COMISIÓN PARA EL MERCADO FINANCIERO

REF: **REGULA EL REGISTRO, AUTORIZACIÓN Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS FINANCIEROS DE LA LEY FINTEC**

NORMA DE CARÁCTER GENERAL N°502

12 de enero de 2024

Esta Comisión, en uso de las facultades que le confieren los artículos 1, 3, 5 en sus numerales 1, 8 y 18, y 20 en su numeral 3 del Decreto Ley N°3.538; los artículos 4, 5, 6, 7, 8, 9, 10, 11, 12 y 13 de la Ley N° 21.521; y lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°374 de 11 de enero de 2024, ha estimado pertinente impartir las siguientes instrucciones respecto de la prestación de servicios financieros basados en tecnología a los que se refiere el título II de la Ley N°21.521, Ley Fintec:

ÍNDICE

I. REGISTRO DE PRESTADORES DE SERVICIOS FINANCIEROS

A. SOLICITUD DE INSCRIPCIÓN

Para prestar los servicios regulados por la Ley N°21.521 en Chile, se deberá solicitar la previa inscripción en el Registro de Prestadores de Servicios Financieros al que se refiere el artículo 5 de la Ley N° 21.521. Se entenderá que prestan servicios en Chile quienes materialmente los realicen en el país, a través de la habilitación o contratación de medios físicos o electrónicos para prestar sus servicios en el país, así como quienes empleen cualquier medio de comunicación para dirigir la oferta de sus servicios a personas residentes en Chile, independiente del país de origen de dichos medios.

A efectos de solicitar la inscripción en el Registro, se deberá ingresar una solicitud a través del sitio web de la Comisión, la que deberá ser presentada por el representante legal o convencional del solicitante, quien será el responsable de la veracidad e integridad de toda la información proporcionada a la Comisión.

La referida solicitud de inscripción deberá contener la siguiente información:

a) Nombre o Razón social de la persona o entidad y nombre de fantasía o comercial en caso de contar con uno. En el caso entidades extranjeras que pretendan prestar los servicios del título II de la Ley N°21.521 sin constituir una sociedad en Chile, estos antecedentes estarán referidos a la agencia en Chile.

b) Número de cédula de identidad o pasaporte, o Rol Único Tributario o Legal Entity Identifier, si tuviere, en el caso de entidades extranjeras.

c) Identificación de la persona natural con poder para actuar en representación convencional o legal en Chile de la persona o entidad: nombre completo y cédula nacional de identidad o pasaporte.

d) Número de Teléfono.

e) Dirección de correo electrónico para efectos de las notificaciones y comunicaciones que practique esta Comisión.

f) URL del sitio web al que se refiere el inciso primero del artículo 5 de la Ley N°21.521.

Además, junto a la solicitud, se deberán acompañar los siguientes antecedentes:

1. Tratándose de personas jurídicas constituidas en Chile (sean o no de propiedad de extranjeros):

   i. En el caso de sociedades que no estén sometidas al régimen simplificado establecido en la Ley N°20.659 e inscritas en el Registro de Empresas y Sociedades del Ministerio de Economía, Fomento y Turismo, copia de la escritura de constitución y de las escrituras modificatorias de los últimos 10 años, de las inscripciones de los extractos de cada una de éstas, y de la publicación de éstos en el Diario Oficial, junto con el certificado de vigencia de la sociedad y una copia de la inscripción social con constancia de las

anotaciones marginales practicadas, ambos de una antigüedad inferior a 15 días contados desde la fecha de la solicitud.

ii. En el caso de sociedades sometidas al régimen simplificado de la Ley N°20.659, no será necesario acompañar otros antecedentes.

2. Las entidades constituidas en el extranjero y que prestarán los servicios de la Ley N°21.521 sin constituir una sociedad en Chile, deberán establecer una agencia y adjuntar a la solicitud copia del extracto a que se refiere el artículo 123 de la Ley N°18.046 o el artículo 449 del Código de Comercio según corresponda. No obstante, en el caso de acogerse a la excepción contenida en la letra C.3 siguiente, bastará con la declaración a la que se refiere esa letra.

3. En caso de que la solicitud la presente una persona natural en calidad de representante convencional de la persona o entidad que motiva la solicitud, deberá acompañar copia del documento público o privado en el que consta el poder correspondiente.

4. Declaración de no estar afecto a las inhabilidades a que se refiere el inciso segundo del artículo 6 de la Ley N°21.521:

i. En el caso de personas jurídicas, al efectuar la solicitud de inscripción la persona natural facultada para actuar por ésta declarará, identificándose mediante el mecanismo electrónico dispuesto para esos efectos en el sitio en Internet de la Comisión, que ni la entidad ni sus socios principales, directores o administradores se encuentran en alguna de las circunstancias a las que se refiere el inciso segundo del artículo 6 de la Ley N°21.521, en Chile ni en el extranjero.

ii. En el caso de personas naturales que se acojan a la excepción de personalidad jurídica contenida en la letra C.1 de esta sección, declaración efectuada en el sitio en Internet de la Comisión, identificándose mediante el mecanismo electrónico dispuesto para esos efectos, respecto a que no se encuentra en alguna de las circunstancias a las que se refiere el inciso segundo del artículo 6 de la Ley N°21.521, en Chile ni en el extranjero.

5. Certificado de Procedimientos Concursales Vigentes / Quiebras, emitido por la Superintendencia de Insolvencia y Reemprendimiento, en el que conste que la persona o entidad cuya inscripción se solicita no se encuentra en los registros de quiebra, ni está sometida a un procedimiento concursal de liquidación, reorganización o renegociación, de una antigüedad igual o inferior a los 30 días. En el caso de agencias dicha circunstancia estará referida a la entidad extranjera y se declarará en los mismos términos al que se refiere el número 1) del número 4) anterior.

6. En el caso de personas jurídicas:

   i. Identificación de cada socio principal, director o administrador: nombre completo, nacionalidad, y cédula de identidad o número de pasaporte en caso de extranjeros. En virtud de lo señalado en el inciso segundo del artículo 6 de la Ley N°21.521, para estos efectos se entenderá como socio principal a las personas naturales que posean directa o indirectamente una participación igual o superior al 10% del capital o tengan la capacidad de elegir a lo menos un miembro del directorio o administración.

   ii. Estructura de propiedad del grupo empresarial al que pertenece, indicando los principales negocios que realizan las empresas de ese grupo. Para estos efectos, debe estarse a lo establecido en el artículo 96 de la Ley N°18.045.

7. Síntesis del plan estratégico (misión, visión y objetivos) y del plan de negocios, indicando las principales líneas de negocios, las actividades que pretende realizar, refiriéndose expresamente los servicios del Título II de la Ley N°21.521 que llevará a cabo, los ingresos y egresos esperados, tipo de clientes a los cuales se encuentran dirigidos los servicios que prestarán y el organigrama con una descripción de las principales funciones de sus áreas, cargos claves, comités y estructura de responsabilidades.

Ingresada la solicitud y verificada la completitud de los antecedentes requeridos en la presente sección, se procederá a la inscripción de la entidad en el Registro, previo pago por parte del solicitante de los derechos establecidos en el artículo 33 del D.L. N°3.538. Cabe señalar que lo anterior no habilita a las entidades a acompañar material gráfico de propiedad de la Comisión en la divulgación de información, propaganda o publicidad que efectuaren por cualquier medio, por cuanto esta Comisión ha registrado la marca comercial correspondiente y cuenta con la protección de la Ley N°19.039, en especial lo dispuesto en el artículo 19 bis D, que la faculta para oponerse al uso que puedan hacer terceros de la mencionada marca comercial.

Sin perjuicio de lo anterior se hace presente que, conforme al artículo 14 letra a) de la Ley N°21.521, es una infracción grave el prestar los servicios regulados por esa Ley sin estar inscrito en el registro o sin haber obtenido la autorización para prestar los servicios y que entre los agravantes a los que se refiere el artículo 15 de la misma Ley se encuentra el fingir la calidad de inscrito en el Registro o de supervisado por la Comisión, lo cual incluye, entre otros, el presentarse como regulado o dar la impresión de serlo utilizando material gráfico de propiedad de la Comisión en la divulgación de información, propaganda o publicidad que realizaren.

Para el evento que una solicitud se encuentre incompleta o presentada de tal forma que requiera un gran número de correcciones, la Comisión podrá solicitar a la entidad que efectúe una nueva presentación.

En el evento de que por la inactividad del solicitante se produzca por más de treinta días la paralización del procedimiento y se proceda conforme a lo dispuesto en el artículo 43 de la Ley N°19.880 que Establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado, se entenderá por no presentada la solicitud de inscripción.

Desde la fecha de la solicitud de inscripción y mientras la persona esté inscrita en el Registro, se deberá informar, a través del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, cualquier modificación que haya sufrido la información proporcionada con motivo de la solicitud, dentro del plazo de cinco días hábiles de ocurrido el hecho respectivo o tomado conocimiento de este. Lo anterior, sin perjuicio que, tratándose de cambios a la información de identificación del solicitante a que se refieren las letras a) y b) anteriores, dicha comunicación deberá ser acompañada de una solicitud de anotación en el Registro, debiéndose pagar los derechos establecidos en el artículo 33 del D.L. N°3.538. Por consiguiente, junto con la inscripción en el Registro, la Comisión otorgará al representante un nombre de usuario y contraseña para el acceso y utilización del sistema implementado por la Comisión para estos efectos.

De conformidad con lo establecido en el artículo 6 de la Ley N°21.521, sólo procederá la inscripción de personas jurídicas cuyo giro exclusivo sea la prestación de uno o más los servicios regulados por la Ley N°21.521 y aquellas actividades que la Comisión haya autorizado por normativa, razón por la que quienes soliciten su inscripción deberán tener ese sólo objeto social. Lo anterior, con la excepción de quienes se encuentren en las circunstancias y condiciones establecidas en la letra C de esta sección, para lo cual deberán acompañar a su solicitud de inscripción los antecedentes exigidos en dicha sección.

B. CANCELACIÓN DE LA INSCRIPCIÓN

Para efectos de requerir su cancelación del Registro de Prestadores de Servicios Financieros, se deberá remitir a la Comisión una solicitud de cancelación suscrita por el representante de la entidad. En el caso de personas jurídicas, a partir de dicha cancelación deberá procederse con la correspondiente reforma de estatutos para adecuar el objeto social a servicios que no estén regulados ni sometidos a obligación de inscripción.

Lo anterior, sin perjuicio que esta Comisión pueda proceder a la cancelación de oficio de la inscripción de quienes, conforme a lo dispuesto en el artículo 13 de la Ley N° 21.521, no hubieren solicitado la autorización para realizar alguna de las actividades reguladas por dicha Ley dentro del plazo de doce meses contado desde la inscripción correspondiente, así como también de quienes en un periodo de 12 meses continuos no hubieren realizado las actividades que les fueron autorizadas.

Asimismo, la Comisión procederá a la cancelación de la inscripción en el Registro de aquellas entidades que pasen a tener la calidad de deudor en un procedimiento concursal de liquidación, de conformidad a lo prescrito en el artículo 13 de la Ley N° 21.521, o en aquellos casos en que la entidad hubiere sido sancionada por las infracciones graves a que se refiere el artículo 14 de la misma Ley; o, de aquellas que dejen de cumplir con alguno de los requisitos en virtud de los cuales se procedió con su inscripción.

C. EXCEPCIONES

C.1. DEL REQUISITO DE PERSONA JURÍDICA

En virtud de lo establecido en el artículo 4° de la Ley N° 21.521, se exceptúa del requisito de constituirse como persona jurídica a efectos de solicitar su inscripción en el Registro de Prestadores de Servicios Financieros a las personas naturales que sólo se dediquen a la prestación del servicio de asesoría de inversión, y siempre que cumplan los siguientes requisitos copulativos:

a) Que sólo efectúen asesorías a personas determinadas; y

b) Que el número de personas determinadas a las que efectuaron asesorías por medio de cualesquiera de los medios que emplea para ese efecto, incluidas redes sociales, en los últimos doce meses, no supere las 100.000 personas.

Para acreditar esta circunstancia, bastará con la declaración que efectúe la persona a través del sitio en Internet de la Comisión, mediante el mecanismo electrónico dispuesto para esos efectos. Dicha declaración deberá actualizarse cada 12 meses a partir de la fecha de inscripción.

C.2. DEL GIRO EXCLUSIVO Y AUTORIZACIÓN DE SERVICIOS

En virtud de lo establecido en el artículo 4° de la Ley N°21.521 se exceptúa del requisito de giro exclusivo a efectos de solicitar su inscripción en el Registro de Prestadores de Servicios Financieros y del requisito de solicitar autorización para la prestación de los servicios de asesoría de inversión, asesoría crediticia, sistema alternativo de transacción y plataforma de financiamiento colectivo, a quienes cumplan las siguientes circunstancias copulativas:

a) Que, entre los servicios regulados por la Ley N°21.521, sólo presten el servicio de asesoría de inversión, asesoría crediticia, sistema alternativo de transacción y plataforma de financiamiento colectivo.

b) Que la prestación de los servicios regulados por esta normativa sólo sea provista a inversionistas calificados a los que se refiere la letra f) del artículo 4 Bis de la Ley N°18.045.

Para acogerse a esta excepción, el solicitante deberá efectuar una declaración respecto del hecho que dará cumplimiento a las circunstancias antes descritas. Dicha declaración, deberá ser efectuada a través del mecanismo electrónico dispuesto para el ingreso de la solicitud de inscripción, en el sitio en Internet de la Comisión. Además, dicha declaración deberá ser actualizada anualmente a través del mecanismo establecido para ello en el sitio en Internet de la Comisión.

C.3. DEL DOMICILIO EN CHILE Y AUTORIZACIÓN DE SERVICIOS

En virtud de lo establecido en el artículo 4° de la Ley N° 21.521 se exceptúa a las entidades extranjeras del requisito de contar con domicilio en Chile a efectos de solicitar su inscripción en el Registro de Prestadores de Servicios Financieros y del requisito de solicitar autorización para la prestación de los servicios de asesoría de inversión, asesoría crediticia, sistema alternativo de transacción y plataforma de financiamiento colectivo, en las siguientes circunstancias copulativas:

a) Que sólo presten en Chile los servicios de asesoría de inversión, asesoría crediticia, sistema alternativo de transacción y plataforma de financiamiento colectivo; y

b) Que la prestación en Chile de los servicios regulados por esta normativa sólo sea provista a inversionistas calificados a los que se refiere la letra f) del artículo 4 Bis de la Ley N°18.045.

Para acogerse a esta excepción, el solicitante deberá efectuar una declaración respecto del hecho que dará cumplimiento a las circunstancias antes descritas. Dicha declaración deberá ser efectuada a través del mecanismo electrónico dispuesto para el ingreso de la solicitud de inscripción, en el sitio en Internet de la Comisión. Además, dicha declaración deberá ser actualizada anualmente a través del mecanismo establecido para ello en el sitio en Internet de la Comisión.

II. AUTORIZACIÓN PARA LA PRESTACIÓN DE SERVICIOS

Previo a prestar cualesquiera de los servicios regulados por el Título II de la Ley N°21.521, las entidades deberán solicitar la autorización de esta Comisión, la cual podrá ser presentada junto con la solicitud de inscripción en el Registro de Prestadores de Servicios Financieros o una vez inscritas en el mismo. Para estos efectos, deberán remitir la solicitud respectiva a través del sitio web de la Comisión, la que deberá ser presentada por el representante legal o convencional del solicitante, quien será el responsable de la veracidad e integridad de toda la información proporcionada a la Comisión.

Dicha solicitud deberá señalar expresamente el o los servicios para los cuales solicita autorización y ser acompañada de los antecedentes que se indican más adelante según el servicio del que se trate. Los manuales, descripciones y reglamentación interna que se solicitan en esta Sección deberán ser presentados en idioma español o inglés, señalando expresamente en los mismos el caso que estos correspondan a una traducción del original.

Para el evento que una solicitud se encuentre incompleta o presentada de tal forma que requiera un gran número de correcciones, la Comisión podrá requerir al solicitante que efectúe una nueva presentación, entendiendo como no presentada la ingresada con anterioridad.

En el evento de que por la inactividad del solicitante se produzca por más de treinta días la paralización del procedimiento y se proceda conforme a lo dispuesto en el artículo 43 de la Ley N°19.880 que Establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado, se entenderá por no presentada la solicitud de autorización.

En el caso que luego de tramitada la referida solicitud de autorización, la misma sea rechazada para todos los servicios que se hubiere solicitado, se procederá a la cancelación de la inscripción en el Registro de Prestadores de Servicios Financieros de quienes no tuvieren otra autorización vigente a esa fecha.

Desde la fecha de solicitud y mientras se encuentre vigente la autorización será responsabilidad de la entidad o persona mantener actualizada la información a la que se refiere esta sección a través del módulo del sistema de información y comunicación dispuesto por la Comisión para estos efectos.

A. ASESORIA DE INVERSIÓN

a) Identificación de los canales mediante los que interactuará con clientes o el público, indicando, en lo que corresponda:

   1) Los nombres de usuario o apodos que emplea para identificarse en esos canales.

   2) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   3) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Documento que contenga las políticas a que se refiere la letra A de la Sección IV de esta normativa que le resulten aplicables conforme a lo establecido en la letra A.4

de esa sección. Para acogerse a alguna de las excepciones a las que se refiere esa letra A.4 deberá declarar las condiciones que justifican la excepción.

c) Documento con la descripción general del procedimiento y forma en que se prestará el servicio, indicando aquellas partes del proceso que son realizados por personas o por algoritmos informáticos, y cuáles con recursos propios, subcontratados o adquiridos a terceros. Al referirse a las partes del proceso que son realizadas por esos algoritmos, deberá describir en términos generales el funcionamiento del mismo, indicando claramente el grado de automatización e intervención humana requerido.

d) En el caso de que las recomendaciones de inversión emanen de un algoritmo informático, sin intervención humana, se deberá acompañar el certificado de acreditación de conocimientos de la persona responsable de verificar la coherencia de dicho algoritmo, esto es, la coherencia entre los elementos ingresados al algoritmo para realizar la recomendación, los resultados que éste entrega y las necesidades manifestadas por los clientes que contratan dichos servicios, conforme a las exigencias establecidas en la Norma de Carácter General N°503.

e) En el caso que las recomendaciones de inversión emanen de personas naturales, se deberá acompañar el certificado de acreditación de conocimientos de al menos una de esas personas, conforme a las exigencias establecidas en la Norma de Carácter General N°503 Tratándose de personas naturales que se acojan a lo dispuesto en la sección I de la Norma de Carácter General N°503, respecto a las condiciones que le permitan desempeñar excepcionalmente sus funciones de manera temporal sin haber aprobado el examen de acreditación de conocimientos, se deberá hacer expresa mención a ese hecho.

Las personas naturales a las que se refieren las dos letras anteriores, es decir, las responsables de verificar la coherencia de los algoritmos y de las cuales emanan las recomendaciones de inversión, previo a desempeñar esa función deberán haber aprobado un programa académico de carácter profesional o técnico, nacional o extranjero, sobre materias relacionadas con el mercado financiero, su funcionamiento, marco jurídico, participantes o instrumentos, de una duración de al menos 4 semestres. Lo anterior deberá acreditarse en conjunto y en los mismos términos establecidos en las letras d) y e), acompañando un documento en que conste que la persona sobre la que se solicita antecedentes en cada una de esas letras ha aprobado el referido programa académico.

En caso de que el servicio se preste sólo a personas que tengan la condición de Inversionista Calificado a los que se refiere la letra f) del artículo 4 Bis de la Ley N°18.045, bastará con la sola declaración respecto a ese hecho que efectúe el representante de la entidad en el sitio en Internet de la Comisión, mediante el mecanismo electrónico dispuesto para esos efectos, no siendo necesario acompañar los antecedentes a que se refieren las letras a) a e) anteriores. Lo anterior, en ningún caso exime a la entidad de cumplir con los requisitos establecidos en esta normativa y que no se hayan eximido expresamente en virtud de esa circunstancia.

B. ASESORÍA CREDITICIA

a) Identificación de los canales mediante los que interactuará con clientes o el público, indicando, en lo que corresponda:

   1) Los nombres de usuario o apodos que emplea para identificarse en esos canales.

   2) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   3) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Documento que contenga las políticas a que se refiere la letra B de la Sección IV de esta normativa que le resulten aplicables conforme a lo establecido en la letra B.4 de esa sección. Para acogerse a alguna de las excepciones a las que se refiere esa letra B.4 deberá declarar las condiciones que justifican la excepción.

c) Documento con la descripción general del procedimiento y forma en que se prestará el servicio, indicando aquellas partes del proceso que son realizados por personas o por algoritmos informáticos y cuáles con recursos propios, subcontratados o adquiridos a terceros.

d) En el caso de que las evaluaciones o verificaciones de identidad emanen de un algoritmo informático, sin intervención humana, se deberá designar a una persona responsable de verificar la coherencia de dicho algoritmo, esto es, la coherencia entre los elementos ingresados al algoritmo para realizar la evaluación, los resultados que éste entrega y las necesidades manifestadas por los clientes que contratan dichos servicios. Las personas naturales responsables de verificar la coherencia de los algoritmos y de las cuales emanan las evaluaciones o las verificaciones de identidad, previo a desempeñar esa función deberán haber aprobado un programa académico de carácter profesional o técnico, nacional o extranjero, sobre materias relacionadas con análisis de datos, estadísticas, finanzas, evaluación de la identidad o capacidad de pago de personas o entidades, de una duración de al menos 4 semestres. A estos efectos, se deberá acompañar un documento en que conste que la persona natural encargada de verificar la coherencia del algoritmo o al menos una persona natural de la cual emane las evaluaciones o las verificaciones de identidad realizadas por el prestador del servicio, ha aprobado el programa académico referido en el párrafo anterior.

En caso de que el servicio se preste sólo a personas que tengan la condición de Inversionista Calificado a los que se refiere la letra f) del artículo 4 Bis de la Ley N°18.045., bastará con la sola declaración respecto a ese hecho que efectúe el representante de la entidad en el sitio en Internet de la Comisión, mediante el mecanismo electrónico dispuesto para esos efectos, no siendo necesario acompañar los antecedentes a que se refieren las letras a) a d) anteriores. Lo anterior, en ningún caso exime a la entidad de cumplir con los requisitos establecidos en esta normativa y que no se hayan eximido expresamente en virtud de esa circunstancia.

C. PLATAFORMA DE FINANCIAMIENTO COLECTIVO

a) Identificación de los canales mediante los que interactuará con clientes o el público, indicando, en lo que corresponda:

   1) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   2) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Identificación del bloque al que se refiere la letra C.6 de la Sección IV de esta normativa que le resulta aplicable al solicitante, acompañando una declaración en que se detallen las condiciones que justifican la clasificación del prestador de servicios en determinado bloque.

c) Documento que contenga las políticas a que se refieren la letra C de la Sección IV, que le resulten aplicables conforme a la clasificación de bloques a la que se refiere la letra C.6 de la Sección IV.

d) Documento con la descripción de los procedimientos que se llevarán a cabo para prevenir que los proyectos o necesidades de financiamiento que se difundan en la plataforma resulten fraudulentos, o que los recursos provengan o estén destinados a actividades ilícitas.

e) Documento con la descripción de los procedimientos que se llevarán a cabo, de forma adicional a aquellos referidos en la letra d) anterior, para analizar la viabilidad económica, jurídica y financiera de aquellos proyectos de inversión o necesidades de financiamiento que se difundan en la plataforma con el fin de obtener recursos por montos superiores al equivalente a 20.000 Unidades de Fomento. No será necesario acompañar este documento si esa descripción está contenida en los documentos a que se refiere la letra c) anterior.

f) Documento con la descripción de los mecanismos establecidos para acotar o ajustar el grado de exposición al riesgo que tienen en los proyectos quienes entregan financiamiento en la plataforma, conforme a las expectativas o necesidades por ellos manifestadas.

g) Documento con la descripción de la información sobre los proyectos de inversión o necesidades de financiamiento que será divulgada conforme a lo establecido en la Sección III de esta normativa, acompañando un ejemplar, a modo ilustrativo, de la forma en que entregará la información.

D. SISTEMA ALTERNATIVO DE TRANSACCIÓN

a) Identificación de los canales a través de los cuales se accederá al sistema transaccional, indicando, en lo que corresponda:

   1) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   2) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Identificación del bloque al que se refiere la letra C.6 de la Sección IV de esta normativa que resulta aplicable al solicitante, acompañando una declaración en que se detallen las condiciones que justifican la clasificación del prestador de servicios en determinado bloque.

c) Documento que contenga las políticas a que se refiere la letra C de la Sección IV de esta normativa, que le resulten aplicables conforme a la clasificación de bloques a la que se refieren la letra C.6 de la Sección IV.

d) Documento con la descripción de los mecanismos establecidos para acotar o ajustar el grado de exposición al riesgo que tienen en los instrumentos financieros los participantes del sistema, conforme a las expectativas o necesidades por ellos manifestadas.

e) Acreditación de la capacidad operacional conforme a lo establecido en la Sección VI de esta normativa.

f) Documento con la descripción de la información que será divulgada conforme a lo establecido en la Sección III de esta normativa, acompañando un ejemplar, a modo ilustrativo, de la forma en que se entregará la información.

g) Reglamentación interna, la que al menos deberá referirse a las siguientes materias:

   1) **Normas de Acceso**: qué condiciones objetivas y no discriminatorias se exigirán a los participantes para tener acceso a los sistemas y poder ingresar ofertas de compraventa de instrumentos financieros, y cómo se acreditará el cumplimiento de las mismas. Además, las circunstancias en que los participantes pudieran ser suspendidos o expulsados del sistema.

   2) **Normas de admisión a negociación de instrumentos**: qué características o condiciones deberán cumplir los instrumentos financieros, sus emisores, activos representados, garantes, garantías, protocolos, deudores o custodios, según corresponda, para ser admitidos a cotización en el sistema y cómo se verificará su cumplimiento. Para lo cual deberá distinguir entre aquellos instrumentos que, por su naturaleza, requieran reglas de admisión diferenciadas. Además, respecto de activos virtuales, sólo se admitirán a cotización criptoactivos que cuenten con un documento público que contenga las especificaciones técnicas que permitan conocer la tecnología y aspectos relevantes para quienes los adquieren como, por ejemplo, qué activos son representados digitalmente, qué derechos tendrá quien adquiere el criptoactivo, respecto de quién tendrá esos derechos**,** y si son civiles o naturales. Todo ello, de conformidad con las especificaciones mínimas que establezca el sistema alternativo para estos efectos. Dicho documento público

podrá ser la traducción al español o inglés de su original o de aquel que el propio sistema alternativo haya elaborado para ese efecto.

3) **Reglas de formación de precios**: qué mecanismos de recepción de ofertas o posturas, y de calce de las mismas se emplearán; esto es, si será mediante un libro abierto de ofertas, un sistema de calce automático de ofertas compatibles, una subasta abierta o una licitación, entre otros, y cómo se priorizarán las ofertas que compiten entre sí.

4) **Reglas de liquidación**: cómo se deberá proceder con posterioridad al cierre de la negociación al objeto de materializar la entrega física, lógica o simbólica del instrumento financiero adquirido y el pago por la compra del mismo, o a pagar los saldos a favor que se produzcan, según corresponda, y qué rol tendrá en ese proceso el sistema alternativo.

5) **Mecanismos de suspensión**: normas que establezcan si el sistema contará con reglas o criterios para suspender o cancelar la cotización, oferta o transacción de los instrumentos financieros, por variación significativa de precios, ciberataques, fraudes u otras circunstancias relevantes que ameriten adoptar esa medida para prevenir que clientes se vean afectados. Además, el mecanismo que empleará para suspender o cancelar la cotización de aquellos instrumentos que dejen de cumplir las características o condiciones en virtud de las cuales se les admitió al sistema, y comunicar ese hecho a sus clientes.

Sin perjuicio de que la reglamentación no queda sujeta a la aprobación de esta Comisión, toda modificación o actualización de ésta deberá ser remitida a este Servicio a más tardar el día en que entre en vigor.

Quienes presten el servicio de sistema alternativo de transacción en ningún caso podrán admitir a cotización o permitir el ingreso de ofertas que consistan en colocaciones primarias de títulos valores o de criptoactivos (por ejemplo, "Initial Public Offering" o "Initial Coin Offering"), sin haber obtenido la autorización previa para actuar como plataforma de financiamiento colectivo y cumpliendo con todas las obligaciones exigibles a esas plataformas respecto de ese tipo de colocaciones primarias.

Para los efectos de la Ley N°21.521, no quedará comprendido dentro del servicio de sistema alternativo de transacción la mera puesta disposición a personas de un sistema de comunicación (como Whatsapp, IRC, Zoom, MS Teams, entre otros), salvo que éste contemple en su diseño mecanismos o herramientas que tienen por objeto permitir a los usuarios el intercambio o cierre de ofertas, órdenes o posturas de compra o venta de instrumentos financieros o títulos valores.

E. ENRUTAMIENTO DE ÓRDENES

a) Identificación de los canales a través de los cuales se accederá a los servicios, indicando, en lo que corresponda:

   1) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   2) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Documento que contenga las políticas a que se refiere la letra D de la Sección IV de esta normativa que le resulten aplicables conforme a lo establecido en la letra D.4 de esa Sección. Para acogerse a alguna de las excepciones a las que se refiere esa letra D.4 deberá acompañar una declaración en que se detallen las condiciones que justifican la excepción.

c) Documento que acredite la constitución de la garantía del artículo 10° de la Ley N°21.521, de conformidad a lo establecido en la Sección V de esta normativa, que le resulte aplicable conforme a lo establecido en la letra A. de esa Sección.

d) Documento con la descripción de la información que será divulgada conforme a lo establecido en la Sección III de esta normativa, acompañando un ejemplar, a modo ilustrativo, de la forma en que entregará la información.

e) Acreditación de la capacidad operacional conforme a lo establecido en la Sección VI de esta normativa.

F. INTERMEDIACIÓN Y CUSTODIA DE INSTRUMENTOS FINANCIEROS

a) Identificación de los canales a través de los cuales se accederá a los servicios, indicando, en lo que corresponda:

   1) Las aplicaciones que se deben emplear para acceder a esos canales y en qué plataforma se soportan.

   2) En caso de canales físicos, el o los domicilios en que se da esa interacción.

b) Identificación del bloque al que se refiere la letra E.6 de la Sección IV de esta normativa que resulta aplicable al solicitante, acompañando una declaración en que se detallen las condiciones que justifican la clasificación del prestador de servicios en determinado bloque.

c) Documento que contenga las políticas y procedimientos a que se refiere la letra E de la Sección IV de esta normativa, que le resulten aplicables conforme a la clasificación de bloques a la que se refieren la letra E.6 de la Sección IV.

d) Documento que acredite la constitución de la garantía del artículo 10° de la Ley N°21.521, de conformidad a lo establecido en la Sección V de esta normativa, que le resulte aplicable conforme a lo establecido en la letra A de esa Sección.

e) Estados financieros anuales auditados de la entidad con una antigüedad no mayor a 12 meses y, adicionalmente, estados financieros del trimestre inmediatamente anterior a la solicitud cuando los estados financieros auditados sean de una antigüedad superior a 6 meses a la fecha de la solicitud. Además, deberán acompañar una declaración en la cual se detalle el cálculo del patrimonio ajustado, el cual deberá ser actualizado anualmente a través del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

f) Tratándose de quienes soliciten autorización para prestar el servicio de custodia de instrumentos financieros, en el evento que mantengan instrumentos custodiados al momento de realizar la solicitud, deberán remitir un resumen de la cantidad de clientes que poseen y el monto agregado en custodia por instrumento financiero a la fecha de solicitud.

g) Documento con la descripción de la información que será divulgada conforme a lo establecido en la Sección III de esta normativa, acompañando un ejemplar, a modo ilustrativo, de la forma en que entregará la información.

h) Acreditación de la capacidad operacional conforme a lo establecido en la Sección VI de esta normativa**.**

III. OBLIGACIONES DE DIVULGACIÓN Y ENTREGA DE INFORMACIÓN

Los proveedores de servicios financieros, independiente de las actividades que les hayan sido autorizadas, deberán implementar políticas, procedimientos y controles para cumplir con las obligaciones de información a las que se refiere la presente sección.

En particular, toda información que se elabore, entregue, o ponga a disposición de clientes o el público, deberá ser:

a) Expresada en términos acorde a las características y condiciones de quien la recibe, empleando un lenguaje sencillo y evitando tecnicismos, salvo en los casos en que resulte estrictamente necesario, debiendo explicarlos claramente. Deberá tener especial consideración con las personas en situación de discapacidad como, por ejemplo, visual o auditiva, de manera que la información se les entregue o ponga a disposición de una forma que resulte acorde a su situación de discapacidad.

b) Comunicada mediante herramientas, formatos, recursos o medios interactivos y didácticos que faciliten su comprensión. Además, deberá comunicar la información relevante mediante la modalidad de preguntas y respuestas.

c) Perfeccionada sobre la base del análisis que se realice al menos anualmente por la propia entidad o un externo para determinar, entre otras materias, si la información puesta a disposición está siendo leída y comprendida por quienes la recibieron.

d) Comunicada de manera oportuna y mediante canales o medios idóneos para informar al cliente y público en general.

