SEGUNDA SECCION
PODER EJECUTIVO
SECRETARIA DE HACIENDA Y CREDITO PUBLICO

RESOLUCIÓN que modifica las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera. (Continúa en la Tercera Sección).

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- SHCP.- Secretaría de Hacienda y Crédito Público.- Comisión Nacional Bancaria y de Valores.

La Comisión Nacional Bancaria y de Valores, con fundamento en lo dispuesto por los artículos 18, fracción IV; 19, fracción IV; 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

CONSIDERANDO

Que la Comisión Nacional Bancaria y de Valores emitió la resolución publicada en el Diario Oficial de la Federación el 24 de julio de 2017, mediante la cual se reformaron las Disposiciones de carácter general aplicables a las casas de bolsa, para ampliar el plazo con el que estas cuentan para vender o reclasificar sus títulos conservados a vencimiento de 28 a 90 días, satisfaciendo así el artículo 78 de la Ley General de Mejora Regulatoria respecto del costo de cumplimiento de la presente resolución;

Que por otra parte, 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 incorporar el marco normativo sobre seguridad de sus sistemas e infraestructura tecnológica, determinando los controles internos que deberán tener, estableciendo además 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;

Que 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, aplicaciones informáticas, interfaces, páginas de Internet y similares; por ello, resulta indispensable a la luz 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 correspondientes 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 en 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 para emitir 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, estas deberán tener a disposición de los inversionistas 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, designar al 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 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 89 a 93, Segunda a denominarse "De la revelación de información del comportamiento de pago y desempeño del Solicitante o proyecto" con los artículos 94 a 96 y Tercera a denominarse "De la revelación de información al público en general" con el artículo 97; el Título Cuarto a denominarse "De los reportes regulatorios" con el Capítulo I a denominarse "De los reportes en general" con los artículos 98 a 103 y el Capítulo II a denominarse "De los medios de entrega" con el artículo 103; así como los Anexos 11, 12, 13, 14, 15, 16, 17, 18, 19 y 20; 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

De los reportes regulatorios

Capítulo I

De los reportes en general

Capítulo II

De los 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 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.

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

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

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

XXXVII. 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.

XXXVIII. 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 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 dicha institución, 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.

V. 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:

a) Mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio.

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 en manuales las políticas y procedimientos para las autorizaciones de accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con accesos por eventos de contingencia, entre otros. Dichas políticas y procedimientos deberán ser aprobados por el oficial en jefe de seguridad de la información.

b) Cifrado de la información conforme al grado de sensibilidad o clasificación de la información que la institución de financiamiento colectivo determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes o almacenada en la Infraestructura Tecnológica o se acceda de forma remota.

Las instituciones de financiamiento colectivo deberán cifrar al menos, la información que hayan clasificado como crítica en términos de estas disposiciones.

c) Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el Usuario de la Infraestructura Tecnológica sea quien las conozca, así como medidas de seguridad, Cifrado en su almacenamiento y mecanismos para solicitar el cambio de claves de acceso cada noventa días o menos. Tratándose de Clientes, el plazo referido será el definido por las propias instituciones de financiamiento colectivo en los manuales a que alude el último párrafo de este artículo. En el caso de los Usuarios de la Infraestructura Tecnológica asignados a aplicativos o componentes para autenticarse entre ellos, el cambio a que alude este inciso deberá realizarse, al menos, una vez al año. En el evento de que algún Usuario de la Infraestructura Tecnológica tenga conocimiento de las claves de acceso y deje de prestar sus servicios a la institución de financiamiento colectivo, estas deberán inhabilitarse de manera inmediata.

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.

Las instituciones de financiamiento colectivo, en la clasificación de la información a que alude el inciso b) de esta fracción, deberán considerar al menos una categoría referente a la información crítica. En dicha categoría deberán incluir como mínimo la Información Sensible y las imágenes de identificaciones oficiales e información biométrica de los Clientes, así como cualquier otra que determinen de acuerdo con sus políticas.

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 al personal de las diferentes áreas de la institución de financiamiento colectivo para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con el artículo 66 de las presentes disposiciones.

En caso de que se detecte la existencia de vulnerabilidades y deficiencias en la Infraestructura Tecnológica, deberán tomarse las acciones correctivas o controles compensatorios de acuerdo con el nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la institución de financiamiento colectivo puedan verse afectados.

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

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. Las pruebas de penetración 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 componentes, sistemas o aplicativos distintos que hayan sido determinados por la institución de financiamiento colectivo como de mayor riesgo, o bien, cuando lo ordene la CNBV habiendo detectado vulnerabilidades o factores que puedan afectar 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 llevadas 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 dirigidos a todo el personal, así como de concientización en materia de seguridad de la información hacia los Clientes incluyendo, en su caso, a terceros que les presten servicios, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de Infraestructura Tecnológica tengan al respecto.

IX. Realizar, de manera proactiva e interactiva, 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 alteradas 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 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.

Las instituciones de financiamiento colectivo podrán designar como oficial en jefe de seguridad de la información al director general, o en su caso, al administrador único, durante un plazo máximo de doce meses, contados a partir de la fecha en que obtengan la autorización para actuar como tales.

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. Dicho plan 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 de las auditorías realizadas relacionadas 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 su 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 dirigidos a todo el personal, así como de concientización en materia de seguridad de la información 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.- Cuando se presente un Evento de Seguridad de la Información o Incidente de Seguridad de la Información en: (i) los componentes de la Infraestructura Tecnológica de la institución de financiamiento colectivo; (ii) los canales de atención a los Clientes, tales como Medios Electrónicos, o (iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la institución de financiamiento colectivo, el director general o, en su caso, el administrador único, deberá:

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 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.

En el caso de Eventos de Seguridad de la Información, deberán reportarse a través de los medios señalados en el primer párrafo de esta fracción solo aquellos que, de acuerdo con las políticas y procedimientos establecidos por la propia institución de financiamiento colectivo, se califiquen como relevantes por tener potencial afectación para la institución de financiamiento colectivo, sus Clientes, contrapartes, proveedores u otras entidades del sistema financiero, además de los relacionados con Información Sensible, imágenes de identificaciones oficiales e información biométrica de los Clientes. Este reporte únicamente deberá contener la fecha y hora de inicio, así como la descripción del evento de que se trate.

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 pueden realizar.

II. Los mecanismos y procedimientos de identificación y Autenticación.

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 establecidos en 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 los 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.