectivo deberán prever mecanismos y procedimientos por medio de los cuales el Cliente deba modificarlos inmediatamente después de iniciar la Sesión correspondiente y previo a la realización de cualquier Operación, validando que las referidas Contraseñas sean diferentes a las definidas por las propias instituciones de financiamiento colectivo.

III. Factor de Autenticación categoría 3: se compone de información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida o recibida por dispositivos generadores de Contraseñas dinámicas de un solo uso (OTP, one time password por sus siglas en inglés), dichos medios o dispositivos deberán ser proporcionados o validados y registrados por las instituciones de financiamiento colectivo para sus Clientes y la información contenida o generada por ellos podrá ser proporcionada, entre otros formatos, en códigos de respuesta rápida (QR, quick response por sus siglas en inglés). En todo caso se cumplirá con las características siguientes:

a) Contar con propiedades que impidan su duplicación o alteración.

b) Ser información dinámica que no podrá ser utilizada en más de una ocasión.

c) Tener una vigencia que no podrá exceder de dos minutos.

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.

Las instituciones de financiamiento colectivo podrán proporcionar a sus Clientes medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen información de la Cuenta Destino, mediante la captura de datos, de manera que dicha Contraseña únicamente pueda ser utilizada para la Operación solicitada. En este caso, no será aplicable lo dispuesto en el inciso c) de la presente fracción.

IV. Factor de Autenticación categoría 4: se compone de información del Cliente derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano, patrones en iris o retina y reconocimiento facial, entre otras.

El proceso de captura de datos biométricos deberá impedir que un empleado, directivo o funcionario de la institución de financiamiento colectivo registre sus propios datos biométricos en sustitución de los correspondientes a los del Cliente.

**Artículo 73.-** Las instituciones de financiamiento colectivo podrán solicitar a la CNBV que apruebe factores de Autenticación distintos a los señalados en el artículo 72, fracción IV de las presentes disposiciones, siempre que acrediten que la tecnología utilizada, a juicio de la propia CNBV, resulta fiable para autenticar a sus Clientes.

La solicitud para obtener la aprobación de la CNBV deberá contener lo siguiente:

I. La descripción detallada de los procesos relacionados con el uso de la tecnología utilizada.

II. La evidencia que acredite el funcionamiento de la tecnología, así como que esta presenta características similares o superiores en términos de calidad respecto de los Factores de Autenticación.

III. La evidencia de la aprobación del uso de la tecnología por el Órgano de Administración.

**Artículo 74.-** Las instituciones de financiamiento colectivo deberán establecer mecanismos y procedimientos para que sus Clientes puedan verificar la autenticidad de las propias instituciones de financiamiento colectivo al inicio de una Sesión, sujetándose a lo siguiente:

I. Proporcionar a sus Clientes información personalizada para que estos puedan verificar, antes de ingresar todos los elementos de identificación y Autenticación, que se trata efectivamente de su Plataforma con la cual se iniciará la Sesión. Para ello, las instituciones de financiamiento colectivo deberán utilizar al menos, alguna de las siguientes:

a) Información que el Cliente conozca o haya proporcionado a la institución de financiamiento colectivo, o bien, que haya señalado para este fin, tales como nombre, alias, imágenes, entre otros.

b) Información que el Cliente pueda verificar mediante un dispositivo o Medio Electrónico proporcionado por la institución de financiamiento colectivo para este fin.

II. Una vez que el Cliente verifique que se trata de la institución de financiamiento colectivo e inicie la Sesión, esta deberá proporcionar de forma notoria y visible al Cliente, al menos la siguiente información:

a) Fecha y hora del ingreso a su última Sesión, y

b) Nombre y apellido del Cliente.

**Artículo 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:

I. Dar por terminada inmediatamente la Sesión en forma automática e informar al Cliente del motivo en cualquiera de los casos siguientes:

a) Cuando exista inactividad por más de cinco minutos.

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.

II. Impedir el acceso en forma simultánea en un mismo Medio Electrónico, mediante la utilización de un mismo Identificador de Cliente y hacerlo del conocimiento del Cliente.

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.

**Artículo 76.-** Las instituciones de financiamiento colectivo, para la celebración de Operaciones, solicitarán a sus Clientes un segundo Factor de Autenticación a que se refiere 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:

I. Instrucciones para realizar compromisos de inversión o retirar sus recursos.

II. Registro o modificación de Cuentas Destino para el servicio de que se trate.

III. Cambio y Desbloqueo de Contraseñas o Números de Identificación Personal (NIP).

IV. Alta y modificación del medio de notificación a que se refiere el artículo 79 de estas disposiciones.

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 de categoría 3 o 4.

Las instituciones de financiamiento colectivo, cuando acuerden con sus Clientes que la consulta de los estados de cuenta sea a través de correo electrónico, la información que se transmita deberá hacerse de forma cifrada o con mecanismos que eviten su lectura por parte de terceros no autorizados y, para que el Cliente tenga acceso a dicha información, requerirán de un Factor de Autenticación de categoría 2 a que se refiere el artículo 72 de las presentes disposiciones, el cual deberá ser distinto al registrado para iniciar Sesión.

**Artículo 77.-** Las instituciones de financiamiento colectivo deberán asegurarse de que sus Clientes registren las Cuentas Destino previamente a su uso, para lo cual, deberán validar la existencia y pertenencia de la Cuenta Destino registrada por los Clientes en el Medio Electrónico que corresponda.

**Artículo 78.-** Las instituciones de financiamiento colectivo deberán solicitar a sus Clientes que confirmen la Operación y sus características, previo a que se ejecute, haciendo explícita la información para darle certeza al Cliente de la Operación que se realiza.

**Artículo 79.-** Las instituciones de financiamiento colectivo notificarán de forma inmediata a sus Clientes, a través de los medios de comunicación que pongan a su disposición, tales como número de teléfono móvil o dirección de correo electrónico y que estos hayan elegido para tal fin, la realización de Operaciones. Para el cambio de medio de notificación deberá enviarse aviso tanto al medio anterior como al nuevo.