Quienes presten los servicios de asesoría de inversión, asesoría crediticia, plataforma de financiamiento colectivo y sistema alternativo de transacción exclusivamente a inversionistas calificados a los que se refiere la letra f) del artículo 4 Bis de la Ley N°18.045 quedarán exceptuados de todas las exigencias de esta Sección III.

A. ASESORÍA DE INVERSIÓN

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe el asesor, esto es, señalar si cobra una comisión fija o variable a clientes; recibe una retribución de quienes emiten, intermedian, canalizan o colocan los instrumentos adquiridos o mantenidos por los clientes del asesor; o recibe una retribución por referir clientes a otro prestador de servicios; entre otros.

b) Descripción del modelo de asesoría utilizado, esto es, si la recomendación emana de personas, algoritmos informáticos o una combinación de ambos; y, en términos generales, sobre la base de qué elementos se efectúa la recomendación, por ejemplo, si emana de un análisis fundamental que toma como base los estados financieros o situación financiera, o si es un tipo de análisis técnico o estadístico sobre la base del comportamiento histórico del instrumento, o del juicio experto de un individuo, entre otros. En la descripción del modelo la entidad deberá evitar generar percepciones erradas en el público respecto al grado de sofisticación del algoritmo informático utilizado. Por ejemplo, que la recomendación emane de operaciones matemáticas y lógicas simples realizadas en una planilla de cálculo, no debe presentarse como que emana de un algoritmo informático.

c) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos, y cómo los gestiona.

d) En caso que hubiere difundido precios objetivo o recomendaciones para comprar, enajenar o mantener valores, instrumentos financieros o proyectos de inversión a personas indeterminadas en los últimos 3 meses, describir brevemente la recomendación efectuada y su resultado, esto es, si se alcanzó dicho precio en el período respectivo o si, para dicho período, de haberse realizado una operación en línea con la recomendación se habría generado una ganancia o no para aquel cliente que hubiere seguido tal recomendación. Para efectos de la fiscalización de esta obligación, la entidad deberá mantener un registro de las recomendaciones a personas indeterminadas dejando constancia de la recomendación y la fecha en que fue difundida.

Al momento de efectuar la recomendación, deberá entregar al cliente la siguiente información:

a) Las principales características financieras, económicas, tributarias y jurídicas del instrumento financiero recomendado, poniendo especial énfasis en los riesgos que conllevan la inversión en ese instrumento y cómo esas características se adecúan a las necesidades del cliente.

b) Los conflictos de intereses que se susciten entre el prestador del servicio y el cliente en particular, cómo se gestionarán y cómo pueden afectar al cliente si no se resolvieren adecuadamente.

No será necesario entregar la información a que se refieren las letras a) y b) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, y de Inversionista Calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

B. ASESORÍA CREDITICIA

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe el asesor, esto es, señalar si cobra una comisión fija o variable a clientes; recibe una retribución por referir clientes a otro prestador de servicios; o recibe una retribución por el monto del crédito colocado; entre otros.

b) Descripción del modelo de asesoría utilizado, esto es, si la evaluación emana de personas, algoritmos informáticos o una combinación de ambos; y, en términos generales, sobre la base de qué elementos se efectúa la evaluación, por ejemplo, si emana de un análisis fundamental que toma como base los estados financieros o situación financiera, o si es un tipo de análisis técnico o estadístico sobre la base del comportamiento histórico de la persona o entidad evaluada, o del juicio experto de un individuo, entre otros. En la descripción del modelo la entidad deberá evitar generar percepciones erradas en el público respecto al grado de sofisticación del algoritmo informático utilizado. Por ejemplo, que la recomendación emane de operaciones matemáticas y lógicas simples realizadas en una planilla de cálculo, no debe presentarse como que emana de un algoritmo informático.

c) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos, y cómo los gestiona.

Al momento de efectuar la evaluación, deberá entregar al cliente la siguiente información:

a) Si quien solicita la evaluación crediticia es la propia persona natural que requiere el financiamiento, el asesor crediticio deberá informar a esa persona respecto de las consecuencias económicas, financieras y jurídicas que tiene el sobre endeudamiento.

b) Los conflictos de intereses que se susciten entre el prestador del servicio y el cliente en particular y cómo pueden afectar al cliente si no se resolvieren adecuadamente.

No será necesario entregar la información a que se refieren las letras a) y b) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, y de Inversionista Calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

C. PLATAFORMA DE FINANCIAMIENTO COLECTIVO

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe la plataforma, esto es, señalar si cobra una comisión o remuneración a quienes financian, a quienes obtienen financiamiento, o a ambos, y el método de determinación de esa comisión o remuneración.

b) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos y cómo se gestionan.

c) Descripción de los mecanismos que la plataforma ha establecido para prevenir que mediante ella se financien proyectos fraudulentos, lavado de activos, financiamiento del terrorismo, la proliferación de armas de destrucción masiva o la comisión de otro tipo de ilícitos.

d) Descripción de los mecanismos que la plataforma ha establecido para acotar o ajustar el grado de exposición al riesgo que tienen en los proyectos quienes entregan financiamiento a través de ella, conforme a las expectativas o necesidades por ellos manifestadas.

e) Descripción de los procesos que la plataforma ha establecido para analizar la viabilidad económica, financiera y jurídica de los proyectos o de quienes obtienen financiamiento por su intermedio, especificando el límite al que se refiere el literal e) de la letra C de la Sección II anterior, o bien, las circunstancias o parámetros específicos por las cuales se han eximido de los procesos mencionados.

Al momento de difundir un proyecto o necesidad de financiamiento en particular, deberá entregar a los clientes que potencialmente realizarán el financiamiento, la siguiente información:

a) Información sobre quien tiene el proyecto de inversión o necesidad de financiamiento y cómo el cliente podría contactarle si así lo requiriera.

   1) Tratándose de personas naturales, los datos de identificación de las mismas y los antecedentes que resulten relevantes para comprender su capacidad para gestionar el proyecto de inversión o cumplir con las obligaciones que contrajere con el financiamiento que obtenga para la necesidad de financiamiento respectiva.

   2) Tratándose de personas jurídicas, se deberá entregar su identificación, sus socios y representante legal; una breve reseña de la historia de la entidad, señalando cuál es su objeto social y los hitos más relevantes desde su fundación a la fecha. Junto con lo anterior deberá proveer una descripción sobre la conformación del equipo de administración de la entidad, ya sea un directorio u órgano equivalente y ejecutivos principales, suficiente al menos para que se identifique a cada uno de sus integrantes y el rol que les corresponde dentro de la organización. Deberá también referirse a los productos y servicios que desarrolla en la actualidad y, en tal contexto, proveer una descripción de él o los sectores industriales o económicos en que se

desarrollan, incluyendo, en caso de que corresponda, una referencia al marco legal o normativo que regule o que afecte la industria en la cual participa.

b) Una explicación sobre el uso que se dará a los recursos que se obtengan con el financiamiento, incluyendo el monto que se espera recaudar y el monto total de recursos que se destinarán al mismo objetivo, esto es, si el financiamiento obtenido a través de la plataforma será complementado con otros recursos, señalando de donde provienen los mismos.

c) Indicadores y controles que se generarán para que los financistas puedan monitorear y verificar el desarrollo del proyecto y, cuando corresponda, el pago de la deuda conforme a lo planificado.

d) Descripción de la naturaleza jurídica del instrumento a través del cual se concretará el financiamiento, esto es, si es mediante acciones de sociedades anónimas o de sociedades por acciones, títulos de crédito, cuotas de fondos o comunidades, contratos de mutuo, criptoactivos, etc. Se deberá hacer especial énfasis en los derechos, preferencias, obligaciones, formas de ejercer derechos societarios, tecnología y protocolos de soporte, y riesgos asociados al mismo, especificando si se adquieren obligaciones civiles o naturales.

e) Una explicación de cómo se procederá al momento de cerrar la ronda de financiamiento, ya sea en el caso que se complete el financiamiento solicitado o no, indicando cómo se deberá proceder para materializar el aporte y la contraprestación al financiamiento. Por ejemplo, si el financista quedará en contacto directo con quien tiene el proyecto o necesidad de financiamiento, o si deberá entregar a un tercero.

f) Nivel recomendado de exposición al riesgo de financiamiento, esto es, para qué tipos de necesidades de riesgo-retorno-horizonte de inversión el proyecto es aconsejable.

D. SISTEMA ALTERNATIVO DE TRANSACCIÓN

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Reglamentación interna a que se refiere el literal g) de la Sección II.D.

b) Descripción general de la estructura de comisiones o remuneraciones que recibe el sistema, esto es, señalar si cobra una comisión o remuneración fija o variable, el monto o porcentaje, y la forma de su determinación.

c) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos y cómo se gestionan.

d) Descripción de las normas de admisión de los instrumentos financieros, destacando los mecanismos establecidos para prevenir que en el sistema se negocien instrumentos financieros que resulten o tengan un fin fraudulento.

e) Descripción de las principales características de los instrumentos admitidos a cotización, así como el nivel recomendado de exposición al riesgo, esto es, para qué tipos de necesidades de riesgo-retorno-horizonte de inversión el instrumento es aconsejable. Tratándose de activos virtuales, además se deberá facilitar el acceso al documento público que se hubiere elaborado para referirse a las especificaciones técnicas respecto de la tecnología y aspectos relevantes que subyacen al instrumento.

f) Precios de cotización, unidades y montos por transacción, con un desfase inferior a los 5 minutos de efectuada la cotización o negociación.

g) Precios de cierre, unidades y montos totales diarios negociados de cada instrumento, al cierre del día o a las 00:00 del día siguiente si el sistema no tuviere horario de cierre.

h) Identificación de los instrumentos que hubieren sido cancelados o suspendidos de negociación y las razones de aquello, conforme a las reglas establecidas para esos efectos.

i) Descripción de las políticas de gestión de riesgo operacional y los niveles de servicio comprometidos en cuanto a disponibilidad, desempeño y continuidad, así como la forma y oportunidad en que serán informados los incidentes que comprometan la disponibilidad y seguridad de la información. A su vez, la forma en que se procederá en caso de que aquéllos se produzcan para las entidades del Bloque 3 de acuerdo con la Sección IV.C.

La siguiente información deberá ser puesta a disposición del cliente al momento de la negociación:

a) Condiciones pactadas en la negociación, esto es, instrumento, contraparte, precio, unidades y monto, con indicación clara de la moneda en la que se acordaron esas condiciones.

b) Condiciones, fecha y procedimiento de liquidación de las operaciones y, en caso de que los instrumentos negociados queden en custodia, ese hecho junto a la identificación de la entidad encargada de la misma.

No será necesario entregar la información a que se refieren las letras a) y b) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, y de Inversionista Calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

E. ENRUTAMIENTO DE ÓRDENES

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe el enrutador, esto es, señalar si cobra a los clientes por canalizar órdenes o percibe una retribución del intermediario o sistema al que canaliza la orden, o del colocador o emisor de los instrumentos objeto de la orden; y si esa comisión o remuneración es fija o variable, el monto o porcentaje, y la forma de su determinación.

b) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos y cómo los gestiona.

c) Descripción de las políticas de gestión de riesgo operacional y los niveles de servicio comprometidos en cuanto a disponibilidad, desempeño y continuidad.

d) Forma y oportunidad en que serán informados los incidentes que comprometan la disponibilidad y seguridad de la información.

e) Identificación de las garantías que la entidad haya constituido para indemnizar los perjuicios que se puedan producir a clientes, así como la descripción de la forma o mecanismos de ejecución y asignación de esas garantías.

La siguiente información deberá ser puesta a disposición del cliente al momento de, o previo a, canalizar la orden:

a) El hecho de que se recibió y canalizó la orden, así como la confirmación de su recepción y eventual ejecución por parte del intermediario, sistema alternativo o tercero al que se hubiere derivado esa orden.

b) Los conflictos de intereses que se susciten entre el prestador del servicio y el cliente en particular y cómo pueden afectar al cliente si no se resolvieren adecuadamente.

No será necesario entregar la información a que se refieren las letras a) y b) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, y de Inversionista Calificado, de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

F. INTERMEDIACIÓN DE INSTRUMENTOS FINANCIEROS

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe la entidad, esto es, señalar si cobra a los clientes por ejecutar órdenes; si percibe una retribución del emisor de los instrumentos objeto de la orden o de terceros; y si esa comisión o remuneración es fija o variable, el monto o porcentaje, y la forma de su determinación.

b) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos y cómo los gestiona.

c) Descripción de las políticas de gestión de riesgo operacional y los niveles de servicio comprometidos en cuanto a disponibilidad, desempeño y continuidad.

d) Forma y oportunidad en que serán informados los incidentes que comprometan la disponibilidad y seguridad de la información.

e) Identificación de las garantías que la entidad haya constituido para indemnizar los perjuicios que se puedan producir a clientes, así como la descripción de la forma o mecanismos de ejecución y asignación de esas garantías.

f) Descripción de las principales políticas, procedimientos, mecanismos y controles que ha implementado la entidad con el objeto de preservar su solvencia y liquidez.

g) Situaciones que están pendientes de resolución y que pueden comprometer de manera relevante su solvencia, liquidez o capacidad de cumplir sus obligaciones.

La siguiente información deberá ser puesta a disposición del cliente al momento de, o previo a, recibir y ejecutar la orden:

a) El hecho de que se recibió y ejecutó la orden, así como las condiciones en las que fue ejecutada.

b) Los conflictos de intereses que se susciten entre el prestador del servicio y el cliente en particular, cómo se gestionarán y cómo pueden afectar al cliente si no se resolvieren adecuadamente.

c) Cualquier situación material que esté en conocimiento de la entidad que diga relación con el instrumento objeto de la orden y que, para una persona con conocimientos económicos financieros promedio, sea relevante para sus decisiones de inversión.

No será necesario entregar la información a que se refieren las letras b) y c) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, y de Inversionista Calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

G. CUSTODIA DE INSTRUMENTOS FINANCIEROS

La siguiente información deberá ser puesta a disposición del público en todo momento, debidamente actualizada:

a) Descripción general de la estructura de comisiones o remuneraciones que recibe la entidad, esto es, señalar si cobra a los clientes por almacenar claves, documentación o instrumentos; si esa retribución es fija o variable, y el monto o porcentaje, y la forma de su determinación.

b) La existencia de conflictos de intereses que emanen del modelo de negocios o sus fuentes de ingresos y cómo los gestiona.

c) Descripción de las políticas de gestión de riesgo operacional y los niveles de servicio comprometidos en cuanto a disponibilidad, desempeño y continuidad.

d) Forma y oportunidad en que serán informados los incidentes que comprometan la disponibilidad y seguridad de la información.

e) Identificación de las garantías que la entidad haya constituido para indemnizar los perjuicios que se puedan producir a clientes, así como la descripción de la forma o mecanismos de ejecución y asignación de esas garantías.

f) Situaciones que están pendientes de resolución y que pueden comprometer de manera relevante su solvencia, liquidez o capacidad de cumplir sus obligaciones.

La siguiente información deberá ser puesta a disposición del cliente al momento de, o previo a, recibir los instrumentos en custodia:

a) El hecho de que se recibió el instrumento en custodia.

b) Los conflictos de intereses que se susciten entre el prestador del servicio y el cliente en particular y cómo pueden afectar al cliente si no se resolvieren adecuadamente.

c) Cualquier situación que pueda afectar de manera material la capacidad de la entidad de resguardar adecuadamente los instrumentos en custodia o de restituirlos a sus dueños.

d) Cualquier situación material que esté en conocimiento de la entidad que diga relación con los instrumentos en custodia y que sea relevante para que el cliente pueda resguardar adecuadamente sus intereses.

e) Si la entidad quedará o no a cargo de ejercer los derechos societarios inherentes a los instrumentos financieros y, en caso afirmativo, las políticas de ejercicio de tales derechos.

No será necesario entregar la información a que se refieren las letras b) a la e) del párrafo anterior, en caso de clientes que tengan la calidad de Inversionista Institucional, o de Inversionista Calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

IV. GOBIERNO CORPORATIVO Y GESTIÓN DE RIESGOS

Las disposiciones expuestas en la presente sección deben observarse de manera proporcional, atendiendo a la naturaleza de la entidad, su modelo de negocios y estructura organizacional; de manera de compatibilizar la capacidad de contar con respuestas estratégicas idóneas para los riesgos inherentes a las líneas de negocios, con la viabilidad económica y financiera de la entidad.

En caso de prestar más de un servicio de los regulados por el Título II de la ley N° 21.521, la entidad deberá cumplir los requisitos de gobierno corporativo y gestión de riesgos aplicables a cada uno de ellos. Las políticas que la entidad deba establecer en virtud de esta sección podrán estar contenidas en un mismo documento o manual. Asimismo, la entidad deberá establecer los procedimientos para la implementación de las políticas definidas y aprobadas por el directorio.

Sin perjuicio de lo anterior, todas las entidades objeto de la presente normativa no podrán exceptuarse del cumplimiento de las obligaciones que en materia de datos personales establece la ley N° 21.521.

A. ASESORÍA DE INVERSIÓN

A.1. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El Directorio u órgano equivalente de la entidad es la instancia responsable de aprobar y autorizar las políticas de gestión de riesgos y control interno, como mínimo una vez al año o con la frecuencia necesaria en caso de que se produzcan cambios significativos en las políticas establecidas, dejando evidencia de ello. Para esos efectos, el directorio u órgano equivalente deberá dar cumplimiento a los requisitos de gestión de riesgos que se señalan a continuación:

a) Establecer la misión, visión y objetivos estratégicos, teniendo en consideración las responsabilidades que el marco regulatorio vigente establece para la entidad.

b) Aprobar políticas de gestión de riesgos que sean coherentes con los objetivos estratégicos y el marco regulatorio.

c) Evaluar periódicamente la suficiencia de recursos de las instancias encargadas de la gestión de riesgos.

d) Aprobar el código de conducta, que dé cuenta de los valores y principios organizacionales y establezca directrices en el actuar del personal de la entidad.

e) Establecer una estructura organizacional adecuada para la gestión de riesgos de la entidad, que considere lo siguiente:

   1) La administración y el control de todos los riesgos pertinentes derivados del desarrollo de sus actividades. En ese tenor, la estructura organizacional debe ser la adecuada en relación con el volumen de negocios; el número y tipo de clientes de la entidad; la complejidad de las relaciones con otras entidades, entre otros aspectos.

   2) La definición de los roles, competencias y responsabilidades que permitan realizar sus actividades y gestionar adecuadamente los riesgos que enfrenta la entidad. Lo anterior involucra la segregación apropiada de los deberes y las funciones

claves, especialmente aquéllas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad o sus participantes a riesgos indebidos; y entre las áreas generadoras de riesgo y de control de los mismos.

3) La implementación de la función de gestión de riesgos, de conformidad con lo descrito en el literal A.3. de esta Sección.

f) Establecer políticas de contratación de empleados que aseguren que la entidad disponga de personal con la debida experiencia para desempeñar sus funciones, y velar porque se cuente con el recurso humano calificado para la gestión de riesgos. En el caso del personal que efectúe asesorías a los clientes, deberá cumplir con lo establecido en los requisitos de autorización para la prestación de servicios.

g) Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.

h) El directorio u órgano equivalente deberá evaluar la pertinencia de conformar un Comité de Gestión de Riesgos o una instancia similar que le permitan tratar y monitorear aspectos relevantes de los negocios, referidos a materias tales como conflictos de intereses, seguridad de la información, entre otros. Los fundamentos considerados por el directorio u órgano equivalente para evaluar la conformación de comités o instancias similares deberán estar debidamente documentados.

i) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio u órgano equivalente y los comités, así como las políticas mencionadas previamente. Todo el material que se elabore o presente al directorio u órgano equivalente o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.

A.2. POLÍTICAS Y PROCEDIMIENTOS

Las entidades deberán elaborar y poner en práctica de manera formal, políticas y procedimientos de gestión de riesgos y control interno que contemplen los riesgos asociados a la asesoría de inversión.

La función de gestión de riesgos será la responsable de asegurar la elaboración de la totalidad de las políticas y los procedimientos por parte de los encargados de las distintas áreas generadoras de riesgos; y de la exactitud, integridad y actualización de tales políticas y procedimientos.

Las políticas y procedimientos establecidas deberán cumplir con los siguientes aspectos generales:

a) Deberán guardar relación con el número o tipo de clientes, y al volumen de operaciones efectuadas, y respecto de cada uno de los negocios o actividades que se desarrolle.

b) Las políticas deberán exponer los principios generales y directrices establecidas por el directorio u órgano equivalente para orientar las actividades de la organización.

c) Los procedimientos deberán definir cómo llevar a cabo un proceso, con el fin de asegurar el cumplimiento de las políticas aprobadas por el directorio incorporando, al menos: la descripción de las actividades principales que lo componen y la identificación de sus responsables; determinación de los responsables de supervisar y controlar el resultado de las actividades ejecutadas; documentación que evidencie la ejecución de las actividades que conforman los procedimientos; definición y descripción de los controles asociados a dichas actividades. En el caso de actividades externalizadas, siempre deberá existir una persona responsable dentro de la organización respecto al control de estas.

d) Las políticas, procedimientos y mecanismos de control deberán estar formalmente establecidos y documentados.

A.2.1. POLÍTICAS Y PROCEDIMIENTOS DE GESTIÓN DE RIESGOS Y CONTROL INTERNO

Sin perjuicio de lo anterior, las políticas y procedimientos deberán abordar como mínimo los siguientes aspectos:

a) Conflictos de intereses

Las entidades deberán definir políticas y procedimientos que especifiquen los métodos según los cuales se identificarán, manejarán y vigilarán todos los potenciales conflictos de intereses inherentes a los servicios ofrecidos por ella. Las políticas y procedimientos deberán considerar la identificación, la prevención y monitoreo de los conflictos que puedan surgir entre el servicio de asesoría de inversión y sus clientes, así como de otros productos ofrecidos por la entidad, según le permita la legislación y normativa vigente.

b) Confidencialidad de la información

Las entidades deberán definir políticas y procedimientos destinados a resguardar la naturaleza confidencial de la información entregada por sus clientes para efectos del servicio de asesoría de inversión, debiendo cumplir con todas las disposiciones legales al efecto, en particular, aquellas que establece la ley N°19.628 sobre protección de la vida privada.

Las políticas y procedimientos deberán incluir el consentimiento para el uso de la información por parte de los clientes, de acuerdo con la ley N°19.628 sobre protección de la vida privada, asegurando la protección de los datos contra el acceso y la divulgación no autorizados y los medios para proteger la privacidad personal y la información reservada.

c) Oferta de productos acorde a las necesidades, expectativas y disposición al riesgo del inversionista

Las entidades deberán definir políticas y procedimientos tendientes a que los inversionistas inviertan sus recursos en instrumentos financieros, conociendo la información que les permita entender y aceptar el riesgo que están asumiendo, y a evitar ofrecer productos que no sean acordes a sus las necesidades, expectativas y

disposición al riesgo de los inversionistas, según lo dispuesto en el artículo 28 de la ley N°21.521.

Las entidades deberán contar con procedimientos para asegurar el cumplimiento de la citada obligación. En aquellos casos en que un cliente decida invertir en un instrumento financiero que, en opinión de la entidad, no es acorde a las necesidades, expectativas o riesgos que este le ha comunicado la entidad deberá poder acreditar que aquello fue debidamente advertido, en caso de que le sea solicitado por la Comisión. Para estos efectos, los procedimientos podrán considerar el requerir a sus potenciales clientes antecedentes tales como información sobre sus conocimientos y experiencia como inversionista, su situación financiera, y objetivos de inversión o ahorro, y otra información de esta naturaleza que la entidad considere relevante.

La entidad podrá establecer excepciones en esta política, en caso de que la oferta de productos esté dirigida a clientes que tengan la calidad de inversionista institucional o inversionista calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

d) Información al inversionista

La entidad deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los productos o servicios ofrecidos, según lo dispuesto en el artículo 28 de la ley N°21.521.

Estas políticas deberán especificar, al menos, la información que debe ser conocida por los clientes de acuerdo con la Sección III de esta normativa, y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad controlará el cumplimiento de estas disposiciones.

e) Metodología de aprobación, evaluación y control de algoritmos

En caso de corresponder, las entidades deberán contar con políticas y procedimientos de aprobación, evaluación y control de algoritmos que garanticen su adecuado funcionamiento al otorgar el servicio de asesoría de inversión. Estas políticas y procedimientos deberán velar porque los algoritmos empleados garanticen que las asesorías se realicen en el interés y la protección de los clientes, acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.

Las entidades deberán contar con personal capacitado que comprenda el funcionamiento de los algoritmos y la verificación continua de su correcto funcionamiento de sus algoritmos, incluyendo lo establecido en la letra d) de la Sección II.A de esta normativa.

f) Cumplimiento de requisitos legales y normativos de funcionamiento

Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.

Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a esta Comisión.

A.2.2. RIESGO OPERACIONAL: SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Sin perjuicio de las políticas y procedimientos mínimos que deban implementar las entidades en virtud de la sección anterior, éstas deberán observar los siguientes lineamientos en términos de seguridad de la información y ciberseguridad. Resulta relevante destacar que las entidades deberán adaptar estas exigencias considerando especialmente su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) La capacitación periódica del personal en la materia, de manera que sea consciente de los riesgos de seguridad de la información y ciberseguridad y contribuya a una adecuada gestión de éstos.

b) Resguardo de la información de sus clientes:

   1) Implementar un inventario de los activos de información, incluyendo una clasificación de estos. Esta clasificación deberá considerar dimensiones tales como disponibilidad, confidencialidad e integridad de los activos de información.

   2) Implementar un inventario de servicios relacionados con los activos de información.

   3) Implementar controles de acceso a las instalaciones, infraestructuras de negocios y sistemas de información.

   4) Implementar herramientas de registro, control y monitoreo de la actividad de los usuarios de sistemas.

c) Implementar controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por el personal, y herramientas de gestión de la ciberseguridad como, por ejemplo, programas de gestión de parches de software y firmware, protección de redes ante ataques por medio de firewalls, sistemas de prevención de intrusos, elevación de privilegios, gestión de identidades y acceso físico y lógico, mecanismos de control de identidad para evitar suplantación de terceros entre otras.

d) Gestionar las condiciones ambientales para la localización segura de los equipos y herramientas de la entidad.

e) Procedimientos de identificación de amenazas de ciberseguridad tales como phishing, malware, inyección de código malicioso, entre otros.

A.3. GESTIÓN DE RIESGOS

A.3.1. FUNCIÓN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos es la instancia responsable del monitoreo de los controles definidos en las políticas y los procedimientos de gestión de riesgos y control interno de la entidad. Esta función deberá reportar directamente al directorio u órgano equivalente.

De acuerdo con el literal A.4. de esta Sección, la función de gestión de riesgos podrá ser realizada por una persona o unidad interna o, en ciertos casos, por la alta administración de la entidad. Si la función es ejercida por una unidad de gestión de riesgos corporativa en caso de que la entidad pertenezca a un grupo empresarial, se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, la entidad será siempre responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Asimismo, la función de gestión de riesgos será responsable de la realización de actividades para monitorear el cumplimiento de las políticas definidas por la entidad.

Con objeto de implementar lo anteriormente señalado, la función de gestión de riesgos deberá:

a) Verificar la existencia de las políticas y procedimientos mínimos descritos en el literal A.2 anterior.

b) Emitir un informe, al menos con una periodicidad semestral, al directorio u órgano equivalente para documentar las instancias de incumplimientos detectados, causas que los originaron, medidas adoptadas y efectividad de dichas medidas.

c) Proponer cambios en las políticas y en los procedimientos de gestión de riesgos en función de las deficiencias encontradas en sus actividades de control.

d) Elaborar un plan anual que se refiera a la naturaleza, el alcance y oportunidad de las actividades que la función de gestión de riesgos desarrollará. Este plan deberá ser aprobado por el directorio u órgano equivalente. En todo caso, dicho plan deberá ser actualizado cada vez que se produzcan cambios significativos tales como cambios en condiciones del entorno económico y mercados en que opera la entidad, introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la entidad.

A.3.2. PLAN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos estará a cargo de la elaboración de un plan de gestión de riesgos que incluirá las estrategias de mitigación de riesgos y la planificación de contingencias en relación con los principales riesgos, los que, como mínimo deben contemplar los riesgos provenientes de conflictos de intereses y los riesgos de seguridad de la información y ciberseguridad.

El directorio u órgano equivalente deberá aprobar el plan de gestión de riesgos al menos anualmente, con el fin de reflejar cambios significativos experimentados en la estrategia de negocios de la entidad o cambios en las condiciones de mercado. La función

de gestión de riesgos controlará que se dé cumplimiento al plan de gestión de riesgos y a sus respectivos procedimientos.

La elaboración de estrategias de mitigación de riesgos y planificación de contingencias considerará lo siguiente:

a) Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad, y los respectivos responsables de dichos procesos (mapa de procesos).

   La función de gestión de riesgos, en conjunto con los encargados de los procesos principales, deberá identificar formalmente los riesgos inherentes a los que se expone la entidad en el desarrollo de sus actividades.

b) Medición de los riesgos inherentes identificados en las actividades efectuadas por la entidad.

c) Definición de los mecanismos de control para mitigar los riesgos inherentes identificados. Al respecto, dichos mecanismos de control deberán considerar:

   1) Descripción de cada control y su objetivo.

   2) Identificación de los responsables del control formalmente designados para esos efectos.

   3) Calificación de la efectividad de los controles para la mitigación de los riesgos inherentes, por una instancia independiente del responsable de los mismos.

d) Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al directorio u órgano equivalente y a todas las partes interesadas.

e) Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos y financieros que vaya enfrentando la entidad, cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales.

A.4. PROPORCIONALIDAD

En línea con lo establecido en los artículos 1 y 12 de la ley N°21.521, las entidades podrán adaptar las disposiciones de esta Sección IV.A, conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos.

Sin perjuicio de lo anterior, la Tabla 1 describe los requisitos proporcionales que deberán cumplir las entidades que presten el servicio de asesoría de inversión.

La proporcionalidad se aplicará dependiendo de si los asesores de inversión son personas naturales o jurídicas; si hacen uso de información que califique como datos de carácter personal, en conformidad a la ley N°19.628, para las recomendaciones de inversión; y en función de si tienen menos o más de 100 clientes activos en Chile.

Tabla 1. Proporcionalidad para la prestación del servicio de asesoría de inversión

<table>
<tr><th colspan="3">Características del prestador de asesoría de inversión</th><th>Políticas</th><th>Función de gestión de riesgos</th></tr>
<tr><td rowspan="3">Personas Naturales</td><td colspan="2">No realiza tratamiento de datos personales</td><td colspan="2">Se exime de todos los requisitos de esta Sección IV.A</td></tr>
<tr><td rowspan="2">Realiza tratamiento de datos personales</td><td>Menos de 100 clientes activos</td><td colspan="2">Se exime de todos los requisitos de esta Sección IV.A</td></tr>
<tr><td>100 o más clientes activos</td><td>CI, CINF, OP, II</td><td>No especializada</td></tr>
<tr><td rowspan="4">Personas Jurídicas</td><td rowspan="2">No realiza tratamiento de datos personales</td><td>Menos de 100 clientes activos</td><td colspan="2">Se exime de todos los requisitos de esta Sección IV.A</td></tr>
<tr><td>100 o más clientes activos</td><td>CI, OP, II</td><td>No especializada</td></tr>
<tr><td rowspan="2">Realiza tratamiento de datos personales</td><td>Menos de 100 clientes activos</td><td colspan="2">Se exime de todos los requisitos de esta Sección IV.A</td></tr>
<tr><td>100 o más clientes activos</td><td>CI, CINF, OP, II, ALG, RLN, RO.</td><td>Especializada</td></tr>
</table>

Donde,

a) CI: Conflictos de intereses.

b) CINF: Confidencialidad de la información.

c) OP: Oferta de productos acorde a las necesidades, expectativas y disposición al riesgo del inversionista.

d) II: Información al inversionista.

e) ALG: Metodología de aprobación, evaluación y control de algoritmos.

f) RLN: Cumplimiento de requisitos legales y normativos de funcionamiento.

g) RO: Riesgo operacional.

h) No especializada: La función de gestión de riesgos podrá ser ejercida por algún integrante de la alta administración de la entidad.

i) Tratamiento de datos personales: Datos personales en el sentido de la ley N°19.628 y utilizados para efectuar las recomendaciones de inversión.

En el caso de entidades cuyo requisito sea que la función de gestión de riesgos sea especializada, esta función no podrá ser ejercida por la alta administración, debiendo reportar directamente al directorio u órgano equivalente.

Cuando una entidad alcance los 100 clientes activos en Chile, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de gobierno corporativo y gestión integral de riesgos correspondientes. Una vez alcanzado ese número, las entidades deberán cumplir con las exigencias de gobierno corporativo y gestión integral de riesgos. Para volver a estar exentas de los requerimientos, las entidades deberán mantenerse por más de 6 meses bajo el umbral de clientes señalado y solicitar autorización de la Comisión.

A.5. INFORMACIÓN DE INCIDENTES OPERACIONALES

Las entidades de asesoría de inversión que realicen tratamiento de datos personales en los términos señalados, y tengan más de 100 clientes activos en Chile deberán comunicar a esta Comisión los incidentes operacionales que afecten la información de la entidad o los datos personales de sus clientes, tales como, problemas tecnológicos que afecten la seguridad de la información; virus o malware detectados en los activos de información críticos; pérdidas o fugas de información de la entidad o sus clientes, entre otros.

Para estos efectos, las entidades deberán usar el formato del Reporte de Incidentes Operacionales (RIO) del Anexo N°2 de esta normativa, y dispondrán de un plazo de 2 horas transcurridas desde que la entidad tomó conocimiento del hecho. El plazo señalado es solo para efectos de notificar a la Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados la CMF, posteriormente.

El directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información de incidentes operacionales, así como para mantener informado en forma oportuna al directorio u órgano equivalente respecto al incidente y las medidas adoptadas para resolverlo.

B. ASESORÍA CREDITICIA

B.1. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El Directorio u órgano equivalente de la entidad es la instancia responsable de aprobar y autorizar las políticas de gestión de riesgos y control interno, como mínimo una vez al año o con la frecuencia necesaria en caso de que se produzcan cambios significativos en las políticas establecidas, dejando evidencia de ello. Para esos efectos, el directorio u órgano equivalente deberá dar cumplimiento a los requisitos de gestión de riesgos que se señalan a continuación:

a) Establecer la misión, visión y objetivos estratégicos, teniendo en consideración las responsabilidades que el marco regulatorio vigente establece para la entidad.

b) Aprobar los niveles de apetito por riesgo, verificando que aquellas definiciones permitan a la entidad cumplir con sus obligaciones legales, objetivos estratégicos y ser sostenible en el tiempo.

c) Aprobar políticas de gestión de riesgos que sean coherentes con los objetivos estratégicos, el marco regulatorio, los valores organizacionales y los niveles de apetito por riesgo definidos, estableciendo un proceso adecuado de difusión de una cultura de gestión de riesgos en toda la organización.

d) Revisar las políticas, al menos anualmente, y actualizarlas en caso de que se produzcan cambios significativos tales como introducción de nuevos servicios, o cambios en la regulación aplicable a la entidad.

e) Aprobar el código de conducta, que dé cuenta de los valores y principios organizacionales y establezca directrices en el actuar del personal de la entidad.

f) Aprobar los planes de la función de gestión de riesgos y la función de auditoría interna. Asimismo, tomar conocimiento de los reportes emitidos por los encargados de dichas funciones en forma oportuna.

g) Evaluar periódicamente la suficiencia de recursos de las instancias encargadas de la gestión de riesgos y auditoría interna para efectuar sus labores, para lo cual deberá tener en consideración la cobertura del trabajo de dichas funciones, aprobando la asignación de los recursos necesarios para dichas unidades y monitoreando el grado de cumplimiento del presupuesto asignado a tal fin.

h) Disponer de sistemas de tecnología e información adecuados que apoyen el desarrollo de las actividades de la entidad, y que a su vez permitan la continuidad de la implementación de las políticas y los procedimientos de gestión de riesgos y control interno.

i) Establecer una estructura organizacional adecuada para la gestión de riesgos de la entidad, que considere lo siguiente:

    1) La administración y el control de todos los riesgos pertinentes derivados del desarrollo de sus actividades. En ese tenor, la estructura organizacional debe ser la adecuada en relación con el volumen de negocios; el número y tipo de clientes de la entidad; y la complejidad de las relaciones con otras entidades.

2) La definición de los roles, competencias y responsabilidades que permitan realizar sus actividades y gestionar adecuadamente los riesgos que enfrenta la entidad. Lo anterior involucra la segregación apropiada de los deberes y las funciones claves, especialmente aquéllas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad o sus participantes a riesgos indebidos; y entre las áreas generadoras de riesgo y de control de estos.

3) La implementación de la función de gestión de riesgo, de conformidad con lo descrito en el literal B.3.1 de esta Sección.

4) La implementación de la función de auditoría interna, de conformidad con lo descrito en el literal B.3.3 de esta Sección.

5) Que el directorio u órgano equivalente vele por el cumplimiento de la segregación de funciones y la independencia de las funciones de gestión de riesgos y de auditoría interna.

j) Establecer políticas de contratación de empleados que aseguren que la entidad disponga de personal con la debida experiencia para desempeñar sus funciones, y velar porque se cuente con el recurso humano calificado para la gestión de riesgos.

k) Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.

l) El directorio u órgano equivalente deberá evaluar la pertinencia de conformar un Comité de Gestión de Riesgos o una instancia similar que le permitan tratar y monitorear aspectos relevantes de los negocios, referidos a materias tales como auditoría, seguridad de la información, entre otros. Los fundamentos considerados por el directorio u órgano equivalente para evaluar la conformación de comités o instancias similares deberán están debidamente documentados.

   Sin perjuicio de ello, los siguientes comités, en caso de ser constituidos, deberán estar integrados al menos por un integrante del directorio u órgano equivalente: Comité de Gestión de Riesgos y Comité de Auditoría. Ningún director (o miembro del órgano equivalente) podrá ser parte del Comité de Gestión de Riesgos y de Auditoría al mismo tiempo.

m) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio u órgano equivalente y los comités. Todo el material que se elabore o presente al directorio u órgano equivalente o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.

B.2. POLÍTICAS, PROCEDIMIENTOS Y MECANISMOS DE CONTROL

Las entidades deberán elaborar y poner en práctica de manera formal, políticas y procedimientos de gestión de riesgos y control interno que contemplen los riesgos asociados a la asesoría crediticia. Tales políticas y procedimientos de gestión de riesgos y control interno tienen como propósito controlar con eficacia los riesgos a que se

enfrenta el negocio de la entidad, a la vez que contribuyen a que se minimicen los riesgos asociados a los objetivos de supervisión de esta Comisión.

La instancia encargada de la función de gestión de riesgos será la responsable de asegurar la elaboración de la totalidad de las políticas y los procedimientos por parte de los encargados de las distintas áreas generadoras de riesgos; y de la exactitud, integridad y actualización de tales políticas y procedimientos.

Las políticas y procedimientos establecidas deberán cumplir con los siguientes aspectos generales:

a) Deberán guardar relación con el número o tipo de clientes, y al volumen de operaciones efectuadas, y respecto de cada uno de los negocios o actividades que se desarrolle.

b) Las políticas deberán exponer los principios generales y directrices establecidas por el directorio u órgano equivalente para orientar las actividades de la organización.

c) Los procedimientos deberán definir cómo llevar a cabo un proceso, con el fin de asegurar el cumplimiento de las políticas aprobadas por el directorio, incorporando, al menos: la descripción de las actividades principales que lo componen y la identificación de sus responsables; determinación de los responsables de supervisar y controlar el resultado de las actividades ejecutadas; documentación que evidencie la ejecución de las actividades que conforman los procedimientos; definición y descripción de los controles asociados a dichas actividades. En el caso de actividades externalizadas, siempre deberá existir una persona responsable dentro de la organización respecto al control de estas.

d) Las políticas, procedimientos y mecanismos de control deberán estar formalmente establecidos y documentados, siendo consistentes con los niveles de apetito por riesgo que haya definido la entidad.

e) Las políticas y procedimientos de gestión de riesgo operacional deberán formar parte de las políticas y procedimientos de gestión de riesgos de la entidad, de acuerdo con el literal B.2.2 de esta Sección.

B.2.1. POLÍTICAS Y PROCEDIMIENTOS DE GESTIÓN DE RIESGOS Y CONTROL INTERNO

Sin perjuicio de lo anterior, las políticas y procedimientos deberán abordar como mínimo los siguientes aspectos:

a) Conflictos de intereses

Las entidades deberán definir políticas y procedimientos que especifiquen los métodos según los cuales se identificarán, manejarán y vigilarán todos los potenciales conflictos de intereses inherentes a los servicios ofrecidos por ella. Las políticas y procedimientos deberán considerar la identificación, la prevención y monitoreo de los conflictos que puedan surgir entre el servicio de asesoría crediticia y sus clientes, así como de otros servicios ofrecidos por la entidad según le permita la legislación y normativa vigente.

b) Confidencialidad de la información

Las entidades deberán definir políticas destinadas a resguardar la naturaleza confidencial de la información entregada por sus clientes para efectos del servicio de asesoría crediticia, debiendo cumplir con todas las disposiciones legales al efecto, en particular, aquellas que establece la ley N°19.628 sobre la protección de la vida privada.

Las políticas y procedimientos deberán incluir el consentimiento para el uso de la información por parte de los clientes, de acuerdo con la ley N°19.628 sobre protección de la vida privada, asegurando la protección de los datos contra el acceso y la divulgación no autorizados, y los medios para proteger la privacidad personal y la información reservada.

c) Gestión de consultas, reclamos y denuncias

Las entidades deberán definir políticas y procedimientos que les permitan gestionar y resolver las consultas, denuncias y reclamos de sus clientes, trabajadores y el público general. Para ello deberán considerar, al menos, un manual que establezca, en términos simples, los antecedentes mínimos que se requerirán para efectuar una consulta, denuncia o reclamo, y que describa cómo utilizar los canales especializados que se hubieren dispuesto para esos efectos.

d) Comercialización y publicidad

Las entidades deberán definir políticas y procedimientos que, además de cumplir las disposiciones legales, tengan como un objetivo que los servicios ofrecidos al cliente sean entendidos por él, en particular, en aspectos como los costos asociados y la finalidad del servicio de asesoría crediticia.

e) Información al cliente

La entidad deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los servicios ofrecidos, según lo dispuesto en el artículo 28 de la Ley N°21.521.

Estas políticas y procedimientos deberán especificar, al menos, la información que debe ser conocida por los clientes de acuerdo con la Sección III de esta normativa y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad controlará el cumplimiento de las políticas y procedimientos definidos.

f) Metodología de aprobación, evaluación y control de algoritmos

En caso de corresponder, las entidades deberán contar con políticas y procedimientos de aprobación, evaluación y control de algoritmos que garanticen su adecuado funcionamiento al otorgar el servicio de asesoría crediticia. Estas políticas y procedimientos deberán velar porque los algoritmos empleados garanticen que las asesorías se realicen en el interés y la protección de los clientes, acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.

Las políticas y procedimientos deben considerar, al menos, que la entidad cuente con personal capacitado que comprenda el funcionamiento de los algoritmos y la verificación continua del correcto funcionamiento de sus algoritmos.

g) Cumplimiento de requisitos legales y normativos de funcionamiento

Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.

Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a esta Comisión.

B.2.2. RIESGO OPERACIONAL

Sin perjuicio de las políticas y procedimientos mínimos que deban implementar las entidades en virtud de la sección anterior, éstas deberán observar los siguientes lineamientos en términos de seguridad de la información y ciberseguridad, adaptándolas en base a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) La capacitación del personal en la materia, de manera que sea consciente de los riesgos de seguridad de la información y ciberseguridad y contribuya a una adecuada gestión de éstos.

b) Resguardo de la información de sus clientes:

   1) Implementar un inventario de esos activos de información, incluyendo una clasificación de estos. Esta clasificación deberá considerar dimensiones tales como disponibilidad, confidencialidad e integridad de los activos de información.

   2) Implementar un inventario de servicios relacionados con los activos de información.

   3) Implementar controles de acceso a las instalaciones, infraestructuras de negocios y sistemas de información.

   4) Implementar herramientas de registro, control y monitoreo de la actividad de los usuarios de sistemas.

c) Implementar controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por el personal, y herramientas de gestión de la ciberseguridad como, por ejemplo, programas de gestión de parches de software y firmware, protección de redes ante ataques por medio de firewalls, sistemas de prevención de intrusos, elevación de privilegios, gestión de identidades y acceso físico y lógico, mecanismos de control de identidad para evitar suplantación de terceros, entre otras.

d) Gestionar las condiciones ambientales para la localización segura de los equipos y herramientas.

e) Procedimientos de identificación de amenazas de ciberseguridad tales como phishing, malware, inyección de código malicioso, entre otros.

B.3. PROGRAMA DE GESTIÓN DE RIESGOS, CONTROL Y AUDITORÍA INTERNA

B.3.1. FUNCIÓN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos es la instancia responsable del monitoreo de los controles definidos en las políticas y los procedimientos de gestión de riesgos y control interno de la entidad. Esta función deberá ser independiente de las unidades generadoras de riesgos y de la función de auditoría interna, y reportar directamente al directorio u órgano equivalente.

La función de gestión de riesgos podrá ser realizada por una persona o unidad interna o, en ciertos casos, por la alta administración de la entidad.

En el caso que la entidad pertenezca a un grupo empresarial la función de gestión de riesgos de la entidad podrá ser ejercida por la unidad de riesgos corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que ejercerá la función de riesgos, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación. Para todos los efectos, si la función es ejercida por una unidad de gestión de riesgos corporativa en caso de que la entidad pertenezca a un grupo empresarial se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, la entidad será responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Asimismo, la función de gestión de riesgos será responsable de la realización de actividades para monitorear el cumplimiento de las políticas, procedimientos y controles para las áreas que la entidad defina.

Adicionalmente, deberá adoptar las medidas que permitan garantizar el debido cumplimiento de las disposiciones contenidas en las leyes y normativas, y en lo específico, en lo relativo al debido manejo de materias tales como, actividades prohibidas, conflictos de intereses, eventualidad de fraude, y otros delitos o infracciones.

Con objeto de implementar lo anteriormente señalado, la función de gestión de riesgos deberá:

a) Verificar la existencia de las políticas y procedimientos mínimos descritos en el literal B.2 anterior.

b) Contar con metodologías y herramientas para cuantificar, agregar y gestionar los riesgos que enfrenta la entidad, los cuales deberán evaluarse al menos anualmente y en forma prospectiva, incluyendo escenarios tales como cambios en las condiciones de la economía y situaciones de crisis. Además, deberá contar con metodologías y herramientas que le permita verificar el cumplimiento de las políticas, procedimientos y mecanismos de control.

c) Emitir un informe, al menos con una periodicidad semestral al directorio u órgano equivalente para documentar las instancias de incumplimientos detectados, causas que los originaron, medidas adoptadas y efectividad de dichas medidas.

d) Proponer cambios en las políticas y en los procedimientos de gestión de riesgos en función de las deficiencias encontradas en sus actividades de control.

e) Promover una cultura organizacional responsable en el ámbito de gestión de riesgo, que comprenda programas periódicos de difusión, concientización y capacitación, que contribuyan a que el personal de la entidad, incluyendo el directorio u órgano equivalente y el personal externo que realice funciones críticas para la entidad, comprenda los riesgos atingentes a sus funciones, y cuál es su contribución a la efectividad de la gestión de dichos riesgos.

f) La naturaleza, el alcance y oportunidad de las actividades que desarrollará la función de gestión de riesgos deberán estar contenidos en un plan anual, el que deberá ser aprobado por el directorio u órgano equivalente. En todo caso, dicho plan deberá ser actualizado cada vez que se produzcan cambios significativos tales como cambios en condiciones del entorno económico y mercados en que opera la entidad, introducción de nuevos servicios, o cambios en la regulación aplicable a la entidad.

B.3.2. PLAN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos estará a cargo de la elaboración de un plan de gestión de riesgos que incluirá las estrategias de mitigación de riesgos y la planificación de contingencias en relación con los principales riesgos que surjan de las actividades de la entidad.

El directorio u órgano equivalente deberá aprobar el plan de gestión de riesgos al menos anualmente, con el fin de reflejar cambios significativos experimentados en la estrategia de negocios de la entidad o cambios en las condiciones de mercado. La función de gestión de riesgos controlará que se dé cumplimiento al plan de gestión de riesgos y a sus respectivos procedimientos.

La elaboración de estrategias de mitigación de riesgos y planificación de contingencias considerará lo siguiente:

a) Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad, y los respectivos responsables de dichos procesos (mapa de procesos).

   La función de gestión de riesgos, en conjunto con los encargados de los procesos principales, deberá identificar formalmente los riesgos inherentes a los que se expone la entidad en el desarrollo de sus actividades.

b) Medición de los riesgos inherentes identificados en las actividades efectuadas por la entidad.

c) Definición de los mecanismos de control para mitigar los riesgos inherentes identificados. Al respecto, dichos mecanismos de control deberán considerar:

   1) Descripción de cada control y su objetivo.

   2) Identificación de los responsables del control formalmente designados para esos efectos.

3) Calificación de la efectividad de los controles para la mitigación de los riesgos inherentes, por una instancia independiente del responsable de los mismos.

d) Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al directorio u órgano equivalente y a todas las partes interesadas.

e) Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos y financieros que vaya enfrentando la entidad, cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales.

B.3.3. FUNCIÓN DE AUDITORÍA INTERNA

La función de auditoría interna es la instancia responsable de verificar el correcto funcionamiento del sistema de control interno y de gestión de riesgos de la entidad. Esta función deberá ser independiente de las unidades generadoras de riesgos y de la función de gestión de riesgos, debiendo reportar directamente al directorio u órgano equivalente.

La función de auditoría interna podrá ser realizada por una persona o unidad interna, o externalizada a un tercero. En el caso que la entidad pertenezca a un grupo empresarial, la función de auditoría interna podrá ser ejercida por la unidad de auditoría interna corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que se encargará de la actividad, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación.

Para todos los efectos, si la función de auditoría interna es ejercida por una unidad corporativa del grupo empresarial al que pertenece la empresa, se entenderá que es ejercida por una unidad interna. Sin perjuicio de lo anterior, la entidad será siempre responsable de la función de auditoría interna aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Con el objeto de que la entidad desarrolle una adecuada función de auditoría interna se deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:

a) La función de auditoría interna deberá ser desarrollada por personal con experiencia y conocimientos comprobables en marcos de gestión de los riesgos específicos que dicha función deberá auditar.

b) La función de auditoría interna deberá ser desarrollada sobre la base de una metodología que considere al menos los siguientes aspectos:

1) La naturaleza, alcance y oportunidad de las auditorías que podrían ser efectuadas.

2) Programas de trabajo de auditoría.

3) El seguimiento que se efectuará a las observaciones detectadas.

4) La forma en que se reportarán las deficiencias significativas al directorio u órgano equivalente**.**

5) La elaboración y estructura de los informes que esta función realice.

6) La existencia y ejecución de un plan anual de auditoría que incluya la naturaleza, alcance y oportunidad de las actividades que se desarrollarán, y considerar:

   i) Que las áreas, procesos, líneas de negocio o riesgos más relevantes sean auditados periódicamente, incluyendo la función de gestión de riesgos.

   ii) El seguimiento al cumplimiento de los compromisos adquiridos por las áreas auditadas en revisiones anteriores.

c) La función de auditoría interna deberá emitir un informe semestral al directorio u órgano equivalente que considere:

1) Respecto de las áreas, procesos, líneas de negocio o riesgos auditados durante el periodo:

   i) La calidad y efectividad de las políticas, procedimientos y mecanismos de control.

   ii) El resultado de las auditorías efectuadas con su respectiva calificación.

   iii) Las acciones o medidas propuestas para subsanar las observaciones levantadas y el plazo estimado para su implementación.

   iv) Fecha de la última auditoría realizada a cada unidad auditable.

2) Respecto de la función de gestión de riesgos:

   i) La efectividad del sistema de gestión de riesgos**.**

   ii) Los incumplimientos de políticas y procedimientos de gestión de riesgos detectados en las auditorías, las causas que los originaron y las acciones correctivas adoptadas para evitar su reiteración.

3) El resultado del seguimiento de la corrección de las situaciones detectadas en las auditorías realizadas.

   El informe deberá ser remitido al directorio u órgano equivalente en un plazo no superior a 30 días corridos de finalizado el periodo al cual se refiere.

B.4. PROPORCIONALIDAD

En línea con lo establecido en los artículos 1 y 12 de la ley N°21.521, las entidades podrán adaptar las disposiciones de esta Sección IV.B, conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos.

Sin perjuicio de lo anterior, la Tabla 2 describe los requisitos proporcionales que deberán cumplir las entidades que presten el servicio de asesoría de inversión

La proporcionalidad para asesores crediticios se aplicará dependiendo si hacen uso de información que califique como datos de carácter personal, en conformidad a la ley N°19.628, y en función de si tienen menos o más de 100 clientes activos en Chile.

En caso de que la función de auditoría interna sea no especializada y la función sea realizada por un tercero, en ningún caso dicho tercero podrá ejercer la función de auditoría externa en la entidad, debiendo la entidad velar por la adecuada segregación de ambas funciones.

Tabla 2. Proporcionalidad para la prestación del servicio de asesoría crediticia

Características del prestador de asesoría crediticia		**Políticas**	**Función de gestión de riesgos y auditoría interna**
No realiza tratamiento de datos personales	Menos de 100 clientes activos	Se exime de todos los requisitos de esta Sección IV.B	
	100 o más clientes activos	CI, CINF, GCR, CP, IC, ALG	No especializada
Realiza tratamiento de datos personales	Menos de 100 clientes activos	Se exime de todos los requisitos de esta Sección IV.B	
	100 o más clientes activos	CI, CINF, GCR, CP, IC, ALG, RLN, RO	Especializada

Donde,

a) CI: Conflictos de intereses.

b) CINF: Confidencialidad de la información.

c) GCR: Gestión de consultas, reclamos y denuncias.

d) CP: Comercialización y publicidad.

e) IC: Información al cliente.

f) ALG: Metodología de aprobación, evaluación y control de algoritmos.

g) RLN: Cumplimiento de requisitos legales y normativos de funcionamiento.

h) RO: Riesgo operacional.

i) No especializada: La función de gestión de riesgos podrá ser ejercida por algún integrante de la alta administración de la entidad.

j) Tratamiento de datos personales: Datos de carácter personal, en conformidad a la ley N°19.628, relevantes para efectuar recomendaciones respecto de la capacidad o probabilidad de pago de personas naturales o jurídicas.

En el caso de las entidades que presten el servicio de asesoría crediticia y cuyo requisito sea que la función de gestión de riesgos y auditoría interna sea especializada, esta función no podrá ser ejercida por la alta administración, debiendo reportar directamente al directorio u órgano equivalente

Cuando la función de auditoría interna sea no especializada y sea realizada por un tercero, en ningún caso dicho tercero podrá ejercer la función de auditoría externa en la entidad, debiendo la entidad velar por la adecuada segregación de ambas funciones

En caso de que un asesor crediticio alcance los 100 clientes activos en Chile, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de gobierno corporativo y gestión integral de riesgos correspondientes. Una vez alcanzado ese número, los asesores crediticios deberán cumplir con las exigencias de gobierno corporativo y gestión integral de riesgos. Para volver a estar exentas de los requerimientos, las entidades deberán mantenerse por más de 6 meses bajo el umbral de clientes señalado y solicitar autorización de la Comisión.

B.5. INFORMACIÓN DE INCIDENTES OPERACIONALES

Las entidades asesoras de crédito que realicen tratamiento de datos personales y tengan más de 100 clientes activos en Chile deberán comunicar a esta Comisión los incidentes operacionales que afecten la información de la entidad o los datos personales de sus clientes, tales como, problemas tecnológicos que afecten la seguridad de la información; virus o malware detectados en los activos de información críticos; pérdidas o fugas de información de la entidad o sus clientes, entre otros.

Para estos efectos, las entidades podrán usar el formato del Reporte de Incidentes Operacionales (RIO) del Anexo N°2 de esta normativa, y dispondrán de un plazo de 2 horas transcurridas desde que la entidad tomó conocimiento del hecho. El plazo señalado es solo para efectos de notificar a la Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados la CMF, posteriormente.

El directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información, así como para mantener informado en forma oportuna al directorio u órgano equivalente respecto al incidente y las medidas adoptadas para resolverlo.

C. PLATAFORMAS DE FINANCIAMIENTO COLECTIVO Y SISTEMAS ALTERNATIVOS DE TRANSACCIÓN

C.1. ROL DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El Directorio u órgano equivalente es el responsable de establecer la estructura organizacional, objetivos, políticas que permitan gestionar adecuadamente los riesgos que pueden afectar las actividades que desarrolle la entidad (marco de gestión de riesgos), debiendo asegurarse de contar con una apropiada cultura de gestión de riesgos, entendida como la adecuada comprensión del gobierno corporativo y riesgos inherentes a la entidad. Los miembros del directorio u órgano equivalente deberán contar con los conocimientos, experiencia y dedicación adecuados a este respecto.

El directorio u órgano equivalente deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:

a) Aprobar los niveles de apetito por riesgo de aquellos previamente identificados. Una efectiva definición debiera cuantificar el nivel de riesgo que el directorio u órgano equivalente desee aceptar en consideración a los objetivos estratégicos de la entidad y las responsabilidades que le son aplicables por el marco regulatorio. Además, deberá informarse continuamente del cumplimiento del apetito por riesgo.

b) Aprobar las políticas que se señalan en los literales C.2 al C.5 de esta Sección, considerando para ello:

    1) Que las políticas implementadas para gestionar los riesgos sean coherentes con la misión, visión, objetivos estratégicos, los niveles de apetito por riesgo y el marco regulatorio que le es aplicable a la entidad.

    2) Que las políticas se revisen y actualicen al menos anualmente o con la frecuencia necesaria en caso de que se produzcan cambios significativos tales como introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la entidad.

c) Establecer una estructura organizacional adecuada para la gestión de riesgos de la entidad, que considere lo siguiente:

    1) La definición de los roles, competencias y responsabilidades que permitan realizar sus actividades y gestionar adecuadamente los riesgos que enfrenta la entidad. Lo anterior involucra la segregación apropiada de los deberes y las funciones claves, especialmente aquéllas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad o sus participantes a riesgos no deseados o no mitigados y controlados; y entre las áreas generadoras de riesgo y de control de estos.

    2) La implementación de la función de gestión de riesgos, de conformidad con lo descrito en las C.4 y C.6 siguientes.

    3) La implementación de la función de auditoría interna, de conformidad con lo descrito en las secciones C.5 y C.6 siguientes.

    4) Que el directorio u órgano equivalente vele por el cumplimiento de la segregación de funciones y la independencia de las funciones de gestión de riesgos y de auditoría interna.

Contar con un Comité de Gestión de Riesgos o una instancia similar. Sin perjuicio de ello, el directorio u órgano equivalente deberá evaluar la pertinencia de conformar otros comités o instancias similares que le permitan tratar y monitorear aspectos relevantes de los negocios y la gestión de los riesgos, referidos a materias tales como, por ejemplo: Auditoría Interna; Prevención del Lavado de Activos, Financiamiento del Terrorismo y Financiamiento de Armas de Destrucción Masiva; Inversiones; Nuevos Servicios o Productos; Continuidad del Negocio; Seguridad de la Información y Ciberseguridad. El directorio u órgano equivalente deberá establecer los procedimientos para la conformación y funcionamiento de los comités o instancias similares, los cuales deberán quedar debidamente documentados, como también sus actuaciones, las que deberán ser reportadas al directorio en forma continua. Sin perjuicio de lo anterior, los Comités de Gestión de Riesgos y de Auditoría Interna (éste último, en caso de ser constituido) deberán estar integrados al menos por un miembro del directorio u órgano equivalente. Ningún director (o miembro del órgano equivalente) podrá ser parte del Comité de Gestión de Riesgos y del Comité de Auditoría Interna al mismo tiempo. La actuación de los comités que se conformen, en las materias antes mencionadas, deberá constar por escrito en actas, las que deberán reflejar con claridad los asuntos tratados.

d) Aprobar los planes anuales de las funciones de gestión de riesgos y de auditoría interna y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.

e) Establecer una política de contratación y capacitación del personal de la entidad, de forma de contar con recursos humanos calificados. Esta política y programa deberá considerar:

   1) La adecuada difusión de los valores, principios organizacionales y marco de gestión de riesgos de la entidad.

   2) Capacitación continua en relación con las actividades que realiza el personal de la entidad.

f) Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.

g) Establecer sistemas de registro y procesamiento de información con medidas de protección y seguridad adecuadas que permitan que:

   1) El directorio u órgano equivalente tenga acceso oportuno a información relacionada con el desarrollo del negocio, la gestión de riesgos, y toda otra información relevante para el cumplimiento de sus funciones.

   2) Las áreas de negocio y las funciones de gestión de riesgos y auditoría interna tengan acceso a información relevante para el cumplimiento de sus funciones.

   3) La entidad dé cumplimiento a la divulgación de información que el marco regulatorio le exige.

h) Evaluar periódicamente la suficiencia de recursos de las funciones de gestión de riesgos y auditoría interna para efectuar su labor, aprobar la asignación de los recursos necesarios para dichas funciones y monitorear el grado de cumplimiento del presupuesto asignado a tal fin.

i) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio u órgano equivalente y los comités. Todo el material que se elabore o presente al directorio u órgano equivalente o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.

C.2. POLÍTICAS, PROCEDIMIENTOS Y MECANISMOS DE CONTROL

C.2.1. ASPECTOS GENERALES

Las políticas, procedimientos y mecanismos de control de la entidad, deberán tener en cuenta los siguientes principios:

a) Establecer políticas, procedimientos y controles operativos efectivos que guarden relación con el número o tipo de participantes; volumen de operaciones; proyectos de inversión, necesidades de financiamiento o instrumentos financieros negociados, cotizados u ofertados; y respecto de cada uno de los negocios o actividades que se desarrolle.

b) Las políticas deberán exponer los principios generales y directrices establecidas por el directorio u órgano equivalente para orientar las actividades de la organización.

c) Los procedimientos definir cómo llevar a cabo un proceso, con el fin de asegurar el cumplimiento de las políticas aprobadas por el directorio. Para ello deben definir cómo llevar a cabo un proceso, incorporando, al menos: la descripción de las actividades principales que lo componen y la identificación de sus responsables; determinación de los responsables de supervisar y controlar el resultado de las actividades ejecutadas; documentación que evidencia la ejecución de las actividades que conforman los procedimientos; definición y descripción de los controles asociados a dichas actividades. En el caso de actividades externalizadas, siempre deberá existir una persona responsable dentro de la organización respecto al control de estas.

d) Las políticas, procedimientos y mecanismos de control deberán estar formalmente establecidos y documentados, siendo consistentes con los niveles de apetito por riesgo que haya definido la entidad.

C.2.2. POLÍTICAS Y PROCEDIMIENTOS A IMPLEMENTAR

La entidad deberá contar, al menos, con las políticas y procedimientos que se detallan a continuación.

a) Admisibilidad de instrumentos financieros, proyectos de inversión o necesidades de financiamiento elegibles para transar u ofertar

Se deberán definir políticas que permitan prevenir que los instrumentos sujetos a negociación en los sistemas alternativos de transacción, o los proyectos de inversión o necesidades de financiamiento que se oferten en plataformas de financiamiento

colectivo, según corresponda, resulten en una finalidad fraudulentaPara estos efectos, los sistemas alternativos de transacción y las plataformas de financiamiento colectivo deberán establecer los procedimientos a los que se refiere la Sección II.D y II.C, respectivamente, en cuanto a requisitos y procesos de acceso y de aprobación que se aplican antes de admitir instrumentos financieros o proyectos de inversión o necesidades de financiamiento, según corresponda.

b) Conflictos de intereses

Las entidades deberán definir políticas y procedimientos que especifiquen los métodos según los cuales se identificarán, manejarán y vigilarán todos los potenciales conflictos de intereses inherentes a los servicios ofrecidos por ella. Las políticas y procedimientos deberán considerar la identificación, prevención y monitoreo de los conflictos que puedan surgir entre la plataforma de financiamiento colectivo con los proyectos de inversión o necesidades de financiamiento publicados, o entre el sistema alternativo de transacción con los emisores de instrumentos financieros admitidos a transacción, según corresponda al tipo de servicio prestado.

c) Oferta de productos acorde a las necesidades, expectativas y disposición al riesgo del inversionista

Las entidades deberán definir políticas y procedimientos tendientes a que se ofrezcan a los inversionistas instrumentos financieros proyectos de inversión o necesidades de financiamiento acordes a sus necesidades, expectativas y disposición al riesgo, entregándoles información que les permita entender y aceptar el riesgo que están asumiendo, evitando ofrecer productos que no sean acordes a sus necesidades, expectativas y disposición al riesgo, según lo dispuesto en el artículo 28 de la ley N°21.521.

Las entidades deberán contar con procedimientos para asegurar el cumplimiento de la citada obligación. En aquellos casos en que un cliente decida contratar un servicio que en opinión de la entidad no sea acorde a las necesidades, expectativas o riesgos que este le haya comunicado la entidad deberá poder acreditar que aquello fue debidamente advertido, en caso de que le sea solicitado por la Comisión. Para estos efectos, los procedimientos podrán considerar el requerir a sus potenciales inversionistas antecedentes tales como información sobre sus conocimientos y experiencia como inversionista, su situación financiera y objetivos de inversión o ahorro, y otra información de esta naturaleza que la entidad considere relevante.