**Artículo 80.-** Las instituciones de financiamiento colectivo establecerán procesos y mecanismos automáticos para Bloquear los Factores de Autenticación, cuando menos para los casos siguientes:

I. Cuando se intente ingresar al Medio Electrónico de que se trate utilizando información de Autenticación incorrecta. En ningún caso los intentos de acceso fallidos podrán exceder de tres ocasiones consecutivas, una vez alcanzado el número de intentos establecido se deberá generar el Bloqueo automático.

II. Cuando el Cliente no acceda al Medio Electrónico de que se trate, por un periodo que determine cada institución de financiamiento colectivo en sus políticas de operación. En ningún caso, dicho periodo podrá ser mayor a un año.

Las instituciones de financiamiento colectivo podrán Desbloquear los Factores de Autenticación que previamente hayan sido Bloqueados en los casos contemplados en las fracciones I y II anteriores, para lo cual podrán utilizar un Factor de Autenticación de categoría 1 o bien, realizar a sus Clientes preguntas secretas, cuyas respuestas deben conservarse almacenadas en forma Cifrada. Para efectos de lo previsto en el presente párrafo, se entenderá por pregunta secreta al cuestionamiento que define el Cliente o la institución de financiamiento colectivo, respecto del cual se genera información como respuesta. Cada pregunta secreta que se defina únicamente podrá ser utilizada en una ocasión.

**Artículo 81.-** Para el manejo de Factores de Autenticación, las instituciones de financiamiento colectivo se sujetarán a lo siguiente:

I. Deberán mantener procedimientos que proporcionen seguridad en la información contenida en los dispositivos de Autenticación en su custodia, así como en la distribución, asignación y reposición de dichos Factores de Autenticación a sus Clientes.

II. Tendrán prohibido contar con mecanismos, algoritmos o procedimientos que les permitan conocer, recuperar o descifrar los valores de cualquier información relativa a la Autenticación de sus Clientes.

III. Tendrán prohibido solicitar a sus Clientes, a través de sus funcionarios, empleados o representantes, la información parcial o completa, de los Factores de Autenticación categoría 2 o 3 a que se refiere el artículo 72 de las presentes disposiciones.

IV. Para los Factores de Autenticación categoría 4, deberán incorporar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Cliente.

**Artículo 82.-** Las instituciones de financiamiento colectivo preverán los procedimientos y mecanismos para que sus Clientes les reporten el robo o extravío de su información de identificación y Autenticación, que permitan a las propias instituciones de financiamiento colectivo impedir su uso indebido.

Asimismo, deberán establecer políticas que definan las responsabilidades tanto del Cliente como de la institución de financiamiento colectivo, respecto de las Operaciones que hayan sido efectuadas previas a un reporte de robo o extravío de su información de identificación o Autenticación.

Cada reporte de robo o extravío generará un folio que se haga del conocimiento del Cliente y que le permita dar seguimiento a dicho reporte.

**Artículo 83.-** Las instituciones de financiamiento colectivo que cuenten con canales remotos tales como centros de atención telefónica o canales electrónicos de mensajería, deberán:

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.

II. Delimitar las funciones de los operadores, a fin de que sean independientes respecto de otras funciones operativas.

III. Impedir que los operadores cuenten con mecanismos que les permitan registrar la información proporcionada por sus Clientes en medios diferentes a los dispuestos por la propia institución de financiamiento colectivo para efectos de Autenticación. Para ello, las instituciones de financiamiento colectivo deberán cerciorarse que las personas que tengan acceso a los canales remotos, no utilicen equipos electrónicos u otros dispositivos, servicios de correo electrónico externo, programas de mensajería instantánea, programas de cómputo, o que a través de estos tengan acceso a páginas de Internet no autorizadas, o a cualquier otro mecanismo que les permita copiar, enviar o extraer por cualquier medio o tecnología información relacionada con los Clientes.

IV. Registrar en bitácoras, los accesos y actividades que los operadores de los centros de atención telefónica o canales electrónicos de mensajería realicen con los Clientes, así como conservar las bitácoras.

Lo establecido en el presente artículo deberá quedar previsto en las políticas en materia de seguridad de la información que establezcan las instituciones de financiamiento colectivo.

**Artículo 84.-** Las instituciones de financiamiento colectivo deberán contar con personal de soporte técnico y operacional capacitado, quienes se encargarán de atender y dar seguimiento a las solicitudes de servicio que tengan sus Clientes en el uso de Medios Electrónicos.

**Capítulo VIII**

De la contratación de servicios con terceros

**Artículo 85.-** Las instituciones de financiamiento colectivo requerirán autorización de la CNBV para contratar con terceros los siguientes servicios:

I. Que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de Información Sensible, identificaciones oficiales o información biométrica de los Clientes, siempre y cuando el tercero contratado tenga privilegios de acceso a dicha información de manera no cifrada o a la información de configuración de seguridad, o bien a la administración de control de accesos.

II. Que realicen procesos en el extranjero relacionados con la contabilidad y tesorería, así como con el registro de cuentas sobre movimientos transaccionales de los Clientes de la institución de financiamiento colectivo.

Las instituciones de financiamiento colectivo, tanto en la contratación de los servicios referidos en las fracciones anteriores como en cualquier otro, deberán cuidar en todo momento que los terceros que les proporcionen los servicios, guarden la debida confidencialidad de la información relativa a las Operaciones celebradas con sus Clientes, así como la relativa a estos últimos, en caso de tener acceso a ella.

Las instituciones de financiamiento colectivo deberán mantener los datos de los terceros que les proporcionen los servicios necesarios para su operación, incluyendo los mencionados en este artículo, en el padrón a que se refiere el artículo 88 de las presentes disposiciones.