La entidad deberá establecer procedimientos que permitan monitorear el cumplimiento de la política de oferta de productos en forma periódica, incluyendo una descripción de los procedimientos de detección de necesidades, expectativas y disposición al riesgo asociadas a cada inversionista. La entidad podrá establecer excepciones en esta política, en caso de que la oferta de productos esté dirigida a clientes que tengan la calidad de inversionista institucional o inversionista calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

d) Prevención del lavado de activos y financiamiento del terrorismo

Las entidades deberán contar con políticas y procedimientos para el cumplimiento de las disposiciones legales y normativas relativas a la prevención del lavado de activos, financiamiento del terrorismo y financiamiento de armas de destrucción masiva, según lo dispuesto en la ley N°19.913 y en la normativa dictada por la Unidad de Análisis Financiero.

e) Información al inversionista

La entidad deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los productos o servicios ofrecidos, según lo dispuesto en el artículo 28 de la ley N°21.521.

Estas políticas deberán especificar, al menos, la información que debe ser conocida por los clientes de acuerdo con la Sección III de esta normativa, y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad controlará el cumplimiento de estas disposiciones.

f) Cumplimiento de requisitos legales y normativos de funcionamiento

Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.

Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a esta Comisión.

g) Gestión de consultas, reclamos y denuncias

Las entidades deberán definir políticas y procedimientos que le permita gestionar y resolver las consultas, denuncias y reclamos de sus clientes, trabajadores y el público general. Para ello deberá considerar, al menos, un manual que establezca, en términos simples, los antecedentes mínimos que se requerirán para efectuar una consulta, denuncia o reclamo, y que describa cómo utilizar los canales especializados que se hubieren dispuesto para esos efectos. El manual deberá establecer:

1) Procedimiento para resolver las consultas del público que considere los diferentes canales que se disponga para estos efectos. El mecanismo deberá permitir hacer un seguimiento de las consultas efectuadas.

2) Procedimientos que permitan resguardar la reserva de quien formula el reclamo o denuncia.

3) El directorio u órgano equivalente deberá mantenerse informado de los reclamos y denuncias relevantes.

4) Definir claramente cómo se calificará la gravedad o relevancia de la denuncia o reclamo, y cómo se comunicará a las instancias que corresponda, incluyendo al directorio u órgano equivalente en el caso de aquellas más relevantes.

5) Las instancias que participarán en la gestión de las consultas, denuncias o reclamos de acuerdo con la relevancia o la gravedad que se hubiere definido para cada caso. Con todo, la gestión de los reclamos deberá ser efectuada por una unidad independiente del área donde se originaron los mismos.

6) Los tiempos máximos establecidos para gestionar y responder cada consulta, denuncia o reclamo de acuerdo con su gravedad o relevancia.

7) Un registro de las consultas, denuncias y reclamos junto con la gravedad o relevancia asignada y la solución implementada.

8) Definir una instancia encargada de analizar, monitorear y proponer medidas para evitar que las situaciones que generaron las consultas, denuncias o reclamos se repitan.

C.3. RIESGO OPERACIONAL

Las plataformas de financiamiento colectivo y los sistemas alternativos de transacción, con el objeto de que la entidad desarrolle una adecuada gestión de riesgo operacional, deberán dar considerar los elementos que se señalan a continuación, adaptándolos de acuerdo con su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Las políticas y procedimientos de gestión de riesgo operacional deberán incluir, al menos, los siguientes ámbitos relacionados, descritos en las próximas secciones: seguridad de la información y ciberseguridad; continuidad de negocio; y externalización de servicios. Los ámbitos mencionados deberán ser considerados por la entidad en los informes que realicen las instancias encargadas de la gestión de riesgos y la auditoría interna, según corresponda. Lo anterior, sin perjuicio del cumplimiento de las normativas aplicables a la entidad que requieren la gestión de sus riesgos operacionales. Las políticas y procedimientos de gestión de riesgo operacional deben estar diseñadas para brindar una seguridad razonable que la entidad pueda desarrollar las operaciones del negocio en forma continua y eficiente, incluso ante la presencia de eventos disruptivos, salvaguardando sus servicios, procesos y activos de información. Estas políticas y procedimientos deben ser establecidas y aprobadas por el directorio, u órgano equivalente, y ser difundidas a todo el personal dentro de la organización. Además, dichas políticas y procedimientos deben establecer los niveles de apetito por riesgo definidos por el directorio u órgano equivalente, que determinará la necesidad de evitar, reducir, transferir o aceptar los riesgos, y acorde con ello, diseñar controles mitigantes.

b) Contar con indicadores claves de medición del riesgo operacional consistentes con la metodología de evaluación y monitoreo de riesgos integrales de la entidad, permitiendo al mismo tiempo establecer niveles de alerta y evaluar la eficacia de los controles adoptados. El detalle de cálculo de estos indicadores deberá ser incluido expresamente en las políticas y procedimientos de gestión de riesgo operacional de misma la entidad.

C.3.1. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

C.3.1.1 DISPOSICIONES GENERALES

En el ámbito de seguridad de la información y ciberseguridad, la gestión de riesgo operacional deberá incluir los siguientes elementos aplicables a todas las entidades, adaptándolos de acuerdo a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política de seguridad de la información y ciberseguridad que considere al menos lo siguiente:

   1) Procedimientos para la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad, de forma de resguardar la disponibilidad, confidencialidad e integridad de los activos de información.

   2) Niveles de apetito por riesgo en materia de seguridad de la información y ciberseguridad.

   3) Principales funciones y responsabilidades sobre la materia.

   4) Procedimientos para la evaluación de los riesgos de seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, servicios, sistemas, emprender nuevas actividades o definir nuevos procesos.

   5) Las políticas de seguridad de la información y ciberseguridad formarán parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizadas y aprobadas al menos anualmente por el directorio, u órgano equivalente, o con una periodicidad mayor en caso de cambios significativos.

b) Contar con una política de tecnologías de información y comunicación (TIC), que considere al menos lo siguiente:

   1) Definición de las líneas de responsabilidad en cuanto a la gestión de los activos de información en la entidad.

   2) Definición de los procesos TIC que aseguren un adecuado diseño, transición, operación de servicio y gestión a través de sus activos de información.

   3) Definición de los procedimientos que se deberán seguir para la adecuada gestión de los procesos TIC.

c) Definición del perfil y número necesario de personas con conocimientos o experiencia comprobables en estándares de seguridad de la información y ciberseguridad.

d) Establecimiento de los procedimientos para que el personal de la entidad, incluyendo el directorio u órgano equivalente, contribuya a una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad, de conformidad con sus roles y responsabilidades, mediante la implementación de:

   1) Procedimientos de difusión, capacitación y concientización que traten sobre los riesgos, vulnerabilidades y amenazas a la seguridad de la información, la gestión de estos, y las lecciones aprendidas respecto de los incidentes en esta materia, para garantizar que el personal de la entidad esté debidamente preparado para

enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de dichos riesgos.

2) Acuerdos contractuales con los empleados que establezcan sus responsabilidades y las de la entidad en materia de seguridad de la información y ciberseguridad, incluyendo sanciones.

e) Generación de acuerdos contractuales para la revocación de derechos de acceso a información y destrucción de activos de información como parte del proceso de cambio de posición o desvinculación de un empleado.

f) Auditoría de los procesos de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

g) Disposición de procedimientos que le permitan al directorio u órgano equivalente mantenerse informado en forma oportuna y periódica sobre el sistema de gestión de la seguridad de la información y ciberseguridad. Deberá dejarse constancia del reporte de la información de estas materias en las respectivas actas del directorio u órgano equivalente y los comités que se conformen para revisar estas materias.

C.3.1.2 PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La entidad deberá considerar los siguientes procedimientos, y adaptarlos en relación con su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Identificación

1) Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.

2) Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad.

3) Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión, clasificados desde una perspectiva de disponibilidad, confidencialidad e integridad.

4) Implementar un inventario de activos de información que permita conocer las principales características del activo, considerando al menos: hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, estaciones de trabajo, servidores, medios de almacenamiento y documentación física.

5) Actualizar el inventario de activos de información en forma continua, para lo cual los distintos procesos de gestión de riesgo operacional deberán reportar la información que pueda tener efecto en dicho inventario.

b) Protección y Detección

1) Controles de acceso a las instalaciones e infraestructuras de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.

2) Controles de acceso a los sistemas, de manera de mitigar los riesgos de suplantación o uso indebido por parte de terceros. En el caso de instalaciones, infraestructuras y sistemas críticos, se deberá privilegiar el uso de mecanismos de autenticación multifactor.

3) Implementación de herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios y administradores de sistemas y activos de información, incluyendo usuarios de alto privilegio.

4) Procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, servicios de red, sistemas operativos, bases de datos y aplicaciones de negocios en función de los roles y responsabilidades del personal y sólo lo estrictamente necesario para que éste cumpla sus funciones actuales.

5) Controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por personal interno o externo, así como también los dispositivos Internet de las Cosas (IoT).

6) Mecanismos de control y monitoreo de las condiciones ambientales para la localización segura para los equipos y herramientas, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de incendios y desastres naturales.

7) Procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:

   i) Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, anti-spyware y anti-malware, entre otros.

   ii) Un proceso de gestión de la configuración de los sistemas y activos de información.

   iii) Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:

      a) Las disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos de los inversionistas, incluyendo acuerdos de no divulgación.

b) Los procesos de administración de respaldos que aseguren la disponibilidad, confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección C.3.2.2 siguiente. Los respaldos de la información se debiesen mantener en lo posible en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

c) Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.

d) Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.

c) Respuesta y Recuperación

1) La entidad deberá contar con procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, considerando:

i) Una instancia de alto nivel definida por el directorio u órgano equivalente encargada de la gestión de incidentes de seguridad de la información y ciberseguridad.

ii) Procedimientos de respuesta y recuperación ante incidentes, aprobados por el directorio u órgano equivalente, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información críticos y las interdependencias con terceros en caso de incidentes. Dichos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección IV.C de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones. Los procedimientos de respuesta y recuperación ante incidentes deberán actualizarse al menos anualmente, cada vez que se registran cambios en los activos de información o se produzcan incidentes que amenacen la seguridad de estos.

iii) Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad, y a esta Comisión, de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección IV.C de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las

medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.

2) Procedimientos para el desarrollo, adquisición y actualización de la infraestructura tecnológica de la entidad, que consideren:

   i) Las necesidades de infraestructura tecnológica de la entidad.

   ii) Implementación de un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información producto de la introducción de nuevos productos, sistemas y actividades sean efectuadas y monitoreadas de manera segura y controlada.

   Como parte de este proceso, previo al paso de producción de un servicio o activo de información se deben realizar pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas, con el propósito de asegurar que no hubiere un impacto adverso en la seguridad de la información y en las operaciones del negocio.

   iii) Implementación de un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas que no generen efectos adversos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial

   iv) Implementación de un proceso de gestión de actualizaciones de seguridad de software (parches).

3) La entidad deberá contar con un procedimiento para el mejoramiento continuo de las herramientas, procedimientos y controles de seguridad de la información y ciberseguridad que considere:

   i) Recolectar y analizar información sobre el funcionamiento de activos de información.

   ii) Analizar los incidentes de seguridad de la información y ciberseguridad y la efectividad de las medidas adoptadas para resolverlo.

   iii) Ejecutar pruebas para identificar amenazas y vulnerabilidades en la seguridad de la información:

      a) Las pruebas deberán ser realizadas con una periodicidad no mayor a un año, y ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

      Las pruebas deberán estar basadas en escenarios de riesgo planificados y diseñados para demostrar que los mecanismos y herramientas implementados para preservar la seguridad de la información cumplen adecuadamente con su objetivo, incluyendo ataques cibernéticos.

b) Los resultados de las pruebas realizadas deberán ser reportados al directorio u órgano equivalente, incluyendo recomendaciones de mejora en las herramientas, procedimientos y controles.

C.3.2. CONTINUIDAD DEL NEGOCIO

C.3.2.1 DISPOSICIONES GENERALES

En el ámbito de continuidad de negocio, la gestión de riesgo operacional deberá tomar en cuenta los siguientes elementos y adaptarlos de acuerdo con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política de continuidad de negocio que considere a lo menos lo siguiente:

   1) Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Para las entidades clasificadas en el Bloque 3, estos procedimientos se deberán referir al menos a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).

   2) Establecer las principales funciones y responsabilidades sobre la materia, en especial, cuáles serán las instancias encargadas de definir, diseñar, ejecutar y mejorar los procedimientos y metodologías para la gestión de continuidad de negocio. Las políticas de continuidad del negocio formarán parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizada y aprobada al menos anualmente por el directorio u órgano equivalente o con una periodicidad menor en caso de cambios significativos.

b) Contar con personas con conocimientos o experiencia comprobables en estándares de continuidad de negocio y experiencia en la gestión de los riesgos asociados, cuyas actividades principales serán el desarrollo y mejora de las políticas, procedimientos y controles para la gestión de continuidad de negocio.

c) Políticas y procedimientos de capacitación y concientización para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de los riesgos del sistema de continuidad de negocio.

d) El directorio u órgano equivalente deberá mantenerse informado sobre la gestión de continuidad de negocio, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

C.3.2.2 PROCEDIMIENTOS PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS

Las entidades deberán implementar los siguientes elementos para la gestión de la continuidad de negocios, adaptándolos en relación con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres, aprobado anualmente por el directorio u órgano equivalente, que contenga:

   1) Los procedimientos para la gestión de eventos de continuidad, con un nivel de detalle que permita a las distintas instancias afectadas determinar las actividades a desarrollar en cada escenario definido.

   2) Los criterios para la activación del Plan y para la vuelta a la normalidad. Esto incluye evaluar oportunamente los riesgos asociados a la continuidad de negocios que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

   3) Roles y responsabilidades del personal.

   La periodicidad de actualización de este Plan podría ser mayor dependiendo de la normativa propia de la entidad, o a requerimiento de esta Comisión.

b) Las entidades clasificadas en el Bloque 3, descrito más abajo, deberán realizar o actualizar, al menos anualmente, ante eventos que amenacen la continuidad de las operaciones del negocio, un BIA con el objeto de identificar los procesos de mayor relevancia para la continuidad de negocio, el impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de estos. El BIA deberá realizarse a nivel estratégico, táctico y operativo. De esos procesos, y considerando los niveles de apetito por riesgo definidos, se deberá determinar:

   1) Los tiempos máximos tolerables de interrupción (MTPD por sus siglas en inglés);

   2) Los tiempos objetivos de recuperación (RTO por sus siglas en inglés);

   3) Los puntos objetivos de recuperación (RPO por sus siglas en inglés);

   4) Los niveles mínimos aceptables de operación; y

   5) Los recursos humanos, tecnológicos y de infraestructura e información necesarios para su continuidad y recuperación.

   Los resultados del BIA deberán ser aprobados por el directorio u órgano equivalente.

c) En el caso de sistemas alternativos de transacción deben disponer de un sitio secundario físico o en la nube que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal, permitiendo restablecer los procesos de mayor relevancia del negocio, tales como plataformas, infraestructura, sistemas y procesamiento de datos.

d) Las entidades clasificadas en el Bloque 3 deberán realizar o actualizar, al menos anualmente, una evaluación de impacto de riesgos (RIA) que permita identificar y analizar los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas; y la falta de provisión de los servicios críticos contratados a proveedores.

e) Las entidades clasificadas en el Bloque 3, en consideración de los resultados del BIA y el RIA, deberán definir una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad.

f) Se deberá implementar un Plan de Crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante respecto del evento de continuidad, las medidas adoptadas para resolverlo y para coordinar una respuesta adecuada dentro de los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA (entidades clasificadas en el Bloque 3 al que se refieren las secciones anteriores).

g) Contar con un procedimiento para el mejoramiento continuo de las políticas, planes y procedimientos de continuidad del negocio con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

h) El Plan de Continuidad de Negocio y Recuperación de Desastres deberá ser probado anualmente, de forma de asegurar que es adecuado y efectivo, sin perjuicio de que esta Comisión pueda solicitar una periodicidad diferente para las entidades clasificadas en el Bloque 3. Estas pruebas deberán considerar a lo menos lo siguiente:

    1) Deberán ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

    2) Estar basadas en escenarios de riesgo que se asimilen a eventos reales incluyendo escenarios severos pero plausibles. Lo anterior, para demostrar que los procedimientos de continuidad de negocio funcionarán en caso de ser necesarios, incluyendo ataques cibernéticos, desastres naturales y contingencias sanitarias.

    3) Las entidades del Bloque 1 y 2, definidas en las secciones anteriores, podrán utilizar indicadores de continuidad del negocio distintos de los establecidos en la Sección B.2.c.

Se deberán emitir reportes de los resultados de las pruebas realizadas al directorio u órgano equivalente, que contengan recomendaciones y acciones para implementar mejoras al Plan de Continuidad de Negocio y Recuperación ante Desastres.

C.3.3. EXTERNALIZACIÓN DE SERVICIOS

C.3.3.1 RIESGOS DE EXTERNALIZACIÓN

Los servicios prestados por proveedores, relacionados con el cumplimiento normativo, la continuidad del negocio, la seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante, deberán ser considerados en los procesos de gestión de riesgo operacional de la entidad. En tal sentido, para la evaluación de riesgos de contratación de proveedores, se deberán considerar, entre otros, los siguientes riesgos:

1) Riesgo de sustitución: la posibilidad de sustituir o no a un proveedor dentro de un plazo determinado que garantice la continuidad del servicio contratado.

2) Riesgo de intervención: la posibilidad de que la entidad tenga que hacerse cargo de la función contratada.

3) Riesgo de subcontratación: la posibilidad de que el proveedor subcontrate a su vez todo o parte del servicio, reduciendo la capacidad de la entidad de supervisar la función subcontratada.

4) Riesgo asociado a la posibilidad que una entidad contrate uno o varios servicios en un mismo proveedor que sea difícil de sustituir, incrementando la posibilidad de fallas o interrupciones prolongadas.

C.3.3.2 PROCEDIMIENTOS PARA LA GESTIÓN DE SERVICIOS EXTERNALIZADOS

En el ámbito de externalización de servicios, la gestión de riesgo operacional deberá considerar los siguientes elementos y adaptarlos de acuerdo con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política para la externalización de servicios que considere a lo menos lo siguiente:

1) Definir la estructura de gobierno y de los procedimientos a seguir para autorizar y gestionar la externalización de servicios por terceros, incluyendo las líneas de reporte y de responsabilidad.

2) Establecer los objetivos en materia de externalización de servicios.

3) Establecer los niveles de apetito por riesgo en la externalización de servicios y las estrategias de mitigación.

4) Cumplir con las disposiciones en materia de seguridad de la información, ciberseguridad y continuidad de negocios.

5) Establecer los procedimientos para la determinación de los servicios críticos. En tal sentido, para entender como crítico un servicio se deberán tener en cuenta las siguientes consideraciones:

   i) El efecto que una debilidad o falla en la provisión o ejecución del servicio tenga sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante.

   ii) La complejidad de las funciones comerciales asociadas.

   iii) El grado en que el servicio puede transferirse rápidamente a otro proveedor, considerando los costos y el tiempo para hacerlo.

6) Definir los servicios que solo pueden ser externalizados con la aprobación previa del directorio u órgano equivalente.

7) Definir los elementos mínimos que deberá incorporar el contrato de prestación de servicios.

8) Definir los elementos de la gestión de riesgos que no serán aplicados a actividades que por su naturaleza no tengan impacto relevante en la prestación de los servicios.

9) Incluir a las políticas de externalización de servicios como parte de las políticas de gestión de riesgos de la entidad, debiendo ser aprobada y actualizada al menos anualmente por el directorio u órgano equivalente, o con una frecuencia mayor en caso de cambios internos o externos significativos.

10) Considerar los riesgos de sustitución, intervención, subcontratación y concentración de la sección anterior.

b) Establecer procedimientos para la selección, contratación y monitoreo de proveedores que consideren:

1) Una definición de los criterios particulares de contratación, cuando el proveedor se trate de una entidad relacionada. Estos criterios deberán estar destinados a evitar los conflictos de intereses que se pueden presentar.

2) La incorporación al análisis de elementos que permitan llevar a cabo un proceso de debida diligencia, de forma de asegurar que los proveedores tengan una adecuada reputación comercial, solvencia financiera, experiencia y recursos suficientes para garantizar la calidad de la provisión del servicio. En el caso de servicios en los que no se pueda garantizar el pleno cumplimiento de las condiciones mencionadas, como puede ser el caso de servicios de procesamiento de datos realizados en el extranjero, el directorio u órgano equivalente de la entidad deberá revisar y evaluar antecedentes que respalden la calidad del servicio prestado, la solidez financiera del proveedor y la existencia de una adecuada legislación de protección de datos personales en la jurisdicción aplicable, haciéndose responsable por la disponibilidad, confidencialidad e integridad de la información entregada al proveedor contratado.

c) Contemplar en los contratos con los proveedores de servicios externalizados los siguientes contenidos mínimos:

1) Una descripción clara del servicio contratado y el plazo de vigencia.

2) Las obligaciones de prestación del servicio por parte del proveedor, definiendo niveles de servicio acordados. La entidad deberá definir las situaciones que se considerarán graves incumplimientos contractuales y causales de término anticipado del contrato.

3) La obligación de comunicar cualquier acontecimiento que pueda tener un impacto material en la capacidad para llevar a cabo el servicio externalizado.

4) Los requisitos de seguridad de la información, ciberseguridad y continuidad de negocios que deberá cumplir el proveedor, que deben ser concordantes con las disposiciones establecidas en esta materia por la entidad. Los proveedores deberán contar con procedimientos de gestión de incidentes y continuidad de negocios que le permitan seguir brindando los servicios en el evento que se presenten situaciones disruptivas.

5) La documentación de los procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado. En el caso de existir subcontratación en cadena, la entidad deberá verificar el cumplimiento de las condiciones pactadas con el proveedor de servicios inicial y las entidades subcontratadas por este último.

6) Los procedimientos para la evaluación y monitoreo periódico de la calidad de la provisión del servicio externalizado. La entidad podrá pactar con el proveedor la realización de auditorías por terceros designados o por la propia entidad, quien será responsable en última instancia por garantizar la calidad de la provisión del servicio externalizado.

7) Las estrategias para el término de la prestación de servicios externalizados sin perjudicar las operaciones de la entidad, considerando esas situaciones en el Plan de Continuidad del Negocio y Recuperación ante Desastres.

d) Contar con un registro de servicios externalizados, para gestionar los riesgos de subcontratación, que deberá incluir al menos la siguiente información:

1) Identificación del servicio externalizado, incluyendo una breve descripción del mismo y de los datos involucrados si corresponde a un servicio crítico, si existe subcontratación en cadena, y si se lleva a cabo en la nube.

2) Identificación del proveedor, incluyendo si corresponde a una entidad relacionada o no.

3) Fecha de inicio, renovación y término del servicio.

4) En el caso de servicios de procesamiento de datos, una descripción de los datos y tratamientos que se subcontratan, las medidas de seguridad adoptadas, y la ubicación geográfica del proveedor.

5) En caso de subcontratación en cadena, se deberá detallar cuáles son las entidades a las que el proveedor subcontrata el servicio, una descripción de los riesgos asociados y si el proveedor realiza un control de la calidad de la provisión del servicio subcontratado en cadena.

e) Monitorear periódicamente que los proveedores cumplen con las condiciones pactadas para garantizar la calidad de la provisión del servicio. La entidad será responsable de la calidad de los servicios externalizados.

f) En el caso que la entidad decida contratar servicios de acceso y tratamiento de información en la nube, o que el proveedor como parte de la subcontratación en cadena considere los servicios en la nube, se deberá realizar un análisis reforzado de los riesgos inherentes a esos servicios, analizando en particular cómo podría afectarse la disponibilidad, confidencialidad e integridad de la información, y la continuidad de negocio de la entidad. Ese análisis deberá tener en consideración factores tales como:

1) Las certificaciones independientes respecto a la gestión de la seguridad de la información y la calidad de la prestación del servicio del proveedor.

2) La celebración del contrato de externalización de servicios directamente entre la entidad y el proveedor, con la finalidad de minimizar los riesgos en este tipo de servicios.

3) El procesamiento o almacenamiento de información en otras jurisdicciones, y en ese caso la existencia de normas que resguardan la protección de datos personales, la disponibilidad, confidencialidad e integridad de la información y la resolución de contingencias legales.

4) La existencia de adecuados mecanismos de seguridad del proveedor, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura en la nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la disponibilidad, confidencialidad e integridad de los datos de la entidad.

5) La utilización de técnicas de encriptación para los datos que la entidad establezca, de acuerdo con su naturaleza y sensibilidad

g) Evaluar que el proveedor de los servicios contratados posea adecuados conocimientos y experiencia.

h) Mantener personal con el debido conocimiento y experiencia para efectuar el control de la prestación de servicios efectuada por sus proveedores. Asimismo, también deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de los servicios contratados.

El directorio u órgano equivalente deberá mantenerse informado sobre las materias referidas a la externalización de servicios, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

C.4. FUNCIÓN DE GESTIÓN DE RIESGOS

C.4.1. DISPOSICIONES GENERALES

La instancia encargada de la función de gestión de riesgos tiene por objeto que las actividades del proceso de gestión de riesgos sean desarrolladas adecuadamente en la entidad (marco de gestión de riesgo), conforme a las políticas y procedimientos establecidos para dicho efecto.

La función de gestión de riesgos podrá ser realizada por una persona o unidad interna, de acuerdo con la Sección C.6 siguiente. Dicha función deberá ser independiente de las áreas operativas y de negocios de la entidad y de la instancia encargada de la función de auditoría interna, con reporte directo al directorio u órgano equivalente.

En el caso que la entidad pertenezca a un grupo empresarial, la función de gestión de riesgos de la entidad podrá ser ejercida por la unidad de riesgos corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que ejercerá la función de riesgos, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación. Para todos los efectos, si la función es ejercida por una unidad de gestión de riesgos corporativa, en el caso de que la entidad pertenezca a un grupo empresarial se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, la entidad será siempre responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

El marco de gestión de riesgos deberá tener como propósito gestionar eficazmente los riesgos que se presentan en el desarrollo de su negocio, como por ejemplo el riesgo general del negocio, riesgo operacional y riesgo reputacional, entre otros. Las políticas, procedimientos y sistemas de gestión de riesgos deberán cautelar además el cumplimiento de los requisitos establecidos en las leyes y la normativa aplicable.

Para el desarrollo de sus actividades, se deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:

a) La función de gestión de riesgos deberá ser independiente de las áreas generadoras de riesgos y de la función de auditoría interna, con línea de responsabilidad directa al directorio u órgano equivalente.

b) El personal encargado deberá contar con experiencia y conocimientos comprobables en estándares o mejores prácticas de común aceptación para la gestión de riesgos y de los riesgos específicos que debe gestionar de acuerdo con el marco de gestión de riesgos.

c) La función de gestión de riesgos deberá proponer políticas y procedimientos para la gestión de riesgos al directorio u órgano equivalente, consistentes con la misión, visión, objetivos estratégicos y las responsabilidades que el marco regulatorio le asigna.

d) La función de gestión de riesgos deberá contar con metodologías y herramientas para cuantificar, agregar y gestionar los riesgos que enfrenta la entidad, los cuales deberán evaluarse al menos anualmente y en forma prospectiva, incluyendo escenarios tales como cambios en las condiciones de la economía y situaciones de crisis. Además, deberá contar con metodologías y herramientas que le permita verificar el cumplimiento de las políticas, procedimientos y mecanismos de control.

e) La naturaleza, el alcance y oportunidad de las actividades que la función de gestión de riesgos desarrollará deberá estar contenido en un plan anual, el que deberá ser aprobado por el directorio u órgano equivalente. En todo caso, dicho plan deberá ser actualizado cada vez que se produzcan cambios significativos tales como cambios en condiciones del entorno económico y mercados en que opera la entidad, introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la entidad.

   La función de gestión de riesgos deberá promover una cultura organizacional responsable en el ámbito de gestión de riesgo, que comprenda programas periódicos de difusión, concientización y capacitación, que contribuyan a que el personal de la entidad, incluyendo directorio u órgano equivalente y personal externo que realice funciones críticas para la organización, comprenda los riesgos atingentes a sus funciones, y cuál es su contribución a la efectividad de la gestión de dichos riesgos.

C.4.2. PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgos considerará las siguientes actividades principales:

a) Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad, y los respectivos responsables de dichos procesos (mapa de procesos).

   La función de gestión de riesgos, en conjunto con los encargados de los procesos principales, deberá identificar formalmente los riesgos inherentes a los que se expone la entidad en el desarrollo de sus actividades.

b) Medición de los riesgos inherentes identificados en las actividades efectuadas por la entidad. Para ello deberá elaborarse una matriz de riesgo que permita estimar una probabilidad de ocurrencia e impacto de los riesgos, como también calificar su severidad considerando estos factores.

c) Definición de los mecanismos de control para mitigar los riesgos inherentes identificados. Al respecto, dichos mecanismos de control deberán considerar:

   1) Descripción de cada control y su objetivo.

   2) Identificación de los responsables del control formalmente designados para esos efectos.

   3) Calificación de la efectividad de los controles para la mitigación de los riesgos inherentes, por una instancia independiente del responsable de estos.

d) Cuantificación de los riesgos residuales, los que serán determinados a partir de los riesgos inherentes considerando la calificación de la efectividad de los controles.

e) Definición del tratamiento de los riesgos residuales, para lo cual se deberá tener en consideración los niveles de apetito por riesgo.

f) Procedimiento de monitoreo de los riesgos y controles establecidos, considerando al menos:

   1) Definición y medición de indicadores clave de evaluación de riesgos.

   2) Procedimientos de monitoreo continuo de riesgos que permitan identificar oportunamente una posible materialización de riesgos por encima de los niveles de apetito por riesgo definidos. Para ello, la entidad deberá implementar un mecanismo de alertas basado en los indicadores clave de riesgos.

   3) Comunicación oportuna de las deficiencias de los controles y la desviación del riesgo residual respecto a los niveles de apetito por riesgo definidos a los responsables de aplicar las medidas correctivas, incluyendo los comités a los que se refiere esta normativa y al directorio u órgano equivalente en el caso de deficiencias significativas.

   4) Seguimiento continuo de las medidas correctivas que se hubieren definido para las deficiencias identificadas en el proceso de monitoreo de riesgos, para que éstas sean efectivamente implementadas en los plazos establecidos.

g) Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al directorio u órgano equivalente y a todas las partes interesadas.

h) Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos y financieros que vaya enfrentando la entidad, cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales.

C.5. FUNCIÓN DE AUDITORÍA INTERNA

La instancia encargada de la función de auditoría interna tiene por objeto verificar el correcto funcionamiento del sistema de gestión de riesgos y su consistencia con los objetivos y políticas de la organización, como también del cumplimiento de las disposiciones legales y normativas que le son aplicables a la entidad.

La función de auditoría interna podrá ser realizada por una persona o unidad interna o externalizada a un tercero, de acuerdo con la Sección C.6 siguiente.

En el caso que la entidad pertenezca a un grupo empresarial, la función de auditoría interna podrá ser ejercida por la unidad de auditoría interna corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que se encargará de la actividad, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación. Para todos los efectos, si la función de auditoría interna es ejercida por una unidad corporativa del grupo empresarial al que pertenece la empresa, se entenderá que es ejercida por una unidad interna.

Sin perjuicio de lo anterior, la entidad será siempre responsable aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Para el desarrollo de sus actividades, se deberá dar cumplimiento, al menos, a los principios y elementos que se señalan a continuación:

a) La función de auditoría interna deberá ser independiente de las áreas generadoras de riesgos y de la función de gestión de riesgos, con línea de responsabilidad directa al directorio u órgano equivalente.

b) El personal encargado deberá tener experiencia y conocimientos comprobables en marcos de gestión de los riesgos específicos que deberá auditar.

c) La auditoría interna deberá ser desarrollada sobre la base de una metodología que considere al menos los siguientes aspectos:

    1) La naturaleza, alcance y oportunidad de las auditorías.
    2) Programas de trabajo de auditoría.
    3) Las categorías utilizadas para calificar las observaciones detectadas.
    4) El seguimiento que se efectuará a las observaciones detectadas.
    5) La forma en que se reportarán las deficiencias significativas al directorio.
    6) La elaboración y estructura de los informes que la función de auditoría interna realice.

d) La existencia y ejecución de un plan anual de auditoría que incluya la naturaleza, alcance y oportunidad de las actividades que la función de auditoría interna desarrollará, y considerar:

    1) Que las áreas, procesos, líneas de negocio o riesgos más relevantes sean auditados periódicamente, incluyendo la función de gestión de riesgos.

    2) El seguimiento al cumplimiento de los compromisos adquiridos por las áreas auditadas en revisiones anteriores.

e) La función de auditoría interna deberá emitir un informe semestral al directorio u órgano equivalente que considere:

    1) Respecto de las áreas, procesos, líneas de negocio o riesgos auditados durante el periodo:

        i) La calidad y efectividad de las políticas, procedimientos y mecanismos de control.

        ii) El resultado de las auditorías efectuadas con su respectiva calificación.

        iii) Las acciones o medidas propuestas para subsanar las observaciones levantadas y el plazo estimado para su implementación.

        iv) Fecha de la última auditoría realizada a cada unidad auditable.

2) Respecto de la función de gestión de riesgos:

   i) La efectividad del sistema de gestión de riesgos.

   ii) Los incumplimientos de políticas y procedimientos de gestión de riesgos detectados en las auditorías, las causas que los originaron y las acciones correctivas adoptadas para evitar su reiteración.

3) El resultado del seguimiento de la corrección de las situaciones detectadas en las auditorías realizadas.

El informe deberá ser remitido al directorio u órgano equivalente en un plazo no superior a 30 días corridos de finalizado el periodo al cual se refiere. Lo anterior, sin perjuicio de la información mensual que la función de auditoría interna le pueda proporcionar al directorio u órgano equivalente, de forma de mantenerlo informado de la labor de esta función.

C.6. PROPORCIONALIDAD

De acuerdo con lo establecido en los artículos 1 y 12 de la ley N°21.521, además de las consideraciones de proporcionalidad, conforme al tamaño, volumen y naturaleza de los negocios y riesgos de la entidad en la Sección IV.C, se definirán los siguientes bloques, de acuerdo con la siguiente clasificación:

1) Bloque 1: entidades que tengan un número de clientes activos en Chile menor a 500, y no cumplan ninguna de las métricas de volumen de negocio de las entidades Bloque 2 o 3. Se considerarán clientes activos aquellos que cumplan con las condiciones definidas en el Anexo N°1 de esta normativa.

2) Bloque 2: entidades que cumplan alguna de las siguientes condiciones:

   i) Tengan un número de clientes activos en Chile entre 500 y 5.000.

   ii) Transacciones promedio diarias en los últimos tres meses (media móvil) entre UF 100.000 y UF 500.000.

   iii) Ingresos en los últimos 12 meses (media móvil) entre UF 25.000 y UF 50.000.

3) Bloque 3: entidades que cumplan alguna de las siguientes condiciones:

   i) Más de 5.000 clientes activos en Chile.

   ii) Más de UF 500.000 en transacciones promedio diarias en los últimos tres meses (media móvil).

   iii) Ingresos en los últimos 12 meses (media móvil) sobre UF 50.000.

En caso de que una entidad sea reclasificada a un bloque superior, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de gobierno corporativo y gestión integral de riesgos correspondientes a dicho bloque. Las entidades podrán ser reclasificadas a bloques inferiores después de un mínimo de 6 meses y con autorización de la Comisión.

Las entidades que clasifiquen dentro de los Bloques 1 o 2 podrán desarrollar la función de auditoría interna por una persona o unidad interna o por un tercero externo, velando siempre por el cumplimiento de la segregación e independencia con la función de gestión de riesgos.

En caso de que la función de auditoría interna sea realizada por un tercero externo, en ningún caso dicho tercero podrá ejercer la función de auditoría externa en la entidad, debiendo la entidad velar por la adecuada segregación de ambas funciones.

Las entidades que clasifiquen dentro del Bloque 3 deberán desarrollar la función de auditoría interna por una persona o unidad interna, velando siempre por el cumplimiento de la segregación e independencia con la función de gestión de riesgos.

Tabla 3. Proporcionalidad para la prestación de los servicios de sistema alternativo de transacción o plataforma de financiamiento colectivo

<table>
<tr><th>Bloque</th><th>Políticas</th><th>Función de gestión de riesgos</th><th>Función de auditoría interna</th></tr>
<tr><td>1</td><td>MIF, CI, OP, PLAFT, II, RO</td><td rowspan="3">Persona o unidad interna</td><td rowspan="2">Persona o unidad interna o ser realizadas por un tercero</td></tr>
<tr><td>2</td><td>MIF, CI, OP, PLAFT, II, RO</td></tr>
<tr><td>3</td><td>MIF, CI, OP, PLAFT, II, RLN, GCR, RO</td><td>Persona o unidad interna</td></tr>
</table>

Donde,

- MIF: Mantención de instrumentos financieros en sistemas alternativos de transacción, o difusión de proyectos de inversión o necesidades de financiamiento en plataformas de financiamiento colectivo.
- CI: Conflictos de intereses.
- OP: Oferta de productos acorde a las necesidades, expectativas y disposición al riesgo del inversionista.
- PLAFT: Prevención del lavado de activos y financiamiento del terrorismo.
- II: Información al inversionista.
- RLN: Cumplimiento de requisitos legales y normativos de funcionamiento.
- GCR: Gestión de consultas, reclamos y denuncias.
- RO: Riesgo operacional definido en la sección IV.C.3.

C.7. INFORMACIÓN DE INCIDENTES OPERACIONALES

C.7.1. REGISTRO Y COMUNICACIÓN DE INCIDENTES OPERACIONALES

a) Las plataformas de financiamiento colectivo y los sistemas alternativos de transacción, pertenecientes al Bloque 3, deberán comunicar a esta Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en servicios importantes para las operaciones del negocio; problemas tecnológicos que afecten la seguridad de la información; ataques del ciberespacio; virus o malware detectados en los activos de información críticos; eventos de indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información de la entidad o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos; problemas que afecten la continuidad de proveedores de servicios críticos; entre otros. Esta información deberá ser mantenida por la entidad en una base de datos de incidentes y otra base de datos de pérdidas operacionales para el mejoramiento continuo del proceso de gestión de riesgo operacional.

b) La ocurrencia de un incidente operacional de aquéllos mencionados en el numeral anterior deberá ser informada a esta Comisión en un plazo máximo de 2 horas desde que la entidad tomó. El plazo señalado es solo para efectos de notificar a la Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados la CMF, posteriormente. Las instrucciones para reportar los incidentes operacionales a esta Comisión se encuentran en el Anexo N° 2 de esta normativa.

c) Para estos efectos, el directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información según lo indicado en esta sección. Ambas personas deberán tener un nivel ejecutivo y ser designados por la entidad, tanto para este efecto como para responder eventuales consultas por parte de esta Comisión.

d) Asimismo, en los casos en que esta Comisión lo estime necesario, podrá requerir a la entidad la elaboración de un informe interno que contenga al menos: el análisis de las causas del incidente; la generación de documentación e informes de investigación; un análisis del impacto generado en los servicios; y el procedimiento para evitar con alto grado de seguridad que se vuelva a presentar; y las materias adicionales que esta Comisión pueda requerir.

e) Sin perjuicio de lo anterior, la entidad deberá mantener informado en forma oportuna al directorio u órgano equivalente sobre las actualizaciones de todos los incidentes operacionales relevantes y las medidas adoptadas para resolverlo.

C.7.2. REGISTRO Y COMUNICACIÓN DE PÉRDIDAS OPERACIONALES

a) Se entiende por pérdida operacional toda pérdida financiera resultante de la materialización del riesgo operacional de acuerdo con lo definido anteriormente. Esto incluye las pérdidas financieras debido a cambios legales o regulatorios que afecten las operaciones de la entidad, o producto de incumplimientos con la regulación vigente.

b) La información de todos los incidentes que se materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento este deberá ser enviada a esta Comisión de acuerdo con las instrucciones del Anexo N° 3 de la presente norma, 15 días hábiles después del cierre de junio y diciembre de cada año.

c) Los criterios para la confección del registro de pérdidas operacionales son los siguientes:

   1) La entidad deberá contar con procesos y procedimientos documentados para la identificación, recopilación, uso y comunicación de los registros de pérdida operacional. Esta Comisión podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por empresas de auditoría externa, de aquellos inscritos en el Registro de Empresas de Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.

   2) Los registros internos sobre pérdidas operacionales de la entidad deberán ser integrales e incluir la totalidad de las actividades y exposiciones relevantes, en todos los sistemas y en todas las ubicaciones geográficas pertinentes.

   3) La entidad deberá recopilar información sobre los importes brutos de las pérdidas, y sobre las fechas de referencia de los eventos de riesgo operacional. Además, la entidad deberá recoger información sobre recuperaciones de importes brutos de pérdidas, e información descriptiva sobre los factores determinantes o las causas del evento de pérdida. El grado de detalle de la información descriptiva deberá estar en proporción al importe bruto de la pérdida.

   4) La entidad deberá utilizar la fecha de contabilización del evento para construir el conjunto de registros sobre pérdidas. En el caso de eventos legales, la fecha de contabilización se refiere a cuando se constituye una provisión para esta contingencia legal en el estado de situación financiera, con su reflejo correspondiente en el estado de resultados.

   5) Las pérdidas causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo, pero contabilizadas en el transcurso de varios años, deberán asignarse a los años correspondientes en la base de datos de pérdidas, en consonancia con su tratamiento contable.

d) Por pérdida bruta se entiende una pérdida antes de recuperaciones de cualquier tipo.

   1) Los siguientes ítems deben ser incluidos en los cálculos de las pérdidas brutas para la base de datos de pérdidas:

i) Cargos directos en las cuentas de Estados de Resultados de la entidad y amortizaciones debido a eventos de riesgo operacional del período. Por ej. Costos incurridos como consecuencia de un evento, incluyendo gastos externos con una relación directa al evento por riesgo operacional (ej. Gastos legales directamente relacionados al evento y comisiones pagadas a los asesores, abogados o proveedores) y costos de reparación o reemplazo incurridos para restaurar la posición que prevalecía antes del evento de riesgo operacional.

ii) Cargos directos en las cuentas de Estados de Resultados de la entidad y amortizaciones debido a eventos por riesgo operacional de ejercicios contables previos que afecten los estados financieros de la entidad en el presente periodo.

2) Los siguientes ítems deben ser excluidos de las pérdidas brutas registradas en la base de datos de pérdidas:

i) Costos por contratos de mantenimientos generales de la propiedad, planta o equipos.

ii) Gastos internos o externos con el fin de mejorar el negocio después de las pérdidas por riesgo operacional: actualizaciones, mejoras, iniciativas de gestión del riesgo y mejoras en ellas.

iii) Primas de seguro.

e) Por pérdida neta se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida inicial, que no necesariamente se efectúa en el mismo periodo en el que se perciben los fondos respectivos.

La entidad deberá ser capaz de identificar las recuperaciones no procedentes de seguros y las recuperaciones originadas por el pago de indemnizaciones de seguros para todos los eventos de pérdidas operacionales. Asimismo, deberá utilizar las pérdidas netas de recuperaciones (incluidas las procedentes de seguros) en el conjunto de registros sobre pérdidas operacionales, aunque las recuperaciones sólo podrán utilizarse para reducir las pérdidas cuando se haya recibido el pago.

Las entidades clasificadas en los Bloques 1 y 2 quedan eximidas del reporte de pérdidas operacionales al que se refiere el Anexo N°3 de la presente normativa.

D. ENRUTAMIENTO DE ÓRDENES

D.1. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El Directorio u órgano equivalente de la entidad es la instancia responsable de aprobar y autorizar las políticas de gestión de riesgos y control interno, como mínimo una vez al año o con la frecuencia necesaria en caso de que se produzcan cambios significativos en las políticas establecidas, dejando evidencia de ello. Para esos efectos, el directorio u órgano equivalente deberá dar cumplimiento a los principios y elementos de gestión de riesgos que se señalan a continuación:

a) Establecer la misión, visión y objetivos estratégicos, teniendo en consideración las responsabilidades que el marco regulatorio vigente establece para la entidad.

b) Aprobar políticas de gestión de riesgos que sean coherentes con los objetivos estratégicos y el marco regulatorio.

c) Revisar las políticas, al menos anualmente, y actualizarlas en caso de que se produzcan cambios significativos tales como introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la entidad.

d) Evaluar periódicamente la suficiencia de recursos de las instancias encargadas de la gestión de riesgos.

e) Establecer una estructura organizacional adecuada para la gestión de riesgos de la entidad, que considere lo siguiente:

   1) La identificación y gestión de todos los riesgos pertinentes derivados del desarrollo de sus actividades. En ese tenor, la estructura organizacional debe ser la adecuada en relación con el volumen de negocios; el número y tipo de clientes de la entidad; la complejidad de las relaciones con otras entidades, entre otros aspectos.

   2) La definición de los roles, competencias y responsabilidades que permitan realizar sus actividades y gestionar adecuadamente los riesgos que enfrenta la entidad. Lo anterior involucra la segregación apropiada de los deberes y las funciones claves, especialmente aquéllas que, si fueran realizadas por una misma persona, puedan dar lugar a errores que no se detecten o que expongan a la entidad o sus participantes a riesgos indebidos; y entre las áreas generadoras de riesgo y de control de estos.

   3) La implementación de la función de gestión de riesgos, de conformidad con lo descrito en el literal D.3. de esta Sección.

f) Establecer políticas de contratación de empleados que aseguren que la entidad disponga de personal con la debida experiencia para desempeñar sus funciones, y velar porque se cuente con el recurso humano calificado para la gestión de riesgos.

g) Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.

h) El directorio u órgano equivalente deberá evaluar la pertinencia de conformar un Comité de Gestión de Riesgos o una instancia similar que le permitan tratar y monitorear aspectos relevantes de los negocios, referidos a materias tales como conflictos de intereses, seguridad de la información, entre otros. Los fundamentos considerados por el directorio u órgano equivalente para evaluar la conformación de comités o instancias similares deberán están debidamente documentados.

i) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio u órgano equivalente y los comités, así como las políticas y los procedimientos mencionados previamente. Todo el material que se elabore o presente al directorio u órgano equivalente o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.

D.2. POLÍTICAS Y PROCEDIMIENTOS

Las entidades deberán elaborar y poner en práctica de manera formal, políticas y procedimientos de gestión de riesgos y control interno que contemplen los riesgos asociados al enrutamiento de órdenes.

La función de gestión de riesgos será la responsable de asegurar la elaboración de la totalidad de las políticas y los procedimientos por parte de los encargados de las distintas áreas generadoras de riesgos; y de la exactitud, integridad y actualización de tales políticas y procedimientos.

Las políticas y procedimientos establecidas deberán cumplir con los siguientes aspectos generales:

a) Deberán guardar relación con el número o tipo de clientes, y el volumen de operaciones efectuadas, y respecto de cada uno de los negocios o actividades que se desarrolle.

b) Las políticas deberán exponer los principios generales y directrices establecidas por el directorio u órgano equivalente para orientar las actividades de la organización.

c) Los procedimientos deberán definir cómo llevar a cabo un proceso, con el fin de asegurar el cumplimiento de las políticas aprobadas por el directorio, incorporando, al menos: la descripción de las actividades principales que lo componen y la identificación de sus responsables; determinación de los responsables de supervisar y controlar el resultado de las actividades ejecutadas; documentación que evidencie la ejecución de las actividades que conforman los procedimientos; definición y descripción de los controles asociados a dichas actividades. En el caso de actividades externalizadas, siempre deberá existir una persona responsable dentro de la organización respecto al control de estas.

d) Las políticas, procedimientos y mecanismos de control deberán estar formalmente establecidos y documentados.

D.2.1. POLÍTICAS Y PROCEDIMIENTOS DE GESTIÓN DE RIESGOS Y CONTROL INTERNO

Sin perjuicio de lo anterior, las políticas y procedimientos deberán abordar como mínimo los siguientes aspectos:

a) Conflictos de intereses

Las entidades deberán definir políticas y procedimientos que especifiquen los métodos según los cuales se identificarán, manejarán y vigilarán todos los potenciales conflictos de intereses inherentes a los servicios ofrecidos por ella. Las políticas y procedimientos deberán considerar la identificación, la prevención y monitoreo de los conflictos que puedan surgir entre el servicio de enrutamiento de órdenes y sus clientes, así como de otros productos ofrecidos por la entidad, según le permita la legislación y normativa vigente.

b) Confidencialidad de la información

Las entidades deberán definir políticas destinadas a resguardar la naturaleza confidencial de las órdenes pendientes de ejecución de los clientes, debiendo cumplir con todas las disposiciones legales al efecto, en particular, aquellas que establece la ley N°19.628 sobre protección de la vida privada.

Las políticas deberán incluir el consentimiento para el uso de la información por parte de los clientes, de acuerdo con la ley N°19.628 sobre protección de la vida privada, asegurando la protección de los datos contra el acceso y la divulgación no autorizados y los medios para proteger la privacidad personal y la información reservada.

c) Información al inversionista

La entidad deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los productos o servicios ofrecidos, según lo dispuesto en el artículo 28 de la ley N°21.521.

Estas políticas deberán especificar, al menos, la información que debe ser conocida por los clientes de acuerdo con la Sección III de esta normativa, y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad controlará el cumplimiento de estas disposiciones.

d) Cumplimiento de requisitos legales y normativos de funcionamiento

Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.

Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a esta Comisión.

D.2.2. RIESGO OPERACIONAL

Sin perjuicio de las políticas mínimas que deban implementar las entidades en virtud de la sección anterior, éstas deberán observar los siguientes lineamientos en términos de seguridad de la información y ciberseguridad, adaptándolas según su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) La capacitación del personal en la materia, de manera que sea consciente de los riesgos de seguridad de la información y ciberseguridad y contribuya a una adecuada gestión de éstos.

b) Resguardo de la información de sus clientes:

   1) Implementar un inventario de esos activos de información, incluyendo una clasificación de estos. Esta clasificación deberá considerar dimensiones tales como disponibilidad, confidencialidad e integridad de los activos de información.

   2) Implementar un inventario de servicios relacionados con los activos de información.

   3) Implementar controles de acceso a las instalaciones, infraestructuras de negocios y sistemas de información.

   4) Implementar herramientas de registro, control y monitoreo de la actividad de los usuarios de sistemas.

c) Implementar controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por el personal, y herramientas de gestión de la ciberseguridad tales como programas de gestión de parches de software y firmware, protección de redes ante ataques por medio de firewalls, sistemas de prevención de intrusos, elevación de privilegios, gestión de identidades y acceso físico y lógico, mecanismos de control de identidad para evitar suplantación de terceros, entre otras.

d) Gestionar las condiciones ambientales para la localización segura de los equipos y herramientas de la entidad.

e) Procedimientos de identificación de amenazas de ciberseguridad tales como phishing, malware, inyección de código malicioso, entre otros.

f) Procedimientos de respuesta y recuperación ante incidentes operacionales, los que deberán considerar la recuperación oportuna de funciones críticas; los procesos de respaldo y soporte; los activos críticos de información previamente definidos; y la interdependencia con terceros.

D.3. GESTIÓN DE RIESGOS

D.3.1. FUNCIÓN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos es la instancia responsable del monitoreo de los controles definidos en las políticas y los procedimientos de gestión de riesgos y control interno de la entidad. Esta función deberá reportar directamente al directorio u órgano equivalente.

De acuerdo con el literal D.4. de esta Sección, la función de gestión de riesgos podrá ser realizada por una persona o unidad interna o, en ciertos casos, por la alta administración de la entidad. También podrá ser ejercida por una unidad de gestión de riesgos corporativa en caso de que la entidad pertenezca a un grupo empresarial. Para todos los efectos, si la función es ejercida por una unidad de gestión de riesgos corporativa, en caso de que la entidad pertenezca a un grupo empresarial, se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, la entidad será siempre responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Asimismo, la función de gestión de riesgos será responsable de la realización de actividades para monitorear el cumplimiento de las políticas definidas por la entidad.

Adicionalmente, deberá adoptar las medidas que permitan garantizar el debido cumplimiento de las disposiciones contenidas en las leyes y normativas, y en lo específico, en lo relativo al debido manejo de materias tales como actividades prohibidas, conflictos de intereses, eventualidad de fraude, y otros delitos o infracciones.

Con objeto de implementar lo anteriormente señalado, la función de gestión de riesgos deberá:

a) Verificar la existencia de las políticas y procedimientos mínimos descritos en el literal D.2 anterior.

b) Emitir un informe, al menos con una periodicidad semestral, al directorio u órgano equivalente para documentar las instancias de incumplimientos detectados, causas que los originaron, medidas adoptadas y efectividad de dichas medidas.

c) Proponer cambios en las políticas y en los procedimientos de gestión de riesgos en función de las deficiencias encontradas en sus actividades de control.

d) Elaborar un plan anual que se refiera a la naturaleza, el alcance y oportunidad de las actividades que la función de gestión de riesgos desarrollará. Este plan deberá ser aprobado por el directorio u órgano equivalente. En todo caso, dicho plan deberá ser actualizado cada vez que se produzcan cambios significativos tales como cambios en condiciones del entorno económico y mercados en que opera la entidad, introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la entidad.

D.3.2. PLAN DE GESTIÓN DE RIESGOS

La función de gestión de riesgos estará a cargo de la elaboración de un plan de gestión de riesgos que incluirá las estrategias de mitigación de riesgos y la planificación de contingencias en relación con los principales riesgos, los que, como mínimo deben contemplar los riesgos provenientes de conflictos de intereses y los riesgos de seguridad de la información y ciberseguridad.

El directorio u órgano equivalente deberá aprobar el plan de gestión de riesgos al menos anualmente, con el fin de reflejar cambios significativos experimentados en la estrategia de negocios de la entidad o cambios en las condiciones de mercado. La función

de gestión de riesgos controlará que se dé cumplimiento al plan de gestión de riesgos y a sus respectivos procedimientos.

La elaboración de estrategias de mitigación de riesgos y planificación de contingencias considerará lo siguiente:

a) Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad, y los respectivos responsables de dichos procesos (mapa de procesos).

   La función de gestión de riesgos, en conjunto con los encargados de los procesos principales, deberá identificar formalmente los riesgos inherentes a los que se expone la entidad en el desarrollo de sus actividades.

b) Medición de los riesgos inherentes identificados en las actividades efectuadas por la entidad.

c) Definición de los mecanismos de control para mitigar los riesgos inherentes identificados. Al respecto, dichos mecanismos de control deberán considerar:

   1) Descripción de cada control y su objetivo.

   2) Identificación de los responsables del control formalmente designados para esos efectos.

   3) Calificación de la efectividad de los controles para la mitigación de los riesgos inherentes, por una instancia independiente del responsable de estos.

d) Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al directorio u órgano equivalente y a todas las partes interesadas.

e) Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos y financieros que vaya enfrentando la entidad, cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales.

D.4. PROPORCIONALIDAD

En línea con lo establecido en los artículos 1 y 12 de la ley N°21.521, las entidades podrán adaptar las disposiciones de esta Sección IV.D, conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos.

Sin perjuicio de lo señalado anteriormente, la Tabla 4 describe los requisitos específicos para las entidades que presten el servicio de enrutamiento de órdenes.

La proporcionalidad se aplicará en función de si tienen menos o más de 100 clientes activos en Chile.

Tabla 4. Proporcionalidad para la prestación del servicio de enrutamiento de órdenes

Características del prestador de enrutamiento de órdenes	Políticas	Función de gestión de riesgos
Menos de 100 clientes activos	Se exime de todos los requisitos de esta Sección IV.D	
100 o más clientes activos	CI, CINF, II, RLN.	No especializada

Donde,

a) CI: Conflictos de intereses.

b) CINF: Confidencialidad de la información.

c) II: Información al inversionista.

d) RLN: Cumplimiento de requisitos legales y normativos de funcionamiento.

e) No especializada: La función de gestión de riesgos podrá ser ejercida por algún integrante de la alta administración de la entidad.

La función de gestión de riesgos podrá ser no especializada, es decir, podrá ser ejercida por la alta administración, debiendo reportar directamente al directorio u órgano equivalente

Cuando una entidad alcance los 100 clientes activos en Chile, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de gobierno corporativo y gestión integral de riesgos correspondientes.

Una vez alcanzado ese número, las entidades deberán cumplir con las exigencias de gobierno corporativo y gestión integral de riesgos. Para volver a estar exentas de los requerimientos, las entidades deberán mantenerse por más de 6 meses bajo el umbral de clientes señalado y solicitar autorización de la Comisión.

E. INTERMEDIACIÓN Y CUSTODIA DE INSTRUMENTOS FINANCIEROS

E.1. RESPONSABILIDAD DEL DIRECTORIO U ÓRGANO EQUIVALENTE

El Directorio u órgano equivalente es el principal responsable de que la entidad esté adecuadamente organizada, y de la implementación y funcionamiento del sistema de control interno y gestión de riesgos de la entidad. También deberá promover que tanto la entidad como sus funcionarios se atengan a los procedimientos y normas definidos.

Para esos efectos, el directorio u órgano equivalente deberá dar cumplimiento, al menos, a los principios y elementos de gestión de riesgos que se señalan a continuación:

a) Aprobar el apetito a los riesgos identificados, verificando que las definiciones pertinentes permitan a la entidad cumplir con sus responsabilidades legales, objetivos estratégicos y ser sostenible en el tiempo.

b) Aprobar políticas de gestión de riesgos que sean coherentes con los objetivos estratégicos, el marco regulatorio, los valores organizacionales y el apetito al riesgo definido y la utilización de buenas prácticas en materia de gestión de riesgos asociados a las entidades que prestan servicios de intermediación y/o custodia de instrumentos financieros.

c) Aprobar el código de ética, que dé cuenta de los valores y principios organizacionales y establezca directrices en el actuar del personal de la entidad.

d) Contar con un Comité de Gestión de Riesgos u otra instancia similar. Sin perjuicio de ello, el directorio u órgano equivalente deberá evaluar la pertinencia de conformar comités u otras instancias, que le permitan tratar y monitorear aspectos relevantes de los negocios, referidos a materias tales como Auditoría, Lavado de Activos, Inversiones, Nuevos Productos, Continuidad del Negocio, Seguridad de la Información y Ciberseguridad, entre otros. Los fundamentos de las actuaciones considerados por el directorio u órgano equivalente para evaluar la conformación de comités o instancias similares deberán estar debidamente documentados.

e) El directorio u órgano equivalente establecerá los procedimientos para la conformación y funcionamiento de los comités o instancias similares, los cuales deberán quedar debidamente documentados, como también sus actuaciones. No obstante. Sin perjuicio de ello, los Comités de Gestión de Riesgos y de Auditoría (éste último, en caso de ser constituido) deberán estar integrados al menos por un integrante del directorio u órgano equivalente. Ningún director (o miembro del órgano equivalente) podrá ser parte del Comité de Gestión de Riesgos y del Comité de Auditoría al mismo tiempo.

f) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del directorio u órgano equivalente y los comités, así como las políticas mencionadas previamente. Todo el material que se elabore o presente al directorio u órgano equivalente o los comités, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de esta Comisión.

g) Aprobar los planes anuales de las funciones de gestión de riesgos y de auditoría interna, y estar en conocimiento, en forma oportuna, de su cumplimiento y de los informes que elabore.

h) Evaluar periódicamente la suficiencia de recursos de las funciones de gestión de riesgos y de auditoría interna, para lo cual deberá tener en consideración la cobertura del trabajo de ellas, aprobando la asignación de los recursos necesarios y monitoreando el grado de cumplimiento del presupuesto asignado a tal fin.

i) Conocer y comprender los riesgos inherentes a los negocios y actividades que desarrolla la entidad.

j) Establecer una estructura organizacional adecuada, consistente con el volumen y complejidad de las operaciones y que contemple una apropiada segregación de funciones.

k) Aprobar y revisar al menos una vez al año, o con una mayor frecuencia si es necesario, las políticas de control interno y gestión de riesgos.

l) Velar por la existencia de un adecuado diseño, implementación y documentación de políticas para:

   1) Los distintos tipos de operaciones y actividades que realiza la entidad en el desarrollo de su giro.

   2) El manejo de información confidencial.

   3) La resolución de conflictos de intereses entre la entidad, o sus empleados, y sus clientes.

   4) Para los prestadores del servicio de intermediación de instrumentos financieros, el conocimiento de los clientes, de sus necesidades y objetivos de inversión, y la entrega de información periódica a los mismos, al objeto de no recomendarles u ofrecerles inversiones en instrumentos o activos que no correspondan a las necesidades, expectativas y disposición al riesgo manifestadas por ellos, en conformidad a las disposiciones establecidas en el artículo 28 de la ley N°21.521.

   5) Disponer de controles que eviten la realización de actividades u operaciones prohibidas.

   6) Prevenir, detectar y evitar la realización de operaciones vinculadas al lavado de activos, financiamiento del terrorismo y financiamiento de armas de destrucción masiva, de acuerdo con las disposiciones legales establecidas en la ley N°19.913.

   7) Incorporar un nuevo producto o servicio.

m) Aprobar los sistemas y metodologías de medición y control de los distintos tipos de riesgos que enfrenta la entidad.

n) Aprobar políticas para el tratamiento de excepciones a los límites de exposición a los diversos riesgos.

o) Aprobar un documento donde consten las políticas de gestión de riesgos y asegurarse de su permanente revisión y actualización.

p) Velar por la existencia de una instancia encargada de la función de gestión de riesgos y asegurarse de su independencia y adecuado funcionamiento.

q) Velar por la existencia de una instancia encargada de la función de auditoría interna y asegurarse de su independencia y adecuado funcionamiento.

r) Velar porque la entidad cuente con el recurso humano calificado, con el fin de que las actividades de intermediación y/o custodia de instrumentos financieros se desarrolle bajo altos estándares de profesionalismo e idoneidad, con apego a las disposiciones legales y normativas vigentes.

s) Implementar políticas de remuneración y compensación para quienes presten servicios a la entidad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de la propia entidad y de quienes asesoran o mantienen relaciones comerciales con clientes.

t) Velar por la implementación de un sistema de información para el desarrollo de las actividades de la entidad, el control y gestión de riesgo.

u) Definir un proceso adecuado de difusión de una cultura de gestión de riesgos en toda la organización.

v) Establecer un mecanismo efectivo para la recepción, gestión y resolución de reclamos internos o externos y denuncias de incumplimiento al código de ética, de manera que permitan resguardar la reserva de quien lo formula. El directorio u órgano equivalente deberá mantenerse informado de las denuncias y reclamos relevantes.

w) Tomar conocimiento de los reportes o informes emitidos por las funciones de gestión de riesgos y de auditoría interna.

x) Contar con un programa de mejoramiento continuo del sistema de control interno y gestión de riesgos, incluyendo programas de capacitación al personal de la entidad, a objeto de gestionar con mayor eficacia los riesgos que se presentan en el desarrollo de las actividades de la entidad.

E.2. GESTIÓN DE RIESGOS

Las entidades deberán implementar un sistema de gestión de riesgos adecuado a la naturaleza, volumen y complejidad de sus operaciones. El referido sistema debe tener como propósito gestionar eficazmente los riesgos financieros, operacionales y de cumplimiento normativo que se presentan en los negocios y actividades que realizan en el desarrollo de su giro, como también aquéllos que pueden afectar los intereses y activos de los clientes.

En consecuencia, el sistema de gestión de riesgos debe considerar al menos las siguientes actividades:

a) Identificación de procesos en los que se descomponen las actividades efectuadas por la entidad (mapa de procesos) a través de:

   1) Una descripción de las actividades y negocios principales;

   2) Identificación de los responsables de efectuar dichas actividades, así como de su supervisión; y

   3) La documentación que evidencia dicha ejecución y supervisión.

b) Identificar formalmente los riesgos a los que se expone en el desarrollo de sus negocios y actividades, en los procesos y sistemas que utiliza.

c) Determinar los niveles de apetito al riesgo en relación con sus objetivos y a la protección de los activos e intereses de los inversionistas.

d) Establecer controles tendientes a mitigar los riesgos identificados.

e) Monitorear las alertas definidas, el cumplimiento de los límites y controles establecidos o si se han seguido los procedimientos formales de excepción.

f) Establecer un sistema eficaz de comunicaciones que asegure que la información relevante para la gestión y control de riesgos llega en forma veraz, suficiente y oportuna al directorio u órgano equivalente y otras instancias responsables.

E.2.1. FUNCIÓN DE GESTIÓN DE RIESGOS

La instancia encargada de la función de gestión de riesgos deberá estar adecuadamente segregada de las áreas generadoras de riesgos y de auditoría interna, siendo responsables ante directorio u órgano equivalente. La función de gestión de riesgos deberá ser desarrollada por personal con experiencia y conocimientos comprobables en marcos de referencia o estándares de gestión de riesgos y de los riesgos específicos que la entidad enfrenta en el desarrollo de su negocio.

La función de gestión de riesgos podrá ser realizada por una persona o unidad interna de acuerdo con la sección E.6 siguiente. Dicha función deberá ser independiente de las áreas operativas y de negocios de la entidad y de la instancia encargada de la función de auditoría interna, con reporte directo al directorio u órgano equivalente.

En el caso que la entidad pertenezca a un grupo empresarial, la función de gestión de riesgos podrá ser ejercida por la unidad de riesgos corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que ejercerá la función de riesgos, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación. Para todos los efectos, si la función es ejercida por una unidad de gestión de riesgos corporativa, en caso de que la entidad pertenezca a un grupo empresarial, se considerará realizada por una unidad interna.