**Artículo 86.-** Las instituciones de financiamiento colectivo deberán acompañar a la solicitud de autorización a que se refiere el artículo anterior, lo siguiente:

I. La descripción detallada de los servicios a contratar, considerando las actividades que se pretendan realizar por la institución de financiamiento colectivo así como por prestador del servicio; las áreas de la propia institución de financiamiento colectivo y del tercero que participan en el flujo del servicio; nombre, descripción y funcionalidad de los sistemas que, en su caso, serán contratados para la prestación del servicio, o los sistemas de la institución de financiamiento colectivo que serán utilizados por el proveedor respectivo.

II. La documentación que acredite que el tercero estará en condiciones de cumplir durante la prestación del servicio con lo siguiente:

* 1. 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, a los cuales debe tener acceso personal autorizado de la institución de financiamiento colectivo.

b) Contar con políticas y procedimientos de control de acceso a la información de acuerdo con los niveles de acceso y perfiles determinados por la institución de financiamiento colectivo.

c) Realizar revisiones de seguridad a los servicios contratados o señalar la forma en la que se demostrará la realización de estas revisiones por parte de una persona especializada distinta al proveedor del servicio.

III. El proyecto de contrato de prestación de servicios, en el que deberá señalarse la fecha probable de su celebración, las obligaciones de la institución de financiamiento colectivo y del tercero, incluyendo la determinación sobre la propiedad intelectual respecto de los diseños, desarrollos o procesos utilizados para la prestación del servicio. Dicho proyecto de contrato deberá ser presentado en idioma español.

Asimismo, deberá quedar constancia, dentro del contrato, de la aceptación expresa por parte del tercero de:

a) Apegarse a lo previsto en el artículo 54 de la Ley.

b) Entregar en el desarrollo de una auditoría y a solicitud de la institución de financiamiento colectivo, al auditor externo independiente de la propia institución de financiamiento colectivo y a la CNBV, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitir al auditor externo independiente o al personal de la CNBV el acceso a sus oficinas e instalaciones en general, relacionadas con la prestación del servicio en cuestión.

c) Informar a la institución de financiamiento colectivo respecto de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar la prestación del servicio objeto de la contratación, con por lo menos treinta días de anticipación a que suceda dicha modificación o cambio.

d) Guardar confidencialidad respecto de la información que haya sido recibida, transmitida, procesada o almacenada durante la prestación de los servicios. Asimismo, aceptar que dicha información solamente puede usarse y explotarse para los fines pactados en la prestación del servicio.

e) Ajustarse a las condiciones establecidas por la institución de financiamiento colectivo para efectuar la subcontratación parcial o total de los servicios, cuando así se haya establecido.

f) Presentar dentro del periodo que la institución de financiamiento colectivo establezca, un plan de migración de información que contenga términos, condiciones y procesos para que el tercero garantice a la institución de financiamiento colectivo la transferencia, devolución o eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.

IV. Los términos, condiciones y procesos para que el tercero garantice a la institución de financiamiento colectivo la transferencia o devolución de la información, así como la eliminación completa de la información sujeta al servicio contratado.

V. La descripción de los controles de vigilancia del desempeño del tercero, que deberán considerar cuando menos, el cumplimiento de sus obligaciones contractuales y de las presentes disposiciones, así como de los mecanismos que la institución de financiamiento colectivo llevará a cabo para establecer, revisar de manera permanente y vigilar la calidad y los tiempos de respuesta en los servicios. En dicha descripción se deberá incluir al menos los sistemas o herramientas utilizadas, reportes generados y su periodicidad.

VI. La descripción de los servicios que los terceros podrán subcontratar, ya sea parcial o totalmente.

VII. La descripción de los mecanismos de control e interfaces, que permitan mantener, por parte del tercero, la integridad de la información.

VIII. La siguiente documentación respecto de la Infraestructura Tecnológica:

a) La descripción de los enlaces de comunicación que incluya el nombre del proveedor, el ancho de banda, el tipo de servicio prestado, entre otros.

b) Un diagrama de telecomunicaciones en donde se muestre la conexión existente entre cada uno de los participantes en la prestación del servicio (proveedores, centros de datos, institución de financiamiento colectivo, entre otros), incluyendo los esquemas de redundancia.

c) La dirección completa del lugar en donde se realizarán cada uno de los servicios, así como de los centros de datos, primario y secundario, en donde se almacenará y procesará la información. En caso de que el lugar señalado se encuentre en territorio nacional debe incluirse, por lo menos, calle, número exterior e interior, colonia, alcaldía o municipio, código postal y estado. Tratándose de un sitio localizado en el extranjero deberán incluirse datos similares que permitan ubicar con certeza el lugar señalado.

d) En su caso, el esquema de interrelación de aplicaciones o sistemas objeto de la contratación, incluyendo los sistemas propios de la institución de financiamiento colectivo, así como, los sistemas o aplicaciones utilizados por los terceros que se subcontraten.

e) La descripción de las características técnicas de los sistemas, equipos y aplicaciones objeto de la contratación que contenga al menos lo señalado en el Anexo 14 de estas disposiciones.

f) La documentación sobre la estrategia de continuidad del tercero que proporcione a la propia institución de financiamiento colectivo la capacidad de continuar con la prestación del servicio en caso de contingencias, fallas o interrupciones en las telecomunicaciones o en los equipos de cómputo centrales y otros que estén involucrados en el servicio contratado.

g) El esquema de soporte técnico, a fin de solucionar problemas e incidencias, con independencia, en su caso, de las diferencias en husos horarios y días hábiles, detallando los horarios y canales de atención.

h) Los mecanismos que permitirán a la institución de financiamiento colectivo, mantener en sus instalaciones los registros detallados de todas las Operaciones que se realicen, así como de sus registros contables al cierre diario. Dichos registros deberán mantenerse en un formato que permita su consulta y uso, con independencia de que el servicio contratado con el tercero no se encuentre disponible.