Sin perjuicio de lo anterior, la entidad será siempre responsable de la función de gestión de riesgos aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

La instancia encargada de la función de gestión de riesgos al menos deberá:

a) Desarrollar las actividades señaladas en el literal E.3 siguiente.

b) Proponer políticas y procedimientos para la gestión de riesgos al directorio u órgano equivalente, consistentes con la estrategia de negocios y la protección de los activos e intereses de los clientes.

c) Analizar los riesgos asociados a los cambios en las condiciones del entorno económico, de la industria y de los mercados en los que opera la entidad y sus efectos en la posición de riesgos.

d) Evaluar permanentemente si las políticas y procedimientos de la entidad para gestionar sus riesgos se encuentran actualizados, si son adecuados para la entidad y si éstos se recogen apropiadamente en el documento que contiene las políticas y procedimientos de gestión de riesgos.

e) Establecer procedimientos para que el personal esté en conocimiento de los riesgos, los mecanismos de mitigación y las implicancias del incumplimiento de las políticas y procedimientos de control.

f) Efectuar seguimiento permanente al cumplimiento de los límites de exposición al riesgo y de las medidas correctivas que se hubieren definido para las deficiencias identificadas.

g) Emitir un informe al directorio u órgano equivalente, al menos con una periodicidad trimestral, sobre los incumplimientos detectados en las políticas y procedimientos de gestión de riesgos, causas que los originaron, medidas adoptadas y niveles de exposición al riesgo de la entidad.

h) Emitir un informe al cierre de cada ejercicio anual, destinado al directorio u órgano equivalente, sobre el funcionamiento del sistema de gestión de riesgos respecto del ejercicio que se informa, en el que se pronuncie acerca del funcionamiento de las alertas e indicadores; de la oportuna identificación de eventos relevantes del periodo, debilidades detectadas y mejoras aplicadas al sistema, entre otros aspectos.

i) Proponer un plan anual de actividades para el ejercicio siguiente, el cual debe ser aprobado por el directorio u órgano equivalente.

j) Monitorear la oportuna corrección de las observaciones por falencias o deficiencias detectadas, tanto interna como externamente, que tengan implicancias en la gestión de riesgos de la entidad.

Los fundamentos que sustenten cualquiera de las medidas de este numeral, deberán quedar debidamente documentados en las actas del Directorio u órgano equivalente.

E.2.2. POLÍTICAS Y PROCEDIMIENTOS DE GESTIÓN DE RIESGOS

Las entidades que presten los servicios de intermediación y/o custodia de instrumentos financieros deberán contar con las políticas y procedimientos de gestión de riesgos, debidamente documentados, los cuales deben ser revisados al menos una vez al año y actualizados cada vez que exista un cambio significativo, y deben incorporar los siguientes contenidos mínimos:

a) La matriz de riesgo de la entidad, en la que se identifiquen, para cada una de las líneas de negocio o actividades que desarrolla, los procesos que la integran, los riesgos inherentes asociados a dichos procesos, su importancia relativa en relación con los objetivos de la entidad y la protección de los intereses y activos de los clientes, una evaluación sobre la probabilidad de ocurrencia e impacto de dichos riesgos y los controles mitigantes asociados. El diseño de controles mitigantes deberá considerar:

   1) Una descripción de cada control y de su objetivo.

   2) La identificación de los responsables del control formalmente designados para esos efectos y la oportunidad en que se aplica.

   3) La calificación de la efectividad de los controles.

   4) Los riesgos residuales, esto es, aquella parte de los riesgos inherentes que no puede ser mitigada por los controles correspondientes, ya sea por el tipo de control, la calidad o efectividad del mismo. A partir de los riesgos residuales, se deberá definir su tratamiento teniendo en consideración los niveles de apetito al riesgo.

b) Indicadores claves de riesgos, los que deben ser monitoreados periódicamente para evaluar la exposición a los niveles de apetito al riesgo definidos. Para cada indicador se deberá definir y documentar:

   1) Su metodología de cálculo formal.

   2) Los responsables de su generación, monitoreo y reporte.

   3) Umbrales y niveles de apetito al riesgo para cada indicador

c) Mecanismos de alerta que permitan comunicar oportunamente a las personas responsables toda deficiencia en los controles mitigantes que lleve o pueda llevar a una desviación significativa de los riesgos residuales por encima de los niveles de apetito al riesgo definidos.

d) Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito al riesgo llegue a directorio u órgano equivalente y a todas las instancias pertinentes.

e) La identificación del personal responsable de la aplicación de las políticas y procedimientos, sus cargos y descripción de éstos.

f) La identificación del personal responsable de la supervisión de las personas referidas en el literal precedente, cuyo objetivo es verificar que las políticas y procedimientos se están llevando a cabo de acuerdo con lo definido.

g) En el evento que se definan situaciones de excepción en determinados procedimientos, la identificación de las personas responsables de autorizar tales excepciones.

h) La descripción del proceso de monitoreo, documentación e informe de cumplimiento/incumplimiento de los procedimientos de gestión de riesgo.

i) La descripción del proceso mediante el cual se aprueban, revisan y actualizan los procedimientos y controles y la periodicidad de estas gestiones.

E.3. ORGANIZACIÓN Y CONTROL INTERNO

La organización interna de las entidades dependerá de la naturaleza, tamaño y complejidad de los negocios que realizan y de los riesgos que enfrentan, entre otras variables. No obstante, en su diseño el directorio u órgano equivalente deberá considerar al menos los siguientes aspectos:

E.3.1. POLÍTICAS Y PROCEDIMIENTOS

Las entidades que presten los servicios de intermediación y/o custodia de instrumentos financieros deberán establecer y mantener políticas, procedimientos y controles operativos efectivos en relación con su actividad diaria y respecto de cada uno de los negocios o actividades que desarrollan. Estas políticas, procedimientos y controles deben estar formalmente documentados y deberán referirse al menos a lo siguiente:

a) Conflictos de intereses

Las entidades deberán definir políticas y procedimientos que especifiquen los métodos según los cuales se identificarán, manejarán y vigilarán todos los potenciales conflictos de intereses inherentes a los servicios ofrecidos por ella. Las políticas y procedimientos deberán considerar la identificación, la prevención y monitoreo de los conflictos de intereses que puedan surgir y que puedan afectar a sus clientes.

b) Oferta de productos acorde necesidades, expectativas y disposición al riesgo del inversionista

Las entidades deberán definir políticas y procedimientos tendientes a que los inversionistas inviertan sus recursos en instrumentos financieros, conociendo la información que les permita entender y aceptar el riesgo que están asumiendo y evitando ofrecer productos que no sean acordes a sus necesidades, expectativas y disposición al riesgo, según lo dispuesto en el artículo 28 de la ley N°21.521.

Las entidades deberán contar con procedimientos para asegurar el cumplimiento de la citada obligación. En aquellos casos en que un cliente decida invertir en un instrumento financiero que en opinión de la entidad no sea acorde a las necesidades, expectativas o riesgos que este le haya comunicados por el cliente, la entidad deberá poder acreditar que aquello fue debidamente advertido, en caso de que le sea solicitado por esta Comisión. Para estos efectos, estos procedimientos podrán considerar el requerir a sus potenciales clientes antecedentes tales como, información sobre sus conocimientos y experiencia como inversionista, su situación financiera y objetivos de inversión o ahorro y otra información de esta naturaleza que la entidad considere relevante.

La entidad deberá establecer procedimientos que permitan monitorear el cumplimiento de la política de oferta de productos en forma periódica, incluyendo una descripción de los procedimientos de detección de necesidades, expectativas y disposición al riesgo asociadas a cada inversionista. La entidad podrá establecer excepciones en esta política, en caso de que la oferta de productos esté dirigida a clientes que tengan la calidad de inversionista institucional o inversionista calificado de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N°216.

c) Información al inversionista

La entidad deberá definir políticas y procedimientos que determinen la forma en que se garantizará que los clientes cuenten con información veraz, suficiente y oportuna, relativa a los productos o servicios ofrecidos, según lo dispuesto en el artículo 28 de la ley N°21.521.

Estas políticas deberán especificar, al menos, la información que debe ser conocida por los clientes de acuerdo con la Sección III de esta normativa, y aquella que adicionalmente la entidad estime necesaria que se conozca, así como también la periodicidad establecida para ello. Por su parte, los procedimientos deberán estar referidos a la forma en que la entidad controlará el cumplimiento de estas disposiciones.

d) Metodología de aprobación, evaluación y control de algoritmos

En caso de corresponder, las entidades deberán contar con mecanismos de aprobación, evaluación y control de algoritmos que garanticen su adecuado funcionamiento al otorgar el servicio de intermediación de instrumentos financieros. Estos mecanismos deberán velar porque los algoritmos empleados garanticen que las transacciones se realicen en el interés y la protección de los clientes, acorde con las necesidades, expectativas y disposición al riesgo que éstos les hayan comunicado previamente.

La entidad debe contar con personal capacitado que comprenda el funcionamiento de los algoritmos y la verificación continua de su correcto funcionamiento de sus algoritmos.

e) Garantías

En caso de que las entidades requieran garantías por parte de los inversionistas para realizar operaciones, deberá establecer:

1) La metodología para la valorización de los instrumentos entregados en garantía.
2) La elegibilidad de los instrumentos a entregar en garantías.
3) La revisión periódica de las metodologías.
4) Las pruebas retrospectivas para determinar la suficiencia de las garantías.

Sin perjuicio de lo anterior, esta Comisión podrá solicitar un "informe de procedimiento acordado" por parte de una empresa de auditoría externa para verificar el cumplimiento de estos requisitos, en la medida que durante la actividad de supervisión se hayan identificado deficiencias en dichos procesos, o en los mecanismos de control implementados.

f) Prevención de lavado de activos y financiamiento del terrorismo

Las entidades deberán contar con políticas y procedimientos para el cumplimiento de las disposiciones legales y normativas relativas a la prevención del lavado de activos, financiamiento del terrorismo y financiamiento de armas de destrucción masiva, según lo dispuesto en la ley N°19.913 y en la normativa dictada por la Unidad de Análisis Financiero.

g) Cumplimiento de requisitos legales y normativos de funcionamiento

Se deberán definir políticas y procedimientos que especifiquen la forma en que se monitoreará y garantizará el debido cumplimiento de los requisitos legales y normativos aplicables a la entidad.

Además, se deberá definir procedimientos en caso de presentarse eventos de incumplimiento de los requisitos legales de funcionamiento, los cuales deberán ser informados oportunamente a esta Comisión.

h) Gestión de consultas, reclamos y denuncias

Las entidades deberán definir políticas y procedimientos que les permita gestionar y resolver las consultas, denuncias y reclamos de sus clientes, trabajadores y el público general. Para ello deberá considerar, al menos, un manual que establezca, en términos simples, los antecedentes mínimos que se requerirán para efectuar una consulta, denuncia o reclamo, y que describa cómo utilizar los canales especializados que se hubieren dispuesto para esos efectos. El manual deberá establecer:

1) Procedimiento para resolver las consultas del público que considere los diferentes canales que se disponga para estos efectos. El mecanismo deberá permitir hacer un seguimiento de las consultas efectuadas.

2) Procedimientos que permitan resguardar la reserva de quien formula el reclamo o denuncia.

3) El directorio u órgano equivalente deberá mantenerse informado de los reclamos y denuncias relevantes.

4) Definir claramente cómo se calificará la gravedad o relevancia de la denuncia o reclamo, y cómo se comunicará a las instancias que corresponda, incluyendo al directorio u órgano equivalente en el caso de aquellas más relevantes.

5) Las instancias que participarán en la gestión de las consultas, denuncias o reclamos de acuerdo con la relevancia o la gravedad que se hubiere definido para cada caso. Con todo, la gestión de los reclamos deberá ser efectuada por una unidad independiente del área donde se originaron los mismos.

6) Los tiempos máximos establecidos para gestionar y responder cada consulta, denuncia o reclamo de acuerdo con su gravedad o relevancia.

7) Un registro de las consultas, denuncias y reclamos junto con la gravedad o relevancia asignada y la solución implementada.

8) Definir una instancia encargada de analizar, monitorear y proponer medidas para evitar que las situaciones que generaron las consultas, denuncias o reclamos se repitan.

i) Integridad en las prácticas de custodia

Los prestadores del servicio de custodia de instrumentos financieros deberán implementar políticas y procedimientos que consideren:

1) Los medios de acceso del cliente a los instrumentos financieros y claves criptográficas privadas.

2) El mantenimiento de un registro de custodia con información de operaciones realizadas sobre instrumentos financieros, incluyendo: transacciones efectuadas por el cliente, posiciones mantenidas por el cliente, transferencias y conciliaciones de instrumentos financieros efectuadas por la entidad, cambios en la custodia de claves criptográficas privadas, entre otros. Esta información debe ponerse a disposición del cliente en forma veraz, suficiente y oportuna, de forma tal que el cliente conozca cómo se conservan sus activos y las medidas de salvaguarda de los mismos y de sus claves criptográficas privadas.

3) La segregación de las cuentas y activos de los clientes de los activos de la entidad, de manera que los activos de los clientes estén claramente identificados y no puedan ser reutilizados o prestados sin su consentimiento.

E.4. RIESGO OPERACIONAL

Los intermediarios y custodios de instrumentos financieros, con el objeto de que la entidad desarrolle una adecuada gestión de riesgo operacional, deberán considerar los elementos que se señalan a continuación, adaptándolos de acuerdo a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Las políticas y procedimientos de gestión de riesgo operacional deberán incluir, al menos, los siguientes ámbitos relacionados, descritos en las próximas secciones: seguridad de la información y ciberseguridad, continuidad de negocio; y externalización de servicios. Los ámbitos mencionados deberán ser considerados por la entidad en los informes que realicen las instancias encargadas de la gestión de riesgos y la auditoría interna, según corresponda. Lo anterior, sin perjuicio del cumplimiento de las normativas aplicables a la entidad que requieren la gestión de sus riesgos operacionales. Las políticas y procedimientos de gestión de riesgo

operacional deben estar diseñadas para brindar una seguridad razonable que la entidad pueda desarrollar las operaciones del negocio en forma continua y eficiente, incluso ante la presencia de eventos disruptivos, salvaguardando sus servicios, procesos y activos de información. Estas políticas y procedimientos deben ser establecidas y aprobadas por el directorio, u órgano equivalente, y ser difundidas a todo el personal dentro de la organización. Además, dichas políticas y procedimientos deben establecer los niveles de apetito por riesgo definidos por el directorio u órgano equivalente, que determinará la necesidad de evitar, reducir, transferir o aceptar los riesgos, y acorde con ello, diseñar controles mitigantes.

b) Contar con indicadores claves de medición del riesgo operacional consistentes con la metodología de evaluación y monitoreo de riesgos integrales de la entidad, permitiendo al mismo tiempo establecer niveles de alerta y evaluar la eficacia de los controles adoptados. El detalle de cálculo de estos indicadores deberá ser incluido expresamente en las políticas y procedimientos de gestión de riesgo operacional de misma la entidad.

E.4.1. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

E.4.1.1 DISPOSICIONES GENERALES

En el ámbito de seguridad de la información y ciberseguridad, la gestión de riesgo operacional deberá incluir los siguientes elementos aplicables a todas las entidades adaptándolos de acuerdo a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política de seguridad de la información y ciberseguridad que considere al menos lo siguiente:

1) Procedimientos para la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad, de forma resguardar la disponibilidad, confidencialidad e integridad de los activos de información.

2) Niveles de apetito por riesgo en materia de seguridad de la información y ciberseguridad.

3) Principales funciones y responsabilidades sobre la materia.

4) Procedimientos para la evaluación de los riesgos de seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, servicios, sistemas, emprender nuevas actividades o definir nuevos procesos.

5) Las políticas de seguridad de la información y ciberseguridad formarán parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizadas y aprobadas al menos anualmente por el directorio, u órgano equivalente, o con una periodicidad mayor en caso de cambios significativos.

b) Contar con una política de tecnologías de información y comunicación (TIC), que considere al menos lo siguiente:

   1) Definición de las líneas de responsabilidad en cuanto a la gestión de los activos de información en la entidad.

   2) Definición de los procesos TIC que aseguren un adecuado diseño, transición, operación de servicio y gestión a través de sus activos de información.

   3) Definición de los procedimientos que se deberán seguir para la adecuada gestión de los procesos TIC.

c) Definición del perfil y número necesario de personas con conocimientos o experiencia comprobables en estándares de seguridad de la información y ciberseguridad.

d) Establecimiento de los procedimientos para que el personal de la entidad, incluyendo el directorio u órgano equivalente, contribuya a una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad, de conformidad con sus roles y responsabilidades, mediante la implementación de:

   1) Procedimientos de difusión, capacitación y concientización que traten sobre los riesgos, vulnerabilidades y amenazas a la seguridad de la información, la gestión de estos, y las lecciones aprendidas respecto de los incidentes en esta materia, para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de dichos riesgos.

   2) Acuerdos contractuales con los empleados que establezcan sus responsabilidades y las de la entidad en materia de seguridad de la información y ciberseguridad, incluyendo sanciones.

e) Generación de acuerdos contractuales para la revocación de derechos de acceso a información y destrucción de activos de información como parte del proceso de cambio de posición o desvinculación de un empleado.

f) Auditoría de los procesos de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

g) Disposición de procedimientos que le permitan al directorio u órgano equivalente mantenerse informado en forma oportuna y periódica sobre el sistema de gestión de la seguridad de la información y ciberseguridad. Deberá dejarse constancia del reporte de la información de estas materias en las respectivas actas del directorio u órgano equivalente y los comités que se conformen para revisar estas materias.

E.4.1.2 PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La entidad deberá considerar los siguientes procedimientos, y adaptarlos en relación con su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

d) Identificación

1) Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.

2) Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad.

3) Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión, clasificados desde una perspectiva de disponibilidad, confidencialidad e integridad.

4) Implementar un inventario de activos de información que permita conocer las principales características del activo, considerando al menos: hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, estaciones de trabajo, servidores, medios de almacenamiento y documentación física.

5) Actualizar el inventario de activos de información en forma continua, para lo cual los distintos procesos de gestión de riesgo operacional deberán reportar la información que pueda tener efecto en dicho inventario.

e) Protección y Detección

1) Controles de acceso a las instalaciones e infraestructuras de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.

2) Controles de acceso a los sistemas, de manera de mitigar los riesgos de suplantación o uso indebido por parte de terceros. En el caso de instalaciones, infraestructuras y sistemas críticos, se deberá privilegiar el uso de mecanismos de autenticación multifactor.

3) Implementación de herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios y administradores de sistemas y activos de información, incluyendo usuarios de alto privilegio.

4) Procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, servicios de red, sistemas operativos, bases de datos y aplicaciones de negocios en función de los roles y responsabilidades del personal y sólo lo estrictamente necesario para que éste cumpla sus funciones actuales.

5) Controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por personal interno o externo, así como también los dispositivos Internet de las Cosas (IoT).

6) Mecanismos de control y monitoreo de las condiciones ambientales para la localización segura para los equipos y herramientas, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de incendios y desastres naturales.

7) Procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:

   i) Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, anti-spyware y anti-malware, entre otros.

   ii) Un proceso de gestión de la configuración de los sistemas y activos de información.

   iii) Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:

      a) Las disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos de los inversionistas, incluyendo acuerdos de no divulgación.

      b) Los procesos de administración de respaldos que aseguren la disponibilidad, confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección E.4.2 siguiente. Los respaldos de la información se debiesen mantener en lo posible en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

      c) Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.

      d) Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.

f) Respuesta y Recuperación

1) La entidad deberá contar con procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, considerando:

   i) Una instancia de alto nivel definida por el directorio u órgano equivalente encargada de la gestión de incidentes de seguridad de la información y ciberseguridad.

   ii) Procedimientos de respuesta y recuperación ante incidentes, aprobados por el directorio u órgano equivalente, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información críticos y las interdependencias con terceros en caso de incidentes. Dichos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección IV.E de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones. Los procedimientos de respuesta y recuperación ante incidentes deberán actualizarse al menos anualmente, cada vez que se registran cambios en los activos de información o se produzcan incidentes que amenacen la seguridad de estos.

   iii) Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad, y a esta Comisión, de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección V.E de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.

2) Procedimientos para el desarrollo, adquisición y actualización de la infraestructura tecnológica de la entidad, que consideren:

   i) Las necesidades de infraestructura tecnológica de la entidad.

   ii) Implementación de un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información producto de la introducción de nuevos productos, sistemas y actividades sean efectuadas y monitoreadas de manera segura y controlada.

   Como parte de este proceso, previo al paso de producción de un servicio o activo de información se deben realizar pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas, con el propósito de asegurar que no hubiere un impacto adverso en la seguridad de la información y en las operaciones del negocio.

iii) Implementación de un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas que no generen efectos adversos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial

iv) Implementación de un proceso de gestión de actualizaciones de seguridad de software (parches).

3) La entidad deberá contar con un procedimiento para el mejoramiento continuo de las herramientas, procedimientos y controles de seguridad de la información y ciberseguridad que considere:

i) Recolectar y analizar información sobre el funcionamiento de activos de información.

ii) Analizar los incidentes de seguridad de la información y ciberseguridad y la efectividad de las medidas adoptadas para resolverlo.

iii) Ejecutar pruebas para identificar amenazas y vulnerabilidades en la seguridad de la información:

a) Las pruebas deberán ser realizadas con una periodicidad no mayor a un año, y ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

Las pruebas deberán estar basadas en escenarios de riesgo planificados y diseñados para demostrar que los mecanismos y herramientas implementados para preservar la seguridad de la información cumplen adecuadamente con su objetivo, incluyendo ataques cibernéticos.

b) Los resultados de las pruebas realizadas deberán ser reportados al directorio u órgano equivalente, incluyendo recomendaciones de mejora en las herramientas, procedimientos y controles.

E.4.2. CONTINUIDAD DEL NEGOCIO

E.4.2.1 DISPOSICIONES GENERALES

En el ámbito de continuidad de negocio, la gestión de riesgo operacional deberá tomar en cuenta los siguientes elementos y adaptarlos de acuerdo con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política de continuidad de negocio que considere a lo menos lo siguiente:

1) Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Para las entidades clasificadas en el Bloque 3, estos procedimientos se deberán referir al menos a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).

2) Establecer las principales funciones y responsabilidades sobre la materia, en especial, cuáles serán las instancias encargadas de definir, diseñar, ejecutar y mejorar los procedimientos y metodologías para la gestión de continuidad de negocio. Las políticas de continuidad del negocio formarán parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizada y aprobada al menos anualmente por el directorio u órgano equivalente o con una periodicidad menor en caso de cambios significativos.

b) Contar con personas con conocimientos o experiencia comprobables en estándares de continuidad de negocio y experiencia en la gestión de los riesgos asociados, cuyas actividades principales serán el desarrollo y mejora de las políticas, procedimientos y controles para la gestión de continuidad de negocio.

c) Políticas y procedimientos de capacitación y concientización para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de los riesgos del sistema de continuidad de negocio.

d) El directorio u órgano equivalente deberá mantenerse informado sobre la gestión de continuidad de negocio, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

E.4.2.2 PROCEDIMIENTOS PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS

Las entidades que presten los servicios considerados en esta letra E deberán implementar los siguientes elementos para la gestión de la continuidad de negocios, adaptándolos en relación con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Disponer de un sitio secundario físico o en la nube que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal, permitiendo restablecer los procesos de mayor relevancia del negocio, tales como plataformas, infraestructura, sistemas y procesamiento de datos.

b) Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres, aprobado anualmente por el directorio u órgano equivalente, que contenga:

1) Los procedimientos para la gestión de eventos de continuidad, con un nivel de detalle que permita a las distintas instancias afectadas determinar las actividades a desarrollar en cada escenario definido.

2) Los criterios para la activación del Plan y para la vuelta a la normalidad. Esto incluye evaluar oportunamente los riesgos asociados a la continuidad de negocios que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

3) Roles y responsabilidades del personal.

La periodicidad de actualización de este Plan podría ser mayor dependiendo de la normativa propia de la entidad, o a requerimiento de esta Comisión.

c) Las entidades clasificadas en el Bloque 3 deberán realizar o actualizar, al menos anualmente, ante eventos que amenacen la continuidad de las operaciones del negocio, un BIA con el objeto de identificar los procesos de mayor relevancia para la continuidad de negocio, el impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de estos. El BIA deberá realizarse a nivel estratégico, táctico y operativo. De esos procesos, y considerando los niveles de apetito por riesgo definidos, se deberá determinar:

   1) Los tiempos máximos tolerables de interrupción (MTPD por sus siglas en inglés);

   2) Los tiempos objetivos de recuperación (RTO por sus siglas en inglés);

   3) Los puntos objetivos de recuperación (RPO por sus siglas en inglés);

   4) Los niveles mínimos aceptables de operación; y

   5) Los recursos humanos, tecnológicos y de infraestructura e información necesarios para su continuidad y recuperación.

   Los resultados del BIA deberán ser aprobados por el directorio u órgano equivalente.

d) Las entidades clasificadas en el Bloque 3, definido más abajo, deberán realizar o actualizar, al menos anualmente, una evaluación de impacto de riesgos (RIA) que permita identificar y analizar los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas; y la falta de provisión de los servicios críticos contratados a proveedores.

e) Las entidades clasificadas en el Bloque 3, en consideración de los resultados del BIA y el RIA, deberán definir una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad.

f) Se deberá implementar un Plan de Crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante respecto del evento de continuidad, las medidas adoptadas para resolverlo y para coordinar una respuesta adecuada dentro de los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA (entidades clasificadas en el Bloque 3 al que se refieren las secciones anteriores).

g) Contar con un procedimiento para el mejoramiento continuo de las políticas, planes y procedimientos de continuidad del negocio con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

h) El Plan de Continuidad de Negocio y Recuperación de Desastres deberá ser probado anualmente, de forma de asegurar que es adecuado y efectivo, sin perjuicio de que esta Comisión pueda solicitar una periodicidad diferente para las entidades clasificadas en el Bloque 3. Estas pruebas deberán considerar a lo menos lo siguiente:

   1) Deberán ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

   2) Estar basadas en escenarios de riesgo que se asimilen a eventos reales incluyendo escenarios severos pero plausibles. Lo anterior, para demostrar que los procedimientos de continuidad de negocio funcionarán en caso de ser necesarios, incluyendo ataques cibernéticos, desastres naturales y contingencias sanitarias.

   3) Las entidades del Bloque 1 y 2, definidas en las secciones anteriores, podrán utilizar indicadores de continuidad del negocio distintos de los establecidos en la Sección B.2.c.

Se deberán emitir reportes de los resultados de las pruebas realizadas al directorio u órgano equivalente, que contengan recomendaciones y acciones para implementar mejoras al Plan de Continuidad de Negocio y Recuperación ante Desastres.

E.4.3. EXTERNALIZACIÓN DE SERVICIOS

E.4.3.1 RIESGOS DE EXTERNALIZACIÓN

Los servicios prestados por proveedores, relacionados con el cumplimiento normativo, la continuidad del negocio, la seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante, deberán ser considerados en los procesos de gestión de riesgo operacional de la entidad. En tal sentido, para la evaluación de riesgos de contratación de proveedores, se deberán considerar, entre otros, los siguientes riesgos:

1) Riesgo de sustitución: la posibilidad de sustituir o no a un proveedor dentro de un plazo determinado que garantice la continuidad del servicio contratado.

2) Riesgo de intervención: la posibilidad de que la entidad tenga que hacerse cargo de la función contratada.

3) Riesgo de subcontratación: la posibilidad de que el proveedor subcontrate a su vez todo o parte del servicio, reduciendo la capacidad de la entidad de supervisar la función subcontratada.

4) Riesgo asociado a la posibilidad que una entidad contrate uno o varios servicios en un mismo proveedor que sea difícil de sustituir, incrementando la posibilidad de fallas o interrupciones prolongadas.

E.4.3.2 PROCEDIMIENTOS PARA LA GESTIÓN DE SERVICIOS EXTERNALIZADOS

En el ámbito de externalización de servicios, la gestión de riesgo operacional deberá considerar los siguientes elementos y adaptarlos de acuerdo con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política para la externalización de servicios que considere a lo menos lo siguiente:

1) Definir la estructura de gobierno y de los procedimientos a seguir para autorizar y gestionar la externalización de servicios por terceros, incluyendo las líneas de reporte y de responsabilidad.

2) Establecer los objetivos en materia de externalización de servicios.

3) Establecer los niveles de apetito por riesgo en la externalización de servicios y las estrategias de mitigación.

4) Cumplir con las disposiciones en materia de seguridad de la información, ciberseguridad y continuidad de negocios.

5) Establecer los procedimientos para la determinación de los servicios críticos. En tal sentido, para entender como crítico un servicio se deberán tener en cuenta las siguientes consideraciones:

i) El efecto que una debilidad o falla en la provisión o ejecución del servicio tenga sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante.

ii) La complejidad de las funciones comerciales asociadas.

iii) El grado en que el servicio puede transferirse rápidamente a otro proveedor, considerando los costos y el tiempo para hacerlo.

6) Definir los servicios que solo pueden ser externalizados con la aprobación previa del directorio u órgano equivalente.

7) Definir los elementos mínimos que deberá incorporar el contrato de prestación de servicios.

8) Definir los elementos de la gestión de riesgos que no serán aplicados a actividades que por su naturaleza no tengan impacto relevante en la prestación de los servicios.

9) Incluir a las políticas de externalización de servicios como parte de las políticas de gestión de riesgos de la entidad, debiendo ser aprobada y actualizada al menos anualmente por el directorio u órgano equivalente, o con una frecuencia mayor en caso de cambios internos o externos significativos.

10) Considerar los riesgos de sustitución, intervención, subcontratación y concentración de la sección anterior.

b) Establecer procedimientos para la selección, contratación y monitoreo de proveedores que consideren:

1) Una definición de los criterios particulares de contratación, cuando el proveedor se trate de una entidad relacionada. Estos criterios deberán estar destinados a evitar los conflictos de intereses que se pueden presentar.

2) La incorporación al análisis de elementos que permitan llevar a cabo un proceso de debida diligencia, de forma de asegurar que los proveedores tengan una adecuada reputación comercial, solvencia financiera, experiencia y recursos suficientes para garantizar la calidad de la provisión del servicio. En el caso de servicios en los que no se pueda garantizar el pleno cumplimiento de las condiciones mencionadas, como puede ser el caso de servicios de procesamiento de datos realizados en el extranjero, el directorio u órgano equivalente de la entidad deberá revisar y evaluar antecedentes que respalden la calidad del servicio prestado, la solidez financiera del proveedor y la existencia de una adecuada legislación de protección de datos personales en la jurisdicción aplicable, haciéndose responsable por la disponibilidad, confidencialidad e integridad de la información entregada al proveedor contratado.

c) Contemplar en los contratos con los proveedores de servicios externalizados los siguientes contenidos mínimos:

1) Una descripción clara del servicio contratado y el plazo de vigencia.

2) Las obligaciones de prestación del servicio por parte del proveedor, definiendo niveles de servicio acordados. La entidad deberá definir las situaciones que se considerarán graves incumplimientos contractuales y causales de término anticipado del contrato.

3) La obligación de comunicar cualquier acontecimiento que pueda tener un impacto material en la capacidad para llevar a cabo el servicio externalizado.

4) Los requisitos de seguridad de la información, ciberseguridad y continuidad de negocios que deberá cumplir el proveedor, que deben ser concordantes con las disposiciones establecidas en esta materia por la entidad. Los proveedores deberán contar con procedimientos de gestión de incidentes y continuidad de negocios que le permitan seguir brindando los servicios en el evento que se presenten situaciones disruptivas.

5) La documentación de los procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado. En el caso de existir subcontratación en cadena, la entidad deberá verificar el cumplimiento de las condiciones pactadas con el proveedor de servicios inicial y las entidades subcontratadas por este último.

6) Los procedimientos para la evaluación y monitoreo periódico de la calidad de la provisión del servicio externalizado. La entidad podrá pactar con el proveedor la realización de auditorías por terceros designados o por la propia entidad, quien será responsable en última instancia por garantizar la calidad de la provisión del servicio externalizado.

7) Las estrategias para el término de la prestación de servicios externalizados sin perjudicar las operaciones de la entidad, considerando esas situaciones en el Plan de Continuidad del Negocio y Recuperación ante Desastres.

d) Contar con un registro de servicios externalizados, para gestionar los riesgos de subcontratación, que deberá incluir al menos la siguiente información:

   1) Identificación del servicio externalizado, incluyendo una breve descripción del mismo y de los datos involucrados si corresponde a un servicio crítico, si existe subcontratación en cadena, y si se lleva a cabo en la nube.

   2) Identificación del proveedor, incluyendo si corresponde a una entidad relacionada o no.

   3) Fecha de inicio, renovación y término del servicio.

   4) En el caso de servicios de procesamiento de datos, una descripción de los datos y tratamientos que se subcontratan, las medidas de seguridad adoptadas, y la ubicación geográfica del proveedor.

   5) En caso de subcontratación en cadena, se deberá detallar cuáles son las entidades a las que el proveedor subcontrata el servicio, una descripción de los riesgos asociados y si el proveedor realiza un control de la calidad de la provisión del servicio subcontratado en cadena.

e) Monitorear periódicamente que los proveedores cumplen con las condiciones pactadas para garantizar la calidad de la provisión del servicio. La entidad será responsable de la calidad de los servicios externalizados.

f) En el caso de que la entidad decida contratar servicios de acceso y tratamiento de información en la nube, o que el proveedor como parte de la subcontratación en cadena considere los servicios en la nube, se deberá realizar un análisis reforzado de los riesgos inherentes a esos servicios, analizando en particular cómo podría afectarse la disponibilidad, confidencialidad e integridad de la información, y la continuidad de negocio de la entidad. Ese análisis deberá tener en consideración factores tales como:

   1) Las certificaciones independientes respecto a la gestión de la seguridad de la información y la calidad de la prestación del servicio del proveedor.

   2) La celebración del contrato de externalización de servicios directamente entre la entidad y el proveedor, con la finalidad de minimizar los riesgos en este tipo de servicios.

   3) El procesamiento o almacenamiento de información en otras jurisdicciones, y en ese caso la existencia de normas que resguardan la protección de datos personales, la disponibilidad, confidencialidad e integridad de la información y la resolución de contingencias legales.

   4) La existencia de adecuados mecanismos de seguridad del proveedor, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura en la nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la disponibilidad, confidencialidad e integridad de los datos de la entidad.

   5) La utilización de técnicas de encriptación para los datos que la entidad establezca, de acuerdo con su naturaleza y sensibilidad

g) Evaluar que el proveedor de los servicios contratados posea adecuados conocimientos y experiencia.

h) Mantener personal con el debido conocimiento y experiencia para efectuar el control de la prestación de servicios efectuada por sus proveedores. Asimismo, también deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de los servicios contratados.

i) El directorio u órgano equivalente deberá mantenerse informado sobre las materias referidas a la externalización de servicios, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

E.5. FUNCIÓN DE AUDITORÍA INTERNA

La función de auditoría interna deberá contar con personas con experiencia y conocimientos para desarrollar apropiadamente, al menos, las siguientes actividades:

a) Evaluar la adhesión a los objetivos, políticas y procedimientos en materia de control interno de las distintas unidades o áreas de la entidad.

b) Evaluar la efectividad y el cumplimiento de las políticas, procedimientos y controles implementados conducentes a la protección de activos propios y de sus clientes, a la ejecución de órdenes en el interés de los clientes, a la detección de operaciones ilícitas, a garantizar la seguridad de la información, a la protección de la integridad de los sistemas de información, a garantizar el manejo confidencial de la información relativa a sus clientes, al adecuado manejo de los conflictos de intereses con los clientes, entre otros.

c) Evaluar el funcionamiento de la instancia encargada de la función de gestión de riesgos desarrollada en la entidad.

d) Evaluar que la información financiera utilizada para la conducción de los negocios y aquélla utilizada para efectos de control de los riesgos, sea confiable, oportuna, completa e íntegra.

e) Revisar la estructura organizacional para verificar la adecuada segregación de funciones.

f) Verificar el cumplimiento de las disposiciones legales y normativas que le son aplicables a las entidades, sus directivos y empleados, como así también toda documentación interna tal como códigos de ética y manuales operativos

g) Monitorear la oportuna corrección de las observaciones por falencias o deficiencias detectadas en materia de control interno y gestión de riesgo.

Para llevar a cabo estas labores, la función de auditoría interna deberá contar con un plan de revisión anual, debidamente aprobado por el directorio u órgano equivalente y con procedimientos documentados para el desarrollo de estas revisiones.

La función de auditoría interna deberá informar por escrito al directorio u órgano equivalente en forma periódica, al menos semestral, sobre el desempeño de las labores descritas y sobre el cumplimiento de su plan de revisión anual. La función de auditoría deberá ser independiente de las áreas operativas y de negocios de la entidad y de la instancia encargada de la función de gestión de riesgos, con reporte directo al directorio

u órgano equivalente y podrá ser realizada por una persona o unidad interna o externalizada a un tercero, de acuerdo con la Sección E.6 siguiente.

En el caso que la entidad pertenezca a un grupo empresarial, la función de auditoría interna podrá ser ejercida por la unidad de auditoría interna corporativa, en la medida que ésta tenga un conocimiento acabado del marco de gestión de riesgos y ambiente de control de la entidad y que cumpla con los requisitos establecidos en la presente normativa, lo cual deberá ser acordado por el directorio u órgano equivalente. Se deberá considerar la pertinencia respecto a la idoneidad de la unidad respectiva del grupo empresarial que se encargará de la actividad, en relación con el cumplimiento de los requisitos establecidos en esta norma y los conflictos de intereses que pudieran generarse y, de ser el caso, su mitigación y/o eliminación. Para todos los efectos, si la función de auditoría interna es ejercida por una unidad corporativa del grupo empresarial al que pertenece la empresa, con las condiciones señaladas, se entenderá que es ejercida por una unidad interna.

Sin perjuicio de lo anterior, la entidad será la entidad será siempre responsable de la función de auditoría interna aun cuando ésta sea realizada por una instancia perteneciente al grupo empresarial, debiendo revisar y aprobar los informes realizados al respecto, para lo cual deberá hacerse de toda la documentación relevante.

Los informes que se generen producto del plan de revisión anual deberán dirigirse al directorio u órgano equivalente y contener como mínimo el objetivo, el alcance, las situaciones detectadas, la importancia relativa de las mismas y las conclusiones correspondientes. Asimismo, deberán señalar los comentarios de las áreas que han sido objeto de la revisión, las medidas correctivas que se adoptarán y los plazos estimados para ello.

E.6. PROPORCIONALIDAD

En línea con lo establecido en los artículos 1 y 12 de la ley N°21.521, las entidades podrán adaptar las disposiciones de esta Sección IV.E, conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos, de acuerdo con la siguiente clasificación:

a) **Bloque 1**: entidades que tengan un número de clientes activos en Chile menor a 500, y no cumplan ninguna de las métricas de volumen de negocio de las entidades Bloque 2 o 3. Se considerarán clientes activos aquellos que cumplan con las condiciones definidas en el Anexo N°1 de esta normativa.

b) **Bloque 2**: entidades que cumplan alguna de las siguientes condiciones

   i) Tengan un número de clientes activos en Chile entre 500 y 5.000.

   ii) Transacciones promedio diarias en los últimos tres meses (media móvil) entre UF 100.000 y UF 500.000.

   iii) Activos custodiados promedio diarios en los últimos tres meses (media móvil) entre UF 20.000 y UF 100.000.

   iv) Ingresos en los últimos 12 meses (media móvil) entre UF 25.000 y UF 50.000

c) **Bloque 3**: entidades que cumplan alguna de las siguientes condiciones:

i) Más de 5.000 clientes activos en Chile.

ii) Más de UF 500.000 en transacciones promedio diarias en los últimos tres meses (media móvil).

iii) Activos custodiados promedio diarios en los últimos tres meses (media móvil) sobre UF 100.000.

iv) Ingresos en los últimos 12 meses (media móvil) sobre UF 50.000.

En caso de que una entidad sea reclasificada a un bloque superior, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de gobierno corporativo y gestión integral de riesgos correspondientes a dicho bloque. Las entidades podrán ser reclasificadas a bloques inferiores después de un mínimo de 6 meses y con autorización de la Comisión.

Las entidades que clasifiquen dentro de los Bloques 1 o 2 podrán desarrollar la función de auditoría interna por una persona o unidad interna, por un tercero externo.

En caso de que la función de auditoría interna sea realizada por un tercero externo, en ningún caso dicho tercero podrá ejercer la función de auditoría externa en la entidad, debiendo la entidad velar por la adecuada segregación de ambas funciones.

Las entidades que clasifiquen dentro del Bloque 3 deberán desarrollar la función de auditoría interna por una persona o unidad interna.

Tabla 5. Proporcionalidad para la prestación de los servicios de intermediación y/o custodia de instrumentos financieros.

<table>
<tr><th>Bloque</th><th>Políticas</th><th>Función de gestión de riesgos</th><th>Función de auditoría interna</th></tr>
<tr><td>1</td><td>CI, OP, II, ALG, GAR, PLAFT, CUST, RO</td><td rowspan="3">Persona o unidad interna</td><td rowspan="2">Persona o unidad interna o ser realizadas por un tercero</td></tr>
<tr><td>2</td><td>CI, OP, II, ALG, GAR, PLAFT, CUST, RO</td></tr>
<tr><td>3</td><td>CI, OP, II, ALG, GAR, PLAFT, RLN, GCR, CUST, RO</td><td>Persona o unidad interna</td></tr>
</table>

Donde,

- CI: Conflictos de intereses.
- OP: Oferta de productos acorde a las necesidades, expectativas y disposición al riesgo del inversionista.
- II: Información al inversionista.
- ALG: Metodología de aprobación, evaluación y control de algoritmos.
- GAR: Garantías.

- PLAFT: Prevención de lavado de activos y financiamiento del terrorismo.
- RLN: Cumplimiento de requisitos legales y normativos de funcionamiento.
- GCR: Gestión de consultas, reclamos y denuncias.
- CUST: Integridad en las prácticas de custodia.
- RO: Riesgo operacional.

E.7. OTRAS DISPOSICIONES

Esta Comisión podrá solicitar un "informe de procedimiento acordado" a una empresa de auditoría externa registrada en esta Comisión relativo al cumplimiento de las políticas, procedimientos y controles de riesgos las entidades.

E.8. INFORMACIÓN DE INCIDENTES OPERACIONALES

E.8.1. REGISTRO Y COMUNICACIÓN DE INCIDENTES OPERACIONALES

a) Los intermediarios y custodios de instrumentos financieros, pertenecientes al Bloque 3, deberán comunicar a esta Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en servicios importantes para las operaciones del negocio; problemas tecnológicos que afecten la seguridad de la información; ataques del ciberespacio; virus o malware detectados en los activos de información críticos; eventos de indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información de la entidad o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos; problemas que afecten la continuidad de proveedores de servicios críticos; entre otros. Esta información deberá ser mantenida por la entidad en una base de datos de incidentes y otra base de datos de pérdidas operacionales para el mejoramiento continuo del proceso de gestión de riesgo operacional.

b) La ocurrencia de un incidente operacional de aquéllos mencionados en el numeral anterior deberá ser informada a esta Comisión en un plazo máximo de 2 horas desde que la entidad tomó. El plazo señalado es solo para efectos de notificar a la Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados la CMF, posteriormente. Las instrucciones para reportar los incidentes operacionales a esta Comisión se encuentran en el Anexo N° 2 de esta normativa.

c) Para estos efectos, el directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información según lo indicado en esta sección. Ambas personas deberán tener un nivel ejecutivo y ser designados por la entidad, tanto para este efecto como para responder eventuales consultas por parte de esta Comisión.

d) Asimismo, en los casos en que esta Comisión lo estime necesario, podrá requerir a la entidad la elaboración de un informe interno que contenga al menos: el análisis de las causas del incidente; la generación de documentación e informes de investigación; un análisis del impacto generado en los servicios; y el procedimiento para evitar con alto grado de seguridad que se vuelva a presentar; y las materias adicionales que esta Comisión pueda requerir.

e) Sin perjuicio de lo anterior, la entidad deberá mantener informado en forma oportuna al directorio u órgano equivalente sobre las actualizaciones de todos los incidentes operacionales relevantes y las medidas adoptadas para resolverlo.

E.8.2. REGISTRO Y COMUNICACIÓN DE PÉRDIDAS OPERACIONALES

a) Se entiende por pérdida operacional toda pérdida financiera resultante de la materialización del riesgo operacional de acuerdo con lo definido anteriormente. Esto incluye las pérdidas financieras debido a cambios legales o regulatorios que afecten las operaciones de la entidad, o producto de incumplimientos con la regulación vigente.

b) La información de todos los incidentes que se materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento deberá ser enviada a esta Comisión de acuerdo con las instrucciones del Anexo N° 3 de la presente norma, 15 días hábiles después del cierre de junio y diciembre de cada año.

c) Los criterios para la confección del registro de pérdidas operacionales son los siguientes:

   1) La entidad deberá contar con procesos y procedimientos documentados para la identificación, recopilación, uso y comunicación de los registros de pérdida operacional. Esta Comisión podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por empresas de auditoría externa, de aquellos inscritos en el Registro de Empresas de Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.

   2) Los registros internos sobre pérdidas operacionales de la entidad deberán ser integrales e incluir la totalidad de las actividades y exposiciones relevantes, en todos los sistemas y en todas las ubicaciones geográficas pertinentes.

   3) La entidad deberá recopilar información sobre los importes brutos de las pérdidas, y sobre las fechas de referencia de los eventos de riesgo operacional. Además, la entidad deberá recoger información sobre recuperaciones de importes brutos de pérdidas, e información descriptiva sobre los factores determinantes o las causas del evento de pérdida. El grado de detalle de la información descriptiva deberá estar en proporción al importe bruto de la pérdida.

   4) La entidad deberá utilizar la fecha de contabilización del evento para construir el conjunto de registros sobre pérdidas. En el caso de eventos legales, la fecha de contabilización se refiere a cuando se constituye una provisión para esta contingencia legal en el estado de situación financiera, con su reflejo correspondiente en el estado de resultados.

5) Las pérdidas causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo, pero contabilizadas en el transcurso de varios años, deberán asignarse a los años correspondientes en la base de datos de pérdidas, en consonancia con su tratamiento contable.

d) Por pérdida bruta se entiende una pérdida antes de recuperaciones de cualquier tipo.

1) Los siguientes ítems deben ser incluidos en los cálculos de las pérdidas brutas para la base de datos de pérdidas:

i) Cargos directos en las cuentas de Estados de Resultados de la entidad y amortizaciones debido a eventos de riesgo operacional del período. Por ej. Costos incurridos como consecuencia de un evento, incluyendo gastos externos con una relación directa al evento por riesgo operacional (ej. Gastos legales directamente relacionados al evento y comisiones pagadas a los asesores, abogados o proveedores) y costos de reparación o reemplazo incurridos para restaurar la posición que prevalecía antes del evento de riesgo operacional.

ii) Cargos directos en las cuentas de Estados de Resultados de la entidad y amortizaciones debido a eventos por riesgo operacional de ejercicios contables previos que afecten los estados financieros de la entidad en el presente periodo.

2) Los siguientes ítems deben ser excluidos de las pérdidas brutas registradas en la base de datos de pérdidas:

i) Costos por contratos de mantenimientos generales de la propiedad, planta o equipos.

ii) Gastos internos o externos con el fin de mejorar el negocio después de las pérdidas por riesgo operacional: actualizaciones, mejoras, iniciativas de gestión del riesgo y mejoras en ellas.

iii) Primas de seguro.

e) Por pérdida neta se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida inicial, que no necesariamente se efectúa en el mismo periodo en el que se perciben los fondos respectivos.

La entidad deberá ser capaz de identificar las recuperaciones no procedentes de seguros y las recuperaciones originadas por el pago de indemnizaciones de seguros para todos los eventos de pérdidas operacionales. Asimismo, deberá utilizar las pérdidas netas de recuperaciones (incluidas las procedentes de seguros) en el conjunto de registros sobre pérdidas operacionales, aunque las recuperaciones sólo podrán utilizarse para reducir las pérdidas cuando se haya recibido el pago.

Las entidades clasificadas en los Bloques 1 y 2 quedan eximidas del reporte de pérdidas operacionales al que se refiere el Anexo N°3 de la presente normativa.

V. CAPITAL Y GARANTÍAS

En esta sección se establecen los requisitos de patrimonio mínimo y garantías para las entidades que presten los servicios de intermediación de instrumentos financieros y custodia de instrumentos financieros, así como requisitos de garantías a las entidades que presten el servicio de enrutamiento de órdenes, conforme lo establecido en los artículos 7, 10 y 11 de la Ley N°21.521.

A. CLASIFICACIÓN DE ACUERDO CON EL VOLUMEN DE NEGOCIOS

Se definen tres bloques de entidades de acuerdo con su volumen de negocios, con el objetivo de establecer requisitos de patrimonio mínimo y garantías proporcionales para cada una de ellas.

a) Bloque 1: entidades que tengan un número de clientes activos menor a 500, y no cumplan ninguna de las métricas de volumen de negocio de las entidades del Bloque 2 o 3. Se considerarán clientes activos aquellos que cumplan con las condiciones definidas en el Anexo N°1 de esta normativa.

b) Bloque 2: entidades que cumplan alguna de las siguientes condiciones:

i) Tengan un número de clientes activos entre 500 y 5.000.

ii) Transacciones promedio diarias en los últimos tres meses (media móvil) entre UF 100.000 y UF 500.000.

iii) Activos custodiados promedio diarios en los últimos tres meses (media móvil) entre UF 20.000 y UF 100.000.

iv) Ingresos en los últimos 12 meses (media móvil) entre UF 25.000 y UF 50.000.

c) Bloque 3: entidades que cumplan alguna de las siguientes condiciones:

i) Más de 5.000 clientes activos.

ii) Más de UF 500.000 en transacciones promedio diarias en los últimos tres meses (media móvil).

iii) Activos custodiados promedio diarios en los últimos tres meses (media móvil) sobre UF 100.000.

iv) Ingresos en los últimos 12 meses (media móvil) sobre UF 50.000.

En caso de que la entidad sea reclasificada a un bloque superior, dispondrá de un plazo máximo de 6 meses para dar cumplimiento a los requisitos de patrimonio mínimo y garantías correspondiente a dicho bloque.

Las entidades podrán ser reclasificadas a bloques inferiores después de un mínimo de 6 meses y con autorización de la Comisión.

B. REQUISITO DE PATRIMONIO MÍNIMO Y GARANTÍAS

De acuerdo con el artículo 7 de la Ley Fintec, en el caso de que una entidad preste de manera simultánea dos o más de los servicios comprendidos en esta norma, deberá acreditar que cumple todos y cada uno de los requisitos aplicables a cada uno de los servicios sin entenderse por este motivo, la necesidad de acumular el cumplimiento de los requisitos de patrimonio mínimo y garantías de los artículos 10 y 11. De este modo:

a) Las entidades del Bloque 1 que presten los servicios de intermediación de instrumentos financieros, custodia de instrumentos financieros o enrutamiento de órdenes se encuentran exentas de requisitos de patrimonio mínimo y de garantías.

b) Las entidades del Bloque 2 que presten los servicios de intermediación y/o custodia de instrumentos financieros deberán disponer permanentemente de un patrimonio ajustado y/o garantías igual o superior a UF 1.000 de acuerdo con la metodología de cálculo indicada en la sección C. Si la entidad descrita también presta el servicio de enrutamiento de órdenes, no deberá cumplir adicionalmente el requisito de garantías por UF 500 descrito más adelante.

c) Las entidades del Bloque 3 que presten los servicios de intermediación y/o custodia de instrumentos financieros, deberán contar permanentemente con un patrimonio ajustado) y/o garantías que sea igual o superior al mayor entre:

    1) UF 5.000.

    2) El 3% (o hasta 6%) de los activos ponderados por riesgo financiero y operacional de la entidad, de acuerdo con lo dispuesto en la letra D siguiente.

d) Los requisitos de patrimonio por riesgos financieros (mercado y crédito) serán cumplidos exclusivamente por medio del patrimonio ajustado. El requisito de patrimonio por riesgo operacional podrá ser cumplido por patrimonio ajustado y/o garantías.

e) Las entidades del Bloque 2 o 3 que presten el servicio de enrutamiento de órdenes, deberán contar permanentemente con patrimonio ajustado y/o garantías igual o superior a UF 500.

f) Las entidades del Bloque 3 que presten los servicios de intermediación y/o custodia de instrumentos financieros que cumplan con los requisitos mencionados en el literal c), y que también presten el servicio de enrutamiento de órdenes no deberán cumplir adicionalmente el requisito de garantías por UF 500.

g) La entidad podrá constituir una garantía mediante una póliza de seguro o boleta de garantía bancaria para el cumplimiento de los requisitos establecidos en esta norma.

    1) En caso de la póliza de seguro, esta deberá cubrir los daños y perjuicios causados a terceros, de los cuales sea civilmente responsable, que resulten de la prestación de los servicios propios de intermediación de instrumentos financieros, enrutamiento de órdenes o custodia de instrumentos financieros, por actos, errores u omisiones ocurridos durante la vigencia de la póliza y que afecten a los terceros atendidas profesionalmente por el asegurado. Deberá cubrir, asimismo, la responsabilidad civil de sus dependientes, de sus administradores, representantes, apoderados o de cualquier persona que participe en las funciones

de asesoría por su cuenta, y en general, la de toda persona por la cual sea civilmente responsable en el ejercicio de la actividad de intermediación de instrumentos financieros, enrutamiento de órdenes o custodia de instrumentos financieros. La cobertura deberá comprender tanto los daños y perjuicios causados a terceros, como los gastos y costas del proceso que éstos o sus causahabientes promuevan en contra del asegurado.

También deberá ser de cargo de la compañía aseguradora los gastos de defensa del asegurado, incluso los honorarios respectivos, aun cuando se trate de reclamaciones infundadas.

Por último, el seguro deberá indicar que el pago de la indemnización al tercero perjudicado se efectuará en virtud de sentencia ejecutoriada, o de transacción judicial o extrajudicial celebrada por el asegurado con el consentimiento de la compañía.

2) En el caso de constituirse la garantía mediante boleta bancaria, ella deberá ser tomada en un banco autorizado para operar en el mercado nacional. El documento deberá señalar que es tomada a favor de los beneficiarios de la garantía, esto es, los acreedores presentes o futuros que llegare a tener en razón de sus operaciones de intermediación de instrumentos financieros, enrutamiento de órdenes o custodia de instrumentos financieros, y con el exclusivo objeto de ser usada en los términos de la Ley N°21.521, y ser pagadera a simple requerimiento.

El monto de la boleta bancaria será el que se determine por aplicación de lo dispuesto en esta norma.

La entidad deberá designar a un banco como representante de los posibles beneficiarios de la boleta bancaria, quien será el tenedor de esta.

El representante de los beneficiarios de la boleta bancaria, para hacerla efectiva y sin que sea necesario acreditarlo a la entidad otorgante, deberá ser notificado judicialmente del hecho de haberse interpuesto demanda en contra de la entidad caucionada.

La boleta bancaria deberá poder hacerse efectiva hasta 30 días después de su vencimiento, pero sólo por hechos ocurridos durante el período de su vigencia.

El dinero proveniente de la realización de la boleta bancaria quedará en prenda de pleno derecho en sustitución de la garantía, manteniéndose en depósitos reajustables por el representante, hasta que cese la obligación de mantener la garantía.

h) En lo referente a la vigencia de la garantía, las entidades deberán mantener siempre vigente la garantía en los términos y por los montos establecidos en la presente norma para poder actuar en el desarrollo de su giro (en la medida que no haya sido cubierto por patrimonio de acuerdo a lo señalado en esta sección).

En caso de hacerse efectiva la garantía, la entidad estará obligada a la presentación de una nueva garantía, conforme a lo establecido en esta norma, para poder continuar desarrollando las actividades inherentes a su giro.

Tratándose de pólizas de seguros, ante cualquier indemnización pagada por el asegurador con cargo a dichas pólizas -que reduzca el monto asegurado en igual cantidad- la entidad afectada deberá rehabilitar el monto asegurado original de la póliza, simultáneamente con el pago del siniestro por parte de la compañía. Se deberá acreditar dicha rehabilitación ante la Comisión, el mismo día en que se haya efectuado el pago de la indemnización.

La entidad que no diere cumplimiento oportuno a las obligaciones anteriores no podrá celebrar nuevos contratos inherentes al desarrollo de su giro, sin perjuicio de las medidas que al efecto disponga la Comisión.

Tabla 6. Requisitos de patrimonio mínimo y garantías para la prestación de servicios de intermediación y/o custodia de instrumentos financieros, y enrutamiento de órdenes.

Servicio		**Bloque**	**Requisito de patrimonio por riesgo**		**Sección norma**
EO		1	Exento		V.B.(a)
		2	Requisito de patrimonio mínimo o garantías de UF 500		V.B.(e)
		3			
Custodia	**Con y sin IIF**	1	Exento		V.B.(a)
		2	Requisito de patrimonio mínimo o garantías de UF 1.000		V.B.(b)
	Sin IIF	3	Operacional		V.D.1.(b.2)
	Con IIF				V.D.1.(b.1)
IIF	**Cuenta propia y terceros**	1	Exento		V.B.(a)
		2	Requisito de patrimonio mínimo o garantías de UF 1.000		V.B.(b)
		3	Operacional		V.D.1.(a)
	Cuenta propia	3	Mercado	Tasas de interés	V.D.2.1
				Materias primas	V.D.2.2
				Moneda extranjera	V.D.2.3
				Acciones e índices	V.D.2.4
			Crédito	Crédito	V.D.3
				Contraparte	V.D.3.1
			Cripto	Tipo A	V.D.4.(d)
				Tipo B	V.D.4.(e)

Donde:
IIF: Intermediación de instrumentos financieros.

EO: Enrutamiento de órdenes.

Custodia: Custodia de instrumentos financieros.

Sin IIF: Entidad presta solamente el servicio de custodia, sin la intermediación de instrumentos financieros.

Con IIF: la entidad presta el servicio de custodia de forma conjunta con el servicio de intermediación de instrumentos financieros.

Cuenta propia: Intermediación de instrumentos financieros por cuenta propia.

Terceros: Intermediación de instrumentos financieros por cuenta de terceros.

C. PATRIMONIO AJUSTADO

El patrimonio ajustado de la entidad no podrá ser inferior al requisito de patrimonio mínimo establecido en la letra B anterior.

a) Para el cálculo del patrimonio ajustado se rebajará del patrimonio contable:

1) Los activos intangibles.
2) El saldo deudor de las cuentas con personas naturales o jurídicas relacionadas al prestador de servicios financieros.
3) Los activos utilizados para garantizar obligaciones de terceros.
4) Los activos entregados a otras entidades para cubrir las operaciones efectuadas por cuenta propia en derivados o contratos por diferencias.
5) El saldo deudor de las cuentas por cobrar con relacionados.
6) El monto registrado por concepto de gastos anticipados.
7) El saldo neto de activos diferidos.

b) En la determinación del patrimonio ajustado, si existieren activos que permanecieren impagos, se deberá considerar como valor de dichos activos el menor valor que resulte de aplicar uno de los siguientes métodos.

1) Rebajar del valor de los activos las provisiones que se hubieren constituido por concepto de deudas incobrables, de acuerdo con las Normas Internacionales de Información Financiera (NIIF, IFRS en su sigla en inglés) y a las normas de esta Comisión.

2) Según sea el período en que ha permanecido impago, o las veces que ha sido reprogramado:

i) Considerar en un 60% de su valor los activos que permanecieren impagos por un plazo superior a 2 días con posterioridad a su vencimiento o cuyo vencimiento hubiere sido programado por primera vez.

ii) Considerar en un 30% de su valor los activos que permanecieron impagos por un plazo superior a 10 días o cuyo vencimiento hubiere sido reprogramado por segunda vez.

iii) No considerar aquellos activos que permanecieron impagos por un plazo superior a 30 días con posterioridad a su vencimiento o cuyo vencimiento hubiere sido reprogramado más de dos veces.

c) En caso de que las propiedades representen más del 40% del total de activos, se deberá disponer de una tasación comercial independiente con una antigüedad no mayor a dos años. Para estos efectos, tendrán que contratar una tasación comercial con profesionales idóneos, independientes, no relacionados con la entidad ni entre sí, siendo estos tasadores de bancos, arquitectos, ingenieros civiles o constructores civiles de reconocido prestigio. Los tasadores deberán tener la más alta calificación profesional en consideración a las características, uso y destino de los bienes tasados. Las entidades deberán velar por que las personas contratadas para tasar los bienes raíces de su propiedad, no tengan intereses que comprometan su independencia respecto la entidad y de quienes tengan interés económico o puedan ser afectados por la tasación.

D. METODOLOGÍA DE CÓMPUTO DE LOS ACTIVOS PONDERADOS POR RIESGO FINANCIERO Y OPERACIONAL

a) El requerimiento de patrimonio ajustado para la prestación de los servicios de intermediación y/o custodia de instrumentos financieros será calculado por medio de la suma de las siguientes cantidades:

   1) Un monto referido al requerimiento de patrimonio por riesgo operacional calculado según lo dispuesto la sección D.1 siguiente.

   2) Un monto referido al requerimiento de patrimonio por riesgo de mercado según lo dispuesto en la sección D.2 siguiente.

   3) Un monto referido al requerimiento de patrimonio por riesgo de crédito según lo dispuesto en la sección D.3 siguiente.

   4) Un monto referido al requerimiento de patrimonio de riesgo de crédito y mercado para criptoactivos en la sección D.4. siguiente.

b) El valor total de los activos ponderados por riesgo financiero y operacional corresponderá a 33,3 veces el requerimiento de patrimonio de la letra a) precedente.

D.1. REQUISITO DE PATRIMONIO (O GARANTÍAS) POR RIESGO OPERACIONAL

a) El requisito de patrimonio por riesgo operacional para el servicio de intermediación de instrumentos financieros corresponde a un porcentaje del monto de las transacciones totales promedio diarias de los últimos tres meses. El total de transacciones incluye aquellas de compra y venta, tanto por cuenta propia como por cuenta de terceros. Para ello se deberán sumar:

   1) El 0,1% de las transacciones que no correspondan a derivados o contratos por diferencias promedio diarias de los últimos tres meses.

   2) El 0,01% de los montos nocionales de los contratos derivados o contratos por diferencias promedio diario de los últimos tres meses.

b) El requerimiento de patrimonio de riesgo operacional para el servicio de custodia de instrumentos financieros corresponde a un porcentaje del monto de los activos custodiados promedio de los últimos tres meses.

   1) En el caso que los servicios de intermediación y custodia de instrumentos financieros sean prestados de forma conjunta, este monto será el 0,4% de los activos custodiados promedio diario de los últimos tres meses.

   2) En el caso que el servicio de custodia sea prestado de forma exclusiva, este monto será 0,1% de los activos custodiados promedio diario de los últimos tres meses.

c) La Tabla 7 muestra la metodología de cálculo del requisito de patrimonio por riesgo operacional cuando la prestación del servicio de intermediación se realiza en forma conjunta con el servicio de custodia. La Tabla 8 corresponde al caso en que el servicio de custodia se presta de forma exclusiva, sin considerar el servicio de intermediación.

Tabla 7. Cálculo del requisito de patrimonio por riesgo operacional para la prestación conjunta de servicios de intermediación y custodia.

Servicio	Exposición (E)	Ponderador (P)	Requisito de patrimonio
Custodia	Activos custodiados	0,4%	∑E*P
Intermediación transacciones que no corresponden a derivados o CFD	Monto promedio diario del valor de las transacciones	0,1%	
Intermediación transacciones en derivados y CFD	Monto promedio diario del monto nocional de las transacciones	0,01%	

Tabla 8. Cálculo del requisito de patrimonio por riesgo operacional para la prestación del servicio de custodia de forma exclusiva (sin intermediación).

Servicio	Exposición (E)	Ponderador (P)	Requisito de patrimonio
Custodia	Activos custodiados	0,1%	∑E*P

D.2. REQUISITO DE PATRIMONIO POR RIESGO DE MERCADO

Este requisito aplica a los prestadores de servicios de intermediación de instrumentos financieros que dispongan una cartera propia en instrumentos financieros. El requisito total de patrimonio por riesgo de mercado será igual a la suma de los montos requeridos por las exposiciones a los siguientes factores de riesgo:

1. Tasa de interés
2. Materias primas
3. Tipo de cambio
4. Acciones e índices accionarios

D.2.1. TASA DE INTERÉS

a) **Instrumentos representativos de deuda**. El requisito de patrimonio por riesgo de mercado corresponde a un monto referido a las posiciones en instrumentos financieros representativos de deuda que el prestador de servicios de intermediación considere en el cálculo de su patrimonio mínimo.

1) Se deberá clasificar cada uno de los instrumentos financieros de acuerdo con la Tabla 9 referida al plazo de vencimiento.

2) Una vez efectuada esta clasificación se deberán aplicar los porcentajes dispuestos en la Tabla 9, sobre el valor de mercado de los instrumentos financieros.

3) Para el caso de los instrumentos que, de acuerdo con IFRS, se deban constituir provisiones, el requerimiento patrimonial se calculará sobre el activo neto de provisión multiplicado por el ponderador correspondiente.

b) **Derivados de tasas de interés**. El requisito de patrimonio por riesgo de mercado corresponde a un monto referido a los derechos y obligaciones del prestador de servicios de intermediación cuyo valor se reajuste de acuerdo con la variación de tasas de interés del mercado. En el caso de derivados o contratos por diferencias se deberá considerar su valor nocional.

1) Se deberá clasificar cada uno de los instrumentos financieros de acuerdo con la Tabla 9 referida al plazo residual al vencimiento del instrumento.

2) Una vez efectuada esta clasificación se deberán aplicar los porcentajes dispuestos en la Tabla 9, sobre el valor nocional de los instrumentos financieros.