IX. En relación con la seguridad de la información, la documentación siguiente:

a) Aquella en donde se expongan los mecanismos para asegurar la transmisión de la información en forma cifrada punto a punto, incluyendo la versión de los protocolos de cifrado y componentes de seguridad de la Infraestructura Tecnológica implementados en cada uno de los nodos involucrados en el envío y recepción de datos.

b) La que señale los mecanismos utilizados para cifrar la información de la institución de financiamiento colectivo y de los Clientes que será almacenada por el tercero contratado en sus equipos o instalaciones, de acuerdo con el grado de riesgo definido por la institución de financiamiento colectivo.

c) La que contenga el detalle del tipo de información de la institución de financiamiento colectivo y Clientes que será almacenada por el tercero en sus equipos o instalaciones, o a la que podrá tener acceso, en su caso, incluyendo al menos la Información Sensible.

d) Las políticas y procedimientos de respaldo de información del tercero que incluya, al menos, periodicidad de los respaldos, tipo de información que se respalda, ciclo de vida del medio de respaldo y mecanismos de resguardo, así como las políticas de destrucción o borrado seguro de la información.

e) La que contenga la descripción de los mecanismos de control y vigilancia del acceso a los sistemas informáticos y a la Información Sensible transmitida, almacenada, procesada, resguardada o custodiada en dichos sistemas; así como de las bitácoras, bases de datos y configuraciones de seguridad que se establezcan al efecto.

f) Listado de las certificaciones de seguridad y cumplimiento con las que cuenta el tercero prestador del servicio.

X. Las políticas y procedimientos de la institución de financiamiento colectivo relativos a la realización de auditorías internas o externas sobre la Infraestructura Tecnológica y controles relacionados con el servicio contratado, al menos anualmente.

XI. Tratándose de contratación de servicios de Cómputo en la Nube, describir adicionalmente lo siguiente:

a) Tipo de nube, ya sea pública, privada o híbrida.

b) Localidades específicas en donde se almacenará y procesará la información.

c) Nombre del proveedor.

Cuando las instituciones de financiamiento colectivo contraten a terceros que provean esquemas de nubes públicas o de virtualización en infraestructura compartida con otros clientes, se deberá proporcionar la descripción de los mecanismos de control que serán utilizados por la propia institución para garantizar la confidencialidad, integridad y disponibilidad de la Información Sensible.

**Artículo 87.-** Las instituciones de financiamiento colectivo para la contratación de servicios con terceros que sean objeto de autorización por la CNBV en términos de estas disposiciones, adicionalmente observarán lo siguiente:

I. Contar con evidencia que permita verificar que los terceros con los que se contrate mantengan políticas de protección de datos personales y confidencialidad de la información que permitan a la institución de financiamiento colectivo cumplir con las disposiciones legales que la rigen en la materia. Tratándose de servicios que se procesen, proporcionen o ejecuten total o parcialmente fuera de territorio nacional, las instituciones de financiamiento colectivo deberán acompañar la documentación que acredite que los terceros residen en países cuyo derecho interno proporciona protección a los datos de las personas, resguardando su debida confidencialidad, o bien, que dichos países mantengan suscritos con México acuerdos internacionales en dicha materia o de intercambio de información entre los organismos supervisores, tratándose de Entidades Financieras.

II. Mantener en sus oficinas principales, al menos la documentación e información relativa a las evaluaciones, resultados de auditorías y reportes de desempeño de los terceros contratados.

III. Obtener la aprobación de su Órgano de Administración en la que conste que:

a) Al contratar al tercero no se pone en riesgo el cumplimiento de las disposiciones aplicables a la institución de financiamiento colectivo.

b) Las prácticas de negocio del tercero a contratar son consistentes con las de operación de la institución de financiamiento colectivo.

c) No habría impacto en la estabilidad financiera o continuidad operativa de la institución de financiamiento colectivo, con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizaría en la prestación del servicio.

IV. Entregar a la CNBV el contrato de prestación de servicios con el tercero de que se trate dentro de los 5 días hábiles posteriores a su celebración.

V. Elaborar un documento que contenga el resultado del análisis de los riesgos relacionados con los servicios que pretende contratar con el tercero en donde se contemple, al menos, los legales y de reputación de la institución de financiamiento colectivo por incumplimientos del tercero contratado, así como por compartir su Infraestructura Tecnológica con terceros.

VI. Incorporar en sus manuales de operación, de control interno y de administración de riesgos, aspectos que en materia de procesos operativos, Infraestructura Tecnológica, seguridad, y auditoría y supervisión, se contemplen en las presentes disposiciones, y mantenerlos actualizados.

VII. Evaluar a través de su Órgano de Administración en la forma y periodicidad que este determine, el desempeño del tercero y su cumplimiento a las obligaciones contractuales y las derivadas de las disposiciones, pudiendo para tal efecto delegar esta función.

VIII. Cuando existan modificaciones a la descripción a que se refiere el inciso e) de la fracción VIII del artículo 86 de estas disposiciones; que se consideren que tienen un impacto en cuanto al servicio proporcionado o que estén relacionadas con los sistemas, equipos y aplicaciones objeto de la contratación o con sus características técnicas, actualizar la descripción o documentación respectiva debiéndola entregar a la CNBV en un periodo de diez días hábiles posteriores a que se hayan implementado las modificaciones.

**Artículo 88.-** Las instituciones de financiamiento colectivo deberán contar con un padrón de todos sus prestadores de servicios que incluya, al menos, la siguiente información:

I. Nombre, denominación o razón social del prestador de servicios.

II. Nombres del representante legal del prestador de servicios.

III. Descripción del servicio contratado con el tercero, incluyendo los datos o información que, en su caso, son almacenados o manejados por este.

IV. En su caso, nombre del sistema que soporta el servicio contratado con el tercero.

V. En su caso, interfaces con otros sistemas y el propósito de estas, incluyendo el detalle de la información que intercambia.

VI. Ubicación en donde se realiza el servicio y en donde se encuentra el personal responsable de llevarlo a cabo.

VII. Ubicación del centro de datos principal en donde se encuentran los equipos de procesamiento del sistema contratado.

VIII. Ubicación del centro de datos alterno en donde se encuentran los equipos de procesamiento, en caso de recuperación del servicio contratado.

IX. En su caso, número y fecha del oficio con el que la CNBV otorgó la autorización en el momento en que cuenten con ella.

Las instituciones de financiamiento colectivo deberán actualizar el padrón a que se refiere este artículo y entregarlo a la CNBV en el transcurso del primer trimestre de cada año.

**Artículo 89.-** Las instituciones de financiamiento colectivo que contraten con terceros servicios relacionados con algún proceso operativo o tecnológico que contemple la transmisión, almacenamiento, procesamiento, resguardo y custodia de información que no sea Información Sensible, les resultará aplicable lo previsto en los artículos 86, fracciones III, IV, V, VI, VIII, IX y XI, así como su último párrafo y 87, fracciones I a III y VI.

**Capítulo IX**

De la revelación de información

**Sección Primera**

De la revelación de información en la publicación de solicitudes y proyectos

**Artículo 90.-** Las instituciones de financiamiento colectivo incluirán en las publicaciones sobre las ofertas de financiamiento que realicen en sus Plataformas, información respecto del análisis general efectuado y cualquier otra variable que resulte útil para que los Inversionistas tomen una decisión de inversión informada.

**Artículo 91.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Deuda de Préstamos Personales entre Personas deberán revelar, por cada solicitud de financiamiento, la siguiente información:

I. Monto del financiamiento solicitado.

II. Plazo de la Solicitud de Financiamiento Colectivo.

III. Descripción del destino del financiamiento.

IV. Plazo del financiamiento colectivo.

V. Calendario de pagos del principal e intereses, así como su monto.

VI. Tasas de interés ordinaria y, en su caso, moratoria.

VII. En su caso, garantías.

VIII. Calificación de riesgo determinada de acuerdo con la metodología de evaluación de riesgos definida por la institución de financiamiento colectivo, acompañado de una explicación simple de la forma de interpretarla.

IX. En su caso, los esquemas para compartir con los Inversionistas los riesgos de las Operaciones de financiamiento colectivo.

X. Datos relativos al Solicitante que resulten importantes para la toma de decisiones de los posibles Inversionistas, tales como su edad, sexo, ocupación, residencia y fuentes de ingresos.

**Artículo 92.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Deuda de Préstamos Empresariales entre Personas y, para el Desarrollo Inmobiliario, deberán revelar por cada Solicitud o proyecto de financiamiento, en adición a los numerales I a IX del artículo 91 anterior, la información correspondiente al tipo de financiamiento colectivo de que se trate, según se detalla en el Anexo 15 de estas disposiciones.

**Artículo 93.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Capital, deberán revelar para cada proyecto que promuevan en su Plataforma, la información siguiente, según se detalla en el Anexo 16 de estas disposiciones:

I. Monto del financiamiento solicitado.

II. Plazo de Solicitud de Financiamiento Colectivo.

III. Descripción del fin último de los recursos.

IV. Descripción de los títulos representativos del capital social y los derechos que adquiere el Inversionista, así como la forma en que se le retribuirá por las aportaciones que realice.

V. Calificación de riesgo determinada de acuerdo con la metodología de evaluación de riesgos definida por la institución de financiamiento colectivo, acompañado de una explicación simple de la forma de interpretarla.

VI. Nombre y giro de la persona moral, naturaleza jurídica, fecha de constitución, dirección de oficinas principales y, en su caso, sitio de Internet.

VII. Descripción de los elementos principales que integran el modelo o plan de negocios de la persona moral.

VIII. Descripción de la política de dividendos, así como de los factores de riesgo que pueden afectar significativamente el desempeño y la rentabilidad de la persona moral.

IX. Nombre del administrador o administradores y, en su caso, del director general, así como de las personas que ejerzan el Control de la persona moral.

X. Descripción de la situación financiera, al momento de la solicitud de financiamiento, de la persona moral considerando aspectos tales como rentabilidad, apalancamiento, liquidez y eficiencia operativa. Se deberán incluir, al menos, el monto del capital contable, los principales rubros de activos y pasivos, así como el resultado del ejercicio anterior. En caso de tratarse de empresas de nueva creación, deberá señalarse tal situación y, en su caso, incluir información relativa al historial de negocios o conocimientos técnicos de los administradores o ejecutores del proyecto, así como las proyecciones financieras que, en su caso, se tengan.

XI. El precio de los títulos representativos del capital social de la persona moral ofrecidos, incluyendo una descripción de la forma de determinarlo y cualquier limitación que exista para su adquisición.

XII. En su caso, los esquemas para compartir con los Inversionistas los riesgos de las Operaciones de financiamiento colectivo.

**Artículo 94.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Copropiedad o Regalías, deberán revelar, para cada proyecto que promuevan en su Plataforma, la siguiente información:

I. Monto del financiamiento solicitado.

II. Plazo de Solicitud de Financiamiento Colectivo.

III. Descripción del destino del financiamiento incluyendo, en su caso, una descripción del estado o situación financiera actual del proyecto a financiar, así como un modelo o plan de negocios o de inversión de los recursos y la forma de alcanzar los objetivos planteados, así como los indicadores sobre los que se medirán los avances del proyecto o el logro de resultados.

IV. Explicación de la participación que tendrá el Inversionista en los bienes presentes o futuros, ingresos, utilidades, regalías o, en su caso, pérdidas derivadas del proyecto a financiar.

V. Calificación de riesgo determinada de acuerdo con la metodología de evaluación de riesgos definida por la institución de financiamiento colectivo, acompañado de una explicación simple de la forma de interpretarla.

VI. Información relativa al Solicitante:

a) Tratándose de una persona física, deberán revelarse los aspectos señalados en la fracción X del artículo 91 de estas disposiciones, así como una descripción de sus actividades productivas.

b) En caso de tratarse de una persona moral, deberán revelarse los aspectos señalados en las fracciones VI, VII, IX y X del artículo 93 anterior, que le resulten aplicables.

c) Información relativa a los participantes estratégicos con que, en su caso, cuente el Solicitante o el responsable de la ejecución del proyecto, indicando la relación que guardan aquellos con estos últimos, así como una descripción del alcance de su participación o aportaciones al proyecto.