Tabla 9. Porcentajes según plazo al vencimiento riesgo de mercado tasas de interés

Plazo al vencimiento	%
<91 días	2
90 días< y <1 año	5
1 año < y <5 años	8
5 años< y <12 años	12
>12 años	20

D.2.2. MATERIAS PRIMAS

a) Para el cálculo del requisito de patrimonio por riesgo de mercado, se deben incluir todas las posiciones en instrumentos financieros en derivados y contratos por diferencias sobre materias primas o índices sobre materias primas.

b) Para cada materia prima expresada en su unidad estándar de medición y luego convertida a moneda local mediante las tasas spot, se calcula la posición neta como la diferencia entre posiciones activas y pasivas. A esta posición resultante se le aplica un cargo de 15%. Además, se aplica un cargo adicional de 3% sobre la posición bruta en cada materia prima, es decir, sobre la suma de posiciones activas y pasivas (en valor absoluto).

c) Lo anterior se expresa en la siguiente fórmula. Donde Ai corresponde al valor de las posiciones activas en la materia prima "i", Pi corresponde al valor de las posiciones pasivas en la materia prima "i" y "N" corresponde al número de materias primas en las que el prestador de servicios de intermediación mantiene posiciones.

$$\sum_{\mathbf{i=1}}^{\mathbf{N}}(|\mathbf{A_i}-\mathbf{P_i}|)*\mathbf{15\%}+\sum_{\mathbf{i=1}}^{\mathbf{N}}(\mathbf{A_i}+|\mathbf{P_i}|)*\mathbf{3\%}$$

D.2.3. MONEDA EXTRANJERA.

a) Para el cálculo del requisito de patrimonio por riesgo de mercado, se deben considerar las posiciones netas en monedas en todo el balance. La posición neta en cada moneda debe calcularse sumando:

1) La posición neta efectiva o spot.

2) La posición neta en derivados o contratos por diferencias, que incluye todos los montos a recibir menos todos los montos a pagar.

3) Garantías en moneda extranjera.

4) Cualquier otra posición del balance que pueda generar ganancias o pérdidas en monedas extranjeras.

b) Para el cálculo del requisito de patrimonio por riesgo de mercado, se debe ponderar la posición neta en cada moneda por el ponderador de riesgo de mercado (PRM) que le corresponda, mediante la siguiente fórmula.

$$\mathbf{max}(\sum_{\mathbf{i=1}}^{\mathbf{N}}(\mathbf{PNA_i}*\mathbf{PRM_i}),\sum_{\mathbf{i=1}}^{\mathbf{N}}(|\mathbf{PNP_i}*\mathbf{PRM_i}|))$$

c) Donde $PNAi$ y $PNPi$ corresponden a la posición neta activa y pasiva, respectivamente para cada moneda "i"; $PRMi$ corresponde al ponderador de riesgo de mercado, asociado a la moneda "i", que se determina de acuerdo con la Tabla 10.

Tabla 10. Ponderadores de riesgo de tipo de cambio

Riesgos	Monedas	Ponderador
Canasta 1	USD, EUR, EAU, AUD, CAD, CHF, CNY, CZK, DKK, GBP, HKD, ILS, JPY, KRW, NOK, NZD, SAR, SGD, SKK, SEK, TWD	8%
Canasta 2	Resto de monedas	12%

D.2.4. ACCIONES E ÍNDICES ACCIONARIOS

El requisito de patrimonio por riesgo de mercado de cotizaciones bursátiles se aplica a todos los derivados y contratos por diferencias que tengan como subyacentes posiciones en acciones e índices sobre acciones, los que deben ser separados en los subyacentes respectivos. Se deberán calcular de acuerdo con cada mercado del respectivo subyacente y considerar el riesgo específico y riesgo general señalado a continuación.

a) Riesgo específico. Donde "Ai" corresponde al valor de las posiciones activas en el mercado bursátil "i", "Pi" corresponde al valor de las posiciones pasivas en el mercado bursátil "i" y "N" corresponde al número de mercados bursátiles en los que el prestador de servicios de intermediación mantiene posiciones.

$$\sum_{\mathbf{i=1}}^{\mathbf{N}} (\mathbf{A_i} + |\mathbf{P_i}|) * \mathbf{11\%}$$

b) Riesgo general. El requisito de patrimonio por riesgo general se calcula como la exposición neta de instrumentos derivados o contratos por diferencia, es decir, la suma de las posiciones activas menos las posiciones pasivas, multiplicado por un ponderador de riesgo de mercado (PRM) único de 11%. Además de lo anterior, se agrega un cargo adicional de 2% a las posiciones netas en índices sobre acciones. Donde "Ai" corresponde al valor de las posiciones activas en el mercado bursátil "i" (excluye índices y estrategias de arbitraje), "Pi" corresponde al valor de las posiciones pasivas en el mercado bursátil "i" (excluye índices y estrategias de arbitraje), "AIi" corresponde al valor de las posiciones activas en índices y estrategias de arbitraje en el mercado bursátil "i", "PIi" corresponde al valor de las posiciones pasivas en índices y estrategias de arbitraje en el mercado bursátil "i" y "N" corresponde al número de mercados bursátiles en los que el prestador de servicios de intermediación mantiene posiciones.

$$\sum_{\mathbf{i=1}}^{\mathbf{N}} (|\mathbf{A_i} - \mathbf{P_i}|) * \mathbf{11\%} + \sum_{\mathbf{i=1}}^{\mathbf{N}} (|\mathbf{AI_i} - \mathbf{PI_i}|) * \mathbf{13\%}$$

D.3. REQUISITO DE PATRIMONIO POR RIESGO DE CRÉDITO

a) El requisito de patrimonio de riesgo de crédito corresponde a un monto referido a instrumentos representativos de deuda que el prestador de servicios de intermediación de instrumentos financieros considere en el cálculo de su patrimonio mínimo. Se exceptuará de la aplicación de dicho porcentaje el saldo de la cuenta efectivo y equivalentes de efectivo.

   1) Se deberá clasificar cada uno de los instrumentos financieros de acuerdo con la clasificación crediticia y de tipo de contraparte de la Tabla 11.

   2) Una vez efectuada esta clasificación se deberán aplicar los porcentajes dispuestos en la Tabla 11, sobre el valor de los instrumentos financieros.

b) El prestador de servicios financieros de intermediación deberá mantener un registro en el que anotará toda aquella información que permita determinar claramente los activos que han permanecido impagos, el plazo durante el cual estuvieron bajo esa

calidad, el número y fecha en que se efectuaron reprogramaciones y la identificación de los deudores correspondientes. Este registro deberá mantenerse en un medio y sistemas que garanticen su fiabilidad e integridad. Las reprogramaciones deberán constar por escrito y estar debidamente documentadas.

Tabla 11. Porcentajes según clasificación crediticia y tipo de la contraparte para riesgo de crédito

Tipo y clasificación crediticia de la contraparte	%
Grado inversión	1%
BB+/BB-	8%
Bajo BB-	12%
Personas	6%
Pymes	6,8%
Otros	8%

D.3.1. REQUISITO DE PATRIMONIO POR RIESGO DE CONTRAPARTE

a) El requisito de patrimonio de riesgo de contraparte corresponde a un monto referido a la intermediación por cuenta propia de derivados y contratos por diferencias del prestador de servicios, el cual será calculado por medio del "equivalente de crédito" y ponderadores de riesgo de crédito según el tipo y clasificación crediticia de la contraparte.

b) El cálculo del "equivalente de crédito" para derivados y contratos por diferencias considera:

1) El valor razonable del instrumento derivado o contrato por diferencias.

2) Un monto adicional, que considera la variación potencial futura (PFE) del precio del derivado o contrato por diferencias. Para ello, se deberá multiplicar el valor nocional del derivado o contrato por diferencias según el tipo de activo subyacente y plazo al vencimiento de acuerdo con la Tabla 12. Para el "plazo residual" de la Tabla 12, los contratos por diferencia deberán ser considerados en la categoría "hasta un año"

3) Se deberán descontar las garantías constituidas en favor del prestador de servicios de intermediación por parte de sus clientes.

4) El "equivalente de crédito" será igual a el máximo valor entre 0 y la suma de los montos mencionados anteriormente, de acuerdo con la fórmula:

$$\textbf{Equivalente de crédito} = \textbf{Max}(\textbf{Valor razonable} + \textbf{PFE} - \textbf{Garantías}, \textbf{0})$$

c) A efectos de calcular el requisito de patrimonio por riesgo de contraparte, se deberá aplicar al "equivalente de crédito" los ponderadores de crédito según el tipo y clasificación crediticia de la contraparte de acuerdo con la Tabla 11 de la sección anterior.

d) La metodología de cálculo se ejemplifica en la Tabla 13.

Tabla 12. Ponderadores de variación potencial futura (PFE)

Tipo de contrato	Plazo residual	Propuesta ponderadores PFE	
Tasa de interés o inflación	Hasta un año	0%	
	Entre 1 y 5 años	0,5%	
	Más de 5 años	1,5%	
Tipo de cambio		**Canasta 1**	**Canasta 2**
	Hasta 1 año	1,5%	4,5%
	Entre 1 y 5 años	7%	20%
	Más de 5 años	13%	30%
Acciones	Hasta 1 año	6%	
	Entre 1 y 5 años	8%	
	Más de 5 años	10%	
Materias primas		18%	
Otros		32%	

Tabla 13. Cálculo del requisito de patrimonio por riesgo de contraparte

Equivalente de crédito (E)	Ponderador (P)	Requisito de patrimonio
$\text{Max}(\text{Valor razonable} + \text{PFE} - \text{Garantías}, 0)$	• Grado inversión: 1% • BB+/BB-: 8% • Bajo BB-: 12% • Personas: 6% • Pymes: 6,8% • Otros: 8%	∑E*P

D.4. REQUISITO DE PATRIMONIO DE RIESGO DE CRÉDITO Y MERCADO PARA CRIPTOACTIVOS

a) Este requisito aplica a la cartera propia de los prestadores de servicios de intermediación de instrumentos financieros, clasificados en el Bloque 3 de acuerdo con su volumen de negocios.

b) Esta Comisión publicará una lista de criptoactivos elegibles para aplicar el criterio de compensación parcial. Los activos incluidos en esta lista se denominarán activos "Tipo A", el resto será clasificado como "Tipo B". Los criptoactivos "Tipo A" serán incluidos en la lista por esta Comisión de acuerdo con las características de liquidez, capitalización de mercado, transaccionalidad y disponibilidad de precios que dichos activos tengan. Mientras que los activos que no cuenten con dichas características deberán ser clasificados en el segundo grupo.

c) Se aplicará el criterio de compensación parcial a los activos "Tipo A" a efectos de calcular sus requisitos de patrimonio de riesgo de crédito y mercado. A los activos "Tipo B" no les será aplicada dicha compensación.

d) El cálculo del criterio de compensación parcial aplicable a los activos "Tipo A" considera la posición neta de cada activo criptográfico (subíndice "k") de acuerdo con la siguiente fórmula. Se aplica un requisito de patrimonio de 100% sobre la posición neta de cada activo "Tipo A".

$$\mathbf{Posición\ neta_k} = \mathbf{Max}(\mathbf{Posición\ larga_k}, |\mathbf{Posición\ corta_k}|) - \mathbf{0.65} * \mathbf{Min}(\mathbf{Posición\ larga_k}, |\mathbf{Posición\ corta_k}|)$$

e) Para los activos "Tipo B", se aplica un requisito de patrimonio de 100% sobre la posición bruta de cada activo criptográfico (subíndice "k"), de acuerdo con siguiente fórmula.

$$\mathbf{Posición_k} = \mathbf{Max}(\mathbf{abs}(\mathbf{posición\ larga_k}), \mathbf{abs}(\mathbf{Posición\ corta_k}))$$

f) El requisito de patrimonio por riesgo de mercado y crédito para activos criptográficos se ejemplifica en la Tabla 14.

Tabla 14. Cálculo del requisito de patrimonio por riesgo de mercado y crédito de criptoactivos

	Exposición (E)	Ponderador (P)	Requisito de patrimonio
Tipo A	$\text{Posición neta}_k = \text{Max}(\text{Posición larga}_k, \lvert\text{Posición corta}_k\rvert) - 0.65 * \text{Min}(\text{Posición larga}_k, \lvert\text{Posición corta}_k\rvert)$	100%	ΣE*P
Tipo B	$\text{Posición bruta}_k = \text{Max}(\text{abs}(\text{posición larga}_k), \text{abs}(\text{Posición corta}_k))$	100%	

D.4.1. LISTADO DE CRIPTOACTIVOS TIPO A

La Tabla 15 define el listado de criptoactivos de Tipo A, elegibles para aplicar el criterio de compensación parcial.

Tabla 15. Listado de criptoactivos de Tipo A

Nombre	Código
Bitcoin	BTC
Ethereum	ETH
Tether	USDT
BNB	BNB
XRP	XRP
USD Coin	USDC
Cardano	ADA
Dogecoin	DOGE

D.5. DISPOSICIONES GENERALES

a) Cuando un prestador de servicios financieros incurra por cualquier causa en incumplimiento de alguna de las condiciones prescritas en esta norma, deberá dar aviso por medio del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados antes de las 18:00 horas del día hábil siguiente a aquel en que se advirtió el incumplimiento.

b) El prestador de servicios financieros deberá contar con sistemas que le permitan conocer el estado de cumplimiento permanente de las condiciones de patrimonio mínimo y garantías requeridas por la presente norma. La Comisión podrá requerir en cualquier momento los antecedentes y registros que den cuenta de dicho cumplimiento.

VI. CAPACIDAD OPERACIONAL

Quienes presten el servicio de sistema alternativo de transacción, enrutamiento de órdenes, intermediación y custodia de instrumentos financieros deberán contar con la capacidad operacional para soportar el procesamiento de las operaciones o transacciones que mediante sus sistemas o infraestructura se realicen conforme a lo establecido en el artículo 7 de la Ley N°21.521.

Para acreditar dicha capacidad operacional el solicitante, al momento de requerir la autorización de los servicios, deberá declarar, identificándose mediante el mecanismo electrónico dispuesto para esos efectos en el sitio en Internet de la Comisión, que sus sistemas e infraestructura estarán en condiciones de procesar las operaciones o transacciones proyectadas una vez que cuente con la autorización de la Comisión para llevar a cabo el servicio y las estimadas para los próximos tres años. Para esos efectos deberá acompañar una descripción de las estimaciones realizadas sobre la capacidad actual y futura de sus sistemas e infraestructura por tipo de servicio, expresando la capacidad de los mismos como número máximo de operaciones o transacciones que se podrán realizar por unidad de tiempo y dando cuenta de las pruebas de funcionamiento realizadas para verificar dicha capacidad, incluyendo las pruebas de stress o tensión que se hubieren efectuado para determinar la holgura respecto a la demanda esperada y los procedimientos definidos para monitorear y ajustar la capacidad operacional. Tratándose de entidades clasificadas en el Bloque 2 y 3 al que se refiere la Sección IV de esta normativa, además deberán acompañar una certificación efectuada por un tercero especializado conforme a estándares o buenas prácticas internacionales de común aceptación, que se pronuncie respecto de la confiabilidad y suficiencia de las pruebas realizadas por la entidad, así como también de sus resultados.

VII. ACTIVIDADES INHERENTES

Para efectos de lo establecido en el artículo 5 de la Ley Fintec, se reputan inherentes al giro regulado por ley y, por tanto, pueden realizarse sin que se requiera de su autorización como actividad complementaria, las siguientes actividades:

a) Realización de operaciones de cambio de divisas, para quienes tienen autorizada la actividad de intermediación y custodia de instrumentos financieros.

b) Asesoría tributaria y de planificación financiera, y estudios relacionados con ámbitos financieros o micro o macroeconómicos, para quienes tienen autorizada la actividad de asesoría de inversión.

c) Generación, comercialización y difusión de reportes con información crediticia o comercial, en el caso de quienes tienen autorizada la actividad de asesoría crediticia.

d) Cobranza y ejercicio de derechos emanados de la intermediación o custodia de los instrumentos financieros, para quienes tienen autorizado alguno de esos servicios.

e) Comercialización y desarrollo de herramientas tecnológicas para la prestación de servicios financieros o de soporte a los mismos, en la medida que tengan relación con los servicios autorizados a la entidad.

f) Inversión del capital propio en instrumentos financieros y valores.

g) Control de límites de inversión para clientes, para quienes tienen autorizada la actividad de intermediación o custodia de instrumentos financieros.

h) Referir clientes o actuar como mandatarios para la sola recepción de órdenes de clientes por terceros habilitados en Chile o en el extranjero para actuar como intermediarios, en el caso de quienes tienen autorizada la actividad de enrutador de órdenes y de asesoría de inversión.

i) Canalizar órdenes hacia entidades nacionales o internacionales, para quienes tienen autorizada la actividad de enrutador de órdenes.

j) Compilación, tratamiento, comunicación y procesamiento de datos de obligaciones económicas e informes comerciales, para quienes tienen autorizada la actividad de asesoría crediticia.

k) Intermediación de valores de oferta pública exceptuados de su inscripción en los registros que lleva la Comisión, para quienes tienen autorizada la actividad de intermediación de instrumentos financieros.

l) Canalización de órdenes para la compra o venta de valores de oferta pública exceptuados de su inscripción en los registros que lleva la Comisión, para quienes tienen autorizada la actividad de enrutador de órdenes.

m) Custodia de valores de oferta pública exceptuados de su inscripción en los registros que lleva la Comisión, para quienes tienen autorizada la actividad de custodia de instrumentos financieros.

Lo anterior sin perjuicio de las actividades complementarias que esta Comisión autorice mediante normativa.

VIII. DEROGACIÓN

Deróguese la Norma de Carácter General N°493 de 2023 y la Norma de Carácter General N°494 de 2023.

IX. VIGENCIA

La presente normativa entra en vigor a contar del 3 de febrero de 2024.

Por lo anterior, conforme lo dispuesto en el artículo segundo de las disposiciones transitorias de la Ley, los prestadores de los servicios de plataforma de financiamiento colectivo, sistemas alternativos de transacción, asesoría crediticia, custodia de instrumentos financieros, enrutamiento de órdenes e intermediación de instrumentos financieros deberán presentar las respectivas solicitudes de inscripción y autorización para las actividades que estuvieren realizando a la fecha de entrada en vigencia de esta normativa antes del 3 de febrero de 2025. Se hace presente que la sola inscripción no habilita a la respectiva entidad a prestar los servicios que pretende realizar, razón por la que es responsabilidad de cada entidad el procurar obtener, junto con su inscripción, la autorización de los servicios que desea realizar, efectuando ambas solicitudes de manera paralela y acompañando los antecedentes para ambos procesos de forma oportuna.

Los prestadores de servicios a los que se refiere el segundo párrafo de esta sección que no efectúen las solicitudes ante esta Comisión antes del 3 de febrero de 2025, o habiéndola efectuado en ese plazo ésta sea declarada abandonada por no haberse subsanado las observaciones formuladas dentro del plazo establecido por la Comisión o rechazada por ésta, deberán abstenerse de continuar prestando sus servicios para la celebración de nuevas operaciones y deberán realizar únicamente los actos tendientes a la conclusión de las operaciones reguladas en la Ley N°21.521 contratadas antes de la fecha previamente señalada. En el caso de los prestadores del servicio de asesoría de inversión dicho plazo seguirá siendo el establecido en el inciso final de la sección de vigencia de la Norma de Carácter General N°494, esto es, antes del 3 de febrero de 2024.

Las personas naturales y jurídicas que a la fecha de entrada en vigencia de la presente Norma de Carácter General se encuentren inscritas en el Registro de Prestadores de Servicios financieros, deberán ajustarse a lo dispuesto en esta normativa y remitir a esta Comisión los antecedentes para la inscripción y autorización del servicio de asesoría de inversión antes del 3 de agosto de 2024, a través del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados. Cumplido ese plazo sin haber remitido los antecedentes exigidos, la Comisión podrá proceder a la revocación de la autorización respectiva y a la cancelación en dicho Registro. Dichas personas podrán seguir prestando los servicios a los que se refiere el segundo párrafo de esta sección que estuvieren realizando a la fecha de entrada en vigencia de esta normativa, sin perjuicio de que deberán remitir las respectivas solicitudes de autorización antes del 3 de febrero de 2025 y quedarán sujetos a lo dispuesto en el inciso precedente respecto de tales servicios.

Las solicitudes de inscripción en el Registro de Prestadores de Servicios Financieros y de autorización del servicio de asesoría de inversión que estén pendientes de tramitación a la fecha de emisión de esta normativa quedarán sin efecto, debiendo las entidades abstenerse de prestar el servicio de asesoría de inversión en tanto no presenten una nueva solicitud de inscripción y de autorización. Para poder continuar prestando dicho servicio mientras se tramitan ambas solicitudes, deberán ingresarlas nuevamente a más tardar el 3 de febrero de 2024. En caso que se presenten con posterioridad a dicho plazo no podrán prestar el servicio de asesoría de inversión mientras la Comisión no hubiere conferido la respectiva autorización. Declarado abandonado el procedimiento por no haberse subsanado las observaciones formuladas por la Comisión dentro del plazo establecido por ésta para ello, o rechazada la solicitud, la entidad no podrá seguir prestando el servicio de asesoría.

Firma Electrónica FIRMADO CMF -CHILE

Solange Berstein Jáuregui
Presidenta
Comisión para el Mercado Financiero

SOLANGE BERSTEIN JÁUREGUI
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO

ANEXO N° 1: DEFINICIONES

Activos de información: corresponde a los recursos de información o elementos relacionados con el tratamiento de la información, los cuales pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como hardware; software; redes de comunicación; personal; entre otros.

Amenaza: se refiere a cualquiera circunstancia o evento que pudiera explotar una vulnerabilidad.

Análisis de impacto del negocio o BIA: es el procedimiento de análisis de los efectos que puede tener en los procesos de la entidad una interrupción del negocio.

Apetito por riesgo: nivel agregado y tipos de riesgo que una entidad está dispuesta a asumir, previamente decidido y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.

Ataque: en el contexto de ciberseguridad, se refiere a un evento que tuviera como intención destruir, exponer, alterar, deshabilitar, robar, u obtener acceso o hacer un uso no autorizado de un activo de información.

Ciberseguridad: corresponde al conjunto de acciones que realiza la entidad para mitigar los riesgos y proteger la información e infraestructura que la soporta, de eventos del ciberespacio, siendo este último el entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.

Cliente activo: todo cliente que no se considera inactivo será considerado como activo, dependiendo del tipo de servicio prestado:

Tipo de servicio	Clientes activos
Asesoría de inversión o crediticia	Quienes hayan recibido o solicitado un servicio de asesoría determinada durante los últimos 3 meses.
Enrutamiento de órdenes	Quienes hayan ingresado órdenes para ser canalizadas por el enrutador durante los últimos 3 meses.
Plataforma de financiamiento colectiva	Quienes hayan participado en el financiamiento de un proyecto de inversión o necesidad de financiamiento durante los últimos 3 meses.
Sistemas alternativos de transacción	Quienes hayan realizado una cotización, oferta o transacción en el sistema alternativo de transacción en los últimos 3 meses.
Intermediación de instrumentos financieros	Quienes hayan realizado una transacción a través del intermediario durante los últimos 3 meses
Custodia de instrumentos financieros	Quienes posean saldos en custodia por un monto de, al menos, 100.000 pesos.

Cliente inactivo: se define como cliente inactivo aquel que no ha utilizado en ninguna forma los servicios de asesoría crediticia, asesoría de inversión, enrutamiento de órdenes, sistema alternativo de transacción, intermediación de instrumentos financieros, custodia de instrumentos financieros y/o plataforma de financiamiento colectivo en los último 3 meses. También, aquel cliente que no tiene un contrato vigente con el prestador de servicios. Los clientes deberán ser considerados para cada uno de estos servicios por separado, pudiendo un mismo cliente contratar más de un servicio prestado por la entidad.

Se define como cliente inactivo aquellos que cumplan con las siguientes condiciones de forma conjunta:

- No realizan ningún tipo de transacción ni han recibido o solicitado ningún tipo de asesoría en los últimos 3 meses.

- No disponen de saldos (activos o pasivo) en cuentas provistas por la entidad.

- No tienen posiciones vigentes en instrumentos financieros, proyectos de inversión o necesidades de financiamiento ofertados a través de la entidad.

Cliente institucional: inversionistas institucionales de acuerdo con la letra e) del artículo 4 bis de la Ley N°18.045 de Mercado de Valores y la Norma de Carácter General N°410 de esta Comisión

Confidencialidad de la información: protección de los datos contra el acceso y la divulgación no autorizados, definido por el directorio u órgano equivalente. Incluye los medios para proteger la privacidad personal y la información reservada, en especial de los clientes de la entidad.

Downtime: la cantidad de tiempo que el proceso o negocio es interrumpido.

Encargado del proceso: corresponde a aquella persona designada para hacerse responsable de la administración de un proceso y propiciar las mejoras a implementar en éste.

Externalización de servicios: es la ejecución por un proveedor externo de servicios o actividades en forma continua u ocasional, las que normalmente podrían ser realizadas por la entidad contratante

Incidente: evento único o serie de eventos de seguridad de la información inesperados o no deseados, que resultaren en un intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad.

Instancia: se refiere a un nivel o grado de la estructura organizacional de la entidad, esto incluye, comité, unidad, división, departamento u otro equivalente.

Malware: software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la disponibilidad, confidencialidad e integridad de un sistema de información. Un virus, "worm", troyano u otra entidad basada en código que infecta un host. El "spyware" y algunas formas de adware también son ejemplos de código malicioso.

Mecanismos de autenticación: mecanismos utilizados para confirmar la identidad de un usuario. Estos mecanismos pueden utilizar uno o más factores de autenticación, por ejemplo, credenciales, contraseñas, certificados digitales, o características biométricas o biológicas. El mecanismo de autenticación es multifactor cuando utiliza una combinación de factores de autenticación para confirmar la identidad.

Mercado: para el cálculo del requisito de patrimonio por riesgo de mercado de acciones e índices accionarios de los instrumentos derivados y contratos por diferencias, mercado refiere a todas las acciones cotizadas en mercados de valores ubicados en la misma jurisdicción nacional.

Niveles mínimos aceptables de operación: corresponde al mínimo nivel de servicios o productos que se consideran aceptables para que la entidad cumpla con sus objetivos durante una interrupción.

Partes Interesadas: refiere a las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa, tales como empleados, proveedores, clientes, reguladores, entre otros.

Phishing: una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza.

Procesamiento de datos: tratamiento electrónico de datos o de los elementos básicos de información, sometidos a operaciones programadas.

Proveedor de servicios: entidad relacionada o no a la institución contratante, que preste servicios o provea bienes e instalaciones a éste.

Punto objetivo de recuperación (RPO): período de tiempo máximo antes que la pérdida de datos que sigue a un incidente se vuelva inaceptable de acuerdo con los estándares de calidad de la propia entidad.

Riesgo aceptado: corresponde al nivel de riesgo que la entidad está dispuesta a aceptar en concordancia con la política de gestión de riesgos y sus responsabilidades establecidas en el marco legal que las rige.

Riesgo de crédito: potencial exposición a pérdidas económicas debido al incumplimiento por parte de un tercero de los términos y las condiciones estipuladas en el respectivo contrato, convención o acto jurídico. Este riesgo se divide en las siguientes subcategorías:

- **Riesgo de contraparte:** exposición a potenciales pérdidas como resultado de un incumplimiento de contrato por diferencias o derivado o del incumplimiento de una contraparte en una transacción dentro de un proceso de compensación y liquidación.

- **Riesgo crediticio del emisor**: exposición a potenciales quiebras o deterioro de solvencia en los instrumentos financieros de una entidad.

Riesgo de mercado: potencial pérdida causada por cambios en los precios del mercado, que podría generar efectos adversos en la cartera propia o el balance del prestador de

servicios de intermediación de instrumentos financieros. Abarca el riesgo de tasas de interés, el riesgo cambiario y de precios en relación con los instrumentos financieros.

Riesgo inherente: corresponde a aquel riesgo que por su naturaleza no puede ser separado del proceso o subproceso en que éste se presenta. Corresponde al riesgo que debe asumir cada entidad de acuerdo con el ámbito de desarrollo de sus actividades establecido por ley.

Riesgo operacional: el riesgo operacional corresponde al riesgo de que las deficiencias que puedan producirse en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y eventualmente le originen pérdidas financieras. Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente.

Riesgo residual: aquel riesgo que persiste luego de adoptar las medidas de control y mitigación por parte de la entidad.

Servicios en la nube: servicios que proveen infraestructura, plataformas o software a lo que el cliente accede a través de la red, sin la necesidad de instalarlos en su propia infraestructura, sino que están ubicados en un servidor remoto del proveedor del servicio.

Subcontratación en cadena de servicios externalizados: las formadas por terceros subcontratados por el proveedor inicial de servicios para realizar parte importante de las actividades contratadas con éste (subcontrato de otros proveedores).

Tiempos máximos tolerables de interrupción: tiempo máximo tolerable en que un proceso pudiera estar interrumpido sin provocar efectos relevantes en la continuidad operacional.

Tiempo objetivo de recuperación: periodo de tiempo que sigue a un incidente dentro del cual: a) debe reanudarse un producto, servicio o actividad; o b) los recursos deben ser recuperados (entendiendo por recursos los activos, personas, habilidades, información, tecnología, instalaciones, suministros e información necesarios para las operaciones del negocio).

Valor razonable: el precio que se recibiría por vender un activo o se pagaría por transferir un pasivo en una transacción ordenada en el mercado principal (o más ventajoso) en la fecha de medición en las condiciones actuales del mercado (es decir, un precio de salida) independientemente de si ese precio es directamente observable o estimado utilizando otra técnica de valoración.

Vulnerabilidad: en el contexto de ciberseguridad, se refiere a cualquier debilidad de un activo de información o de un mecanismo de control que pudiera ser explotada por un ataque, es decir, puede ser un fallo en un sistema que lo torna accesible a los atacantes o cualquier tipo de debilidad en el propio activo en los procedimientos que deje la seguridad de la información de la entidad expuesta a una amenaza.

ANEXO N° 2: REPORTE DE INCIDENTES OPERACIONALES

A través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar el detalle de cada incidente descrito en la sección IV de acuerdo con el siguiente esquema:

INFORMACION	DETALLE
Fecha y hora de inicio del incidente	
Tipo de incidente	
Descripción detallada del incidente	
Causas posibles o identificadas	
Dependencias o activos afectados	
Dirección dependencias afectadas	
Canales afectados	
Nombre de proveedores involucrados	
Tipo de proveedores involucrado	
Número de clientes afectados	
Tipo de clientes afectados	
Productos o servicios afectados	
Medidas adoptadas y en curso	
Otros antecedentes	
Nombres y cargos de las personas de contacto	
Teléfono de contacto	
Fecha y hora de cierre del incidente	

Para aquellos campos en los que al momento del reporte no se cuente con la información, se debe indicar con texto "En evaluación", y para el caso de los campos numéricos, de no contarse con el dato, éstos deben completarse con un cero.

Será responsabilidad de la entidad la actualización de los antecedentes mencionados cuando se disponga de nueva información y hasta el cierre del incidente (fecha de cierre del incidente).

FECHA Y HORA DEL INICIO DEL INCIDENTE
Se debe señalar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que comenzó el incidente.

TIPO DE INCIDENTE
En este campo se debe señalar el tipo de incidente, eligiendo entre las siguientes opciones:

- Afectación de instalaciones
- Ausencia de Colaboradores
- Sin acceso dependencias y otras áreas específicas
- Falla Sistemas Base (SO, BD)
- Falla aplicativos (negocio, web, batch)
- Falla de comunicaciones
- Falla Hardware

- Falla en servicios básicos (electricidad/agua)
- Pérdida de Recursos Monetarios de la entidad, sus clientes y otras partes interesadas
- Pérdida de Información de la entidad, sus clientes y otras partes interesadas
- Interrupción/ latencia en servicios
- Error de envío de información
- Otros: especificar

DESCRIPCIÓN DETALLADA DEL INCIDENTE
En este campo se debe detallar en qué consiste el incidente reportado.

CAUSAS POSIBLES O IDENTIFICADAS
En este campo se debe realizar un análisis sobre las causas del incidente y sobre la efectividad de las medidas adoptadas para resolverlo.

DEPENDENCIAS AFECTADAS
En este campo se deben señalar las dependencias afectadas, eligiendo entre las siguientes opciones:

- Oficinas
- Sitio Producción
- Sitio Contingencia
- Dependencias proveedor
- Otros: especificar

DIRECCIÓN DEPENDENCIAS AFECTADAS (CALLE, COMUNA, REGIÓN)
En este campo se debe informar la dirección completa de la dependencia afectada. Si existe más de una dependencia afectada, se debe indicar la dirección de cada una de ellas, separándolas con un punto y coma (;).

CANALES AFECTADOS
En este campo se deben seleccionar los canales afectados por el incidente (lo que sea aplicable):

- Terminales
- Mensajería
- Servicios de custodia
- Sucursales
- Otros: especificar

NOMBRE DE PROVEEDORES INVOLUCRADOS
Corresponde al nombre o razón social del proveedor.

TIPO DE PROVEEDOR INVOLUCRADO

- Servicios básicos
- Telecomunicaciones
- Infraestructura tecnológica
- Procesamiento
- Atención telefónica
- Otros: especificar

NÚMERO DE CLIENTES AFECTADOS:
En este campo se debe completar el número de clientes que fueron afectados por el incidente que se reporta.

TIPO DE CLIENTES AFECTADOS:
En este campo se debe seleccionar el tipo de cliente afectado, entre las siguientes opciones:

- Personas
- Empresas no financieras
- Empresas financieras (Especificar)
- Clientes
- Otros: Especificar

NÚMERO DE