VII. En su caso, los esquemas para compartir con los Inversionistas los riesgos de las Operaciones de financiamiento colectivo.

**Sección Segunda**

De la revelación de información del comportamiento de pago y desempeño del Solicitante o proyecto

**Artículo 95.-** Las instituciones de financiamiento colectivo en cuyas Plataformas se realicen Operaciones de Deuda de Préstamos Empresariales entre Personas, de Préstamos Personales entre Personas y para el Desarrollo Inmobiliario, deberán revelar a los Inversionistas que formen parte de dichas Operaciones, la información siguiente:

I. Indicadores del rendimiento anualizado obtenido por participar en el financiamiento, incluyendo una descripción sobre su forma de cálculo.

II. Indicadores de pago y de incumplimiento, indicando como mínimo, si el crédito está al corriente en sus pagos de principal e intereses, o en su defecto, cuántos pagos ha incumplido históricamente y el monto total que adeuda al momento de reportar, desglosado por principal y accesorios financieros. Para tales efectos, se deberá considerar lo siguiente:

a) Incumplimiento, es aquel evento que se presenta cuando el pago realizado por el Solicitante no alcanza a cubrir el pago que se comprometió de acuerdo con la calendarización de pagos programada y convenida al pactar la Operación.

b) Financiamiento vigente, es aquel que esté al corriente en sus pagos tanto de principal como de intereses.

c) Financiamiento emproblemado, es aquel financiamiento respecto del cual, con base en información, hechos actuales y resultado del proceso de revisión que realice la institución de financiamiento colectivo, existe una probabilidad considerable de no recuperación total, tanto su componente de principal como de intereses, conforme a los términos y condiciones pactados originalmente.

III. En su caso, actualización de los indicadores sobre los que se definió que se medirían los avances del proyecto financiado o el logro de resultados.

Las instituciones de financiamiento colectivo deberán actualizar la información a que se refieren las fracciones I y II anteriores de conformidad con la periodicidad de pago definida en cada Operación pactada.

**Artículo 96.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Capital deberán poner a disposición de los Inversionistas que hayan participado en la Operación de que se trate, al menos, durante los dos años siguientes a que se concretó la Operación, los datos siguientes:

I. La información anual de los administradores de la persona moral financiada a que se refiere el artículo 172 de la Ley General de Sociedades Mercantiles o equivalente.

II. Los riesgos y retos que enfrenta la persona moral financiada.

III. Los indicadores financieros al cierre del ejercicio anual reportado en comparación con el periodo anterior, incluyendo una breve descripción de la forma de cálculo y su interpretación:

a) Rentabilidad, que es el resultado de dividir las utilidades netas anuales entre el capital promedio para determinar el rendimiento sobre capital (ROE) o bien, el resultado de dividir las utilidades netas anuales entre el activo promedio para determinar el rendimiento sobre activos (ROA).

b) Apalancamiento, que es el resultado de dividir el pasivo total entre el activo total.

c) Liquidez, que es el resultado de dividir los activos líquidos entre el activo total. Los activos líquidos son la suma de caja y bancos.

d) Eficiencia operativa, que es el resultado de dividir los gastos administrativos anuales entre los ingresos totales anuales.

Los datos a que aluden las fracciones anteriores deberán ponerse a disposición a través de su Plataforma a más tardar el 30 de abril de cada año. Una vez que concluya el plazo de revelación a que hace referencia el párrafo anterior, la institución de financiamiento colectivo, deberá informar a los inversionistas tal circunstancia.

Tratándose de instituciones de financiamiento colectivo que a su vez sean Inversionistas por la implementación de esquemas para compartir riesgos a que alude el artículo 21, segundo párrafo de la Ley, lo dispuesto en este artículo será aplicable durante todo el tiempo en que la institución sea Inversionista.

**Artículo 97.-** Las instituciones de financiamiento colectivo que realicen Operaciones de Financiamiento Colectivo de Copropiedad o Regalías deberán poner a disposición de los Inversionistas que hayan participado en la Operación de que se trate, al menos durante los siguientes dos años a que se concretó la Operación, un informe sobre la marcha de negocio o avance del proyecto, así como divulgar al menos anualmente los indicadores a los que se refiere el artículo 95, fracción III de las presentes disposiciones.

**Sección Tercera**

De la revelación de información al público en general

**Artículo 98.-** Las instituciones de financiamiento colectivo deberán mantener en un sitio de fácil acceso para consulta del público, dentro de las Plataformas que utilicen para operar con sus Clientes, la información agregada por tipo de financiamiento otorgado de conformidad con lo señalado en el Anexo 17 de las presentes disposiciones.

**TÍTULO CUARTO**

Reportes regulatorios

**Capítulo I**

Reportes en general

**Artículo 99.-** Las instituciones de financiamiento colectivo deberán proporcionar a la CNBV, con la periodicidad establecida en el artículo 100 siguiente, la información que se adjunta a las presentes disposiciones como Anexo 18, la cual se identifica con las series y reportes que a continuación se relacionan:

**Serie R01 Catálogo mínimo.**

A-0112 Catálogo mínimo.

**Serie R08 Préstamos bancarios y de otros organismos.**

D-0842 Desagregado de préstamos obtenidos.

**Serie R10 Reclasificaciones.**

A-10112 Reclasificaciones en el estado de situación financiera.

A-10122 Reclasificaciones en el estado de resultado integral.

**Serie R13 Estados financieros.**

A-13112 Estado de cambios en el capital contable.

A-13162 Estado de flujos de efectivo.

B-13212 Estado de situación financiera.

B-13222 Estado de resultado integral.

**Serie R24 Información operativa.**

G-2421 Información de Solicitantes.

G-2422 Información de Inversionistas.

G-2423 Información de seguimiento a Inversionistas.

G-2424 Segregación de cuentas propias y de manejo de recursos de los Clientes.

G-2431 Información de Personas Relacionadas y con Poder de Mando.

**Serie R27 Reclamaciones.**

A-2702 Reclamaciones.

**Serie R36 Financiamientos y seguimiento.**

D-3601 Información de financiamientos colectivos y seguimiento.

D-3602 Información de financiamientos colectivos de deuda.

D-3603 Información de garantías de financiamientos colectivos de deuda.

D-3604 Información de operaciones en mercado secundario.

**Artículo 100.-** Las instituciones de financiamiento colectivo presentarán la información a que se refiere el artículo 99 anterior, con la periodicidad que a continuación se indica:

I. Diariamente, la información relativa a las series R36, exclusivamente por lo que se refiere a los reportes D-3601, D-3602y D-3604, y R24, exclusivamente por lo que se refiere a los reportes G-2423 y G-2424, proporcionándose el día hábil siguiente al de su fecha, con la información generada a partir de las 00:00:00 horas y hasta las 11:59:59 horas del día que corresponda.

II. Mensualmente, la información relativa a las series R01, R08, R10 y R13, exclusivamente por lo que se refiere a los reportes B-13212 y B-13222, la cual deberá proporcionarse dentro del mes inmediato siguiente al cierre del mes calendario que se reporta.

III. Trimestralmente, la Información relativa a las series R13, exclusivamente por lo que se refiere a los reportes A-13112 y A-13162, y R27, la cual deberá proporcionarse dentro del mes inmediato siguiente al cierre del trimestre calendario que se reporta.

IV. Por evento, la información relativa a las series R36, exclusivamente por lo que se refiere al reporte D-3603, y R24, exclusivamente por lo que se refiere a los reportes G-2421, G-2422 y G-2431, proporcionándose el día hábil siguiente al registro de personas por la institución de financiamiento colectivo, ya sea como posibles Solicitantes o Inversionistas, o un cambio en las Personas Relacionadas o con Poder de Mando respecto de dicha institución de financiamiento colectivo.

**Artículo 101.-** Las instituciones de fondos de pago electrónico deberán proporcionar a la CNBV, con la periodicidad establecida en el artículo 102 siguiente, la información que se adjunta a las presentes disposiciones como Anexo 19, la cual se identifica con las series y reportes que a continuación se relacionan:

**Serie R01 Catálogo mínimo.**

A-0111 Catálogo mínimo.

**Serie R08 Préstamos bancarios y de otros organismos.**

D-0843 Desagregado de préstamos obtenidos.

**Serie R10 Reclasificaciones.**

A-10111 Reclasificaciones en el estado de situación financiera.

A-10121 Reclasificaciones en el estado de resultado integral.

**Serie R13 Estados Financieros.**

A-13111 Estado de cambios en el capital contable.

A-13161 Estado de flujos de efectivo.

B-13211 Estado de situación financiera.

B-13221 Estado de resultado integral.

**Serie R24 Información operativa.**

G-2412 Información de clientes.

G-2442 Información de cuentas.

G-2414 Segregación de cuentas propias y de manejo de recursos de los clientes.

**Serie R26 Información de comisionistas.**

A-2610 Altas y bajas de administradores de comisionistas.

A-2611 Desagregado de altas y bajas de comisionistas.

B-2612 Desagregado de altas y bajas de módulos o establecimientos de comisionistas.

C-2613 Desagregado de seguimiento de operaciones de comisionistas.

**Serie R27 Reclamaciones.**

A-2701 Reclamaciones.

**Serie R36 Movimientos y sobregiros.**

D-3605 Desagregado de movimientos.

D-3606 Desagregado de sobregiros.

**Artículo 102.-** Las instituciones de fondos de pago electrónico presentarán la información a que se refiere el artículo 101 anterior, con la periodicidad que a continuación se indica:

I. Diariamente, la información relativa a las series R24 y R36, proporcionándose el día hábil siguiente al de su fecha, con la información generada a partir de las 00:00:00 horas y hasta las 11:59:59 horas del día que corresponda.

II. Mensualmente, la Información relativa a las series R01, R08, R10 y R13, exclusivamente por lo que se refiere a los reportes B-13211 y B-13221, así como R26, exclusivamente por lo que se refiere al reporte C-2613, la cual deberá proporcionarse dentro del mes inmediato siguiente al cierre del mes calendario que se reporta.

III. Trimestralmente, la Información relativa a las series R13, exclusivamente por lo que se refiere a los reportes A-13111 y A-13161, y R27, la cual deberá proporcionarse dentro del mes calendario inmediato siguiente al cierre del trimestre que se reporta.

IV. Por evento, la información relativa a la serie R26, exclusivamente por lo que se refiere a los reportes A-2610, A-2611 y B-2612, proporcionándose el día hábil siguiente al registro de altas y bajas de administradores de comisionistas, de comisionistas y de los módulos o establecimientos con los que cuenten, respecto de dicha institución de fondos de pago electrónico.

**Artículo 103.-** Las ITF requerirán de la previa autorización de la CNBV para la apertura de nuevos conceptos o niveles que no se encuentren contemplados en las series que correspondan exclusivamente para el envío de información de las nuevas operaciones que les sean autorizadas al efecto por la Secretaría, en términos de la legislación relativa, para lo cual solicitarán la referida autorización mediante escrito libre dentro de los quince días hábiles siguientes a la autorización hecha por la Secretaría. Asimismo, en caso de que por cambios en la normativa aplicable se requiera establecer conceptos o niveles adicionales a los previstos en las presentes disposiciones, la CNBV hará del conocimiento de las ITF la apertura de los nuevos conceptos o niveles respectivos.

En los dos casos previstos en el párrafo anterior, la CNBV notificará a través del SITI el mecanismo de registro y envío de la información correspondiente.

**Capítulo II**

Medios de entrega

**Artículo 104.-** Las ITF, salvo disposición expresa en contrario, deberán enviar a la CNBV la información que se menciona en este título, mediante su transmisión vía electrónica utilizando el SITI. En caso de que no exista información de algún reporte, las instituciones deberán realizar el envío vacío, funcionalidad que está disponible en dicho sistema.

La información deberá cumplir con las validaciones establecidas en el SITI, así como los estándares de calidad que indique la CNBV a través de dicho sistema, además deberá existir consistencia entre la información que las Instituciones incluyan en uno o más reportes regulatorios a que se refieren las presentes disposiciones, aunque se encuentre con un nivel distinto de integración. Asimismo, la información deberá enviarse una sola vez y se recibirá asumiendo que reúne todas las características requeridas, en virtud de lo cual no podrá ser modificada, generando el SITI un acuse de recibo electrónico.

Una vez recibida la información será revisada y de no reunir la calidad y características exigibles o ser presentada de forma incompleta, se considerará como no cumplida la obligación de su presentación y, en consecuencia, se procederá a la imposición de las sanciones correspondientes.

Las ITF mediante envío electrónico a la dirección “cesiti@cnbv.gob.mx”, el nombre de la persona responsable de la calidad y envío de la información a que se refiere el presente título, en la forma en que se señala en el Anexo 20 de las presentes disposiciones. La designación del responsable de la calidad de la información deberá recaer en directivos que se encuentren dentro de las dos jerarquías inferiores a la del director general o del administrador único de la ITF, que tengan a su cargo la responsabilidad del manejo de la información. Asimismo, podrán designar como responsables del envío de la información a más de una persona, en función del tipo de información de que se trate.

Las ITF podrán solicitar nuevas claves de usuarios o el acceso a reportes regulatorios en el SITI, mediante envío electrónico a la dirección “cesiti@cnbv.gob.mx” en la misma forma en que se señala en el Anexo 20.

Una vez enviado el correo electrónico al que se refiere el presente artículo, la CNBV notificará a la ITF por el mismo medio, dentro de los cinco días hábiles siguientes a la recepción de la solicitud, la confirmación del alta del responsable que corresponda, así como, en su caso, el acceso de los usuarios de los reportes regulatorios solicitados.

La notificación o sustitución de cualquiera de las personas responsables del envío y calidad de la información a que se refiere el presente artículo, deberá notificarse a la CNBV en los términos antes señalados, dentro de los tres días hábiles siguientes al de su designación o sustitución.

**T R A N S I T O R I O S**

**PRIMERO.-** La presente Resolución entrará en vigor a los ---- días siguientes al de su publicación en el Diario Oficial de la Federación.

**SEGUNDO.-** El Título Cuarto que se adiciona a las Disposiciones de carácter general aplicables a las instituciones de tecnología financiera mediante esta Resolución, entrará en vigor el 1 de enero de 2020, por lo que las instituciones de tecnología financiera comenzarán a entregar la información a que se refieren los artículos 99 y 101, con la periodicidad establecida en los artículos 100 y 102, respectivamente, en las fechas que se señalan a continuación, con la información que se detalla en cada caso:

I. Tratándose de las instituciones de financiamiento colectivo:

a) La información relativa a los reportes regulatorios de las series R01, R08, R10 y R13, exclusivamente por lo que se refiere a los reportes B-13212 y B-13222, a más tardar el 31 de enero de 2020, con la información que comprenda el periodo del 1 al 31 de diciembre de 2019.

b) La información relativa a los reportes regulatorios de la serie R13, exclusivamente por lo que se refiere a los reportes A-13112 y A-13162, a más tardar el 31 de enero de 2020, con la información que comprenda el periodo del 1 de octubre de 2019 al 31 de diciembre de 2019.

c) La información relativa a los reportes regulatorios de la serie R27, el 2 de enero de 2020, con la información que comprenda el periodo entre el 1 de octubre de 2019 al 31 de diciembre de 2019.

d) La información relativa a los reportes regulatorios de las series R24 y R36, el 2 de enero de 2020, con la información al cierre del 31 de diciembre de 2019 y de 1 de enero de 2020.

II. Tratándose de las instituciones de fondos de pago electrónico:

a) La información relativa a los reportes regulatorios de las series las series R01, R08, R10 y R13, exclusivamente por lo que se refiere a los reportes B-13211 y B-13221, a más tardar el 31 de enero de 2020, con la información que comprenda el periodo del 1 al 31 de diciembre de 2019.

b) La información relativa a los reportes regulatorios de las series R13, exclusivamente por lo que se refiere a los reportes A-13111 y A-13161, a más tardar el 31 de enero de 2020, con la información que comprenda el periodo entre el 1 de octubre de 2019 al 31 de diciembre de 2019.

c) La información relativa a los reportes regulatorios de la serie R27, el 2 de enero de 2020, con la información que comprenda el periodo entre el 1 de octubre de 2019 al 31 de diciembre de 2019.

d) La información relativa a los reportes regulatorios de la serie R26, el 2 de enero de 2020 con la información al cierre del 31 de diciembre de 2019.

e) La información relativa a los reportes regulatorios de la serie R36, proporcionándose el día hábil siguiente al de su fecha, el 2 de enero de 2020, con la información al cierre del 31 de diciembre de 2019 y de 1 de enero de 2020.

**TERCERO.-** La obligación prevista en el artículo 98 que se adiciona en esta Resolución a las Disposiciones de carácter general aplicables a las instituciones de tecnología financiera, entrará en vigor el 1 de septiembre de 2020.

**ARTÍCULO SEGUNDO.-** Se **REFORMA** el artículo QUINTO Transitorio y se **DEROGA** el artículo SÉPTIMO Transitorio de las “Disposiciones de carácter general aplicables a las instituciones de tecnología financiera” publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018, para quedar como sigue:

**“QUINTO.-** Las instituciones de financiamiento colectivo podrán considerar a sus Clientes como Inversionistas Experimentados en términos del artículo 2, fracción XXIII, inciso d) de estas disposiciones, si dichos Clientes hubieran realizado Operaciones a través de una o más de las personas a que se refiere la disposición OCTAVA Transitoria de la Ley para Regular las Instituciones de Tecnología Financiera.

**SÉPTIMO.-** Se deroga.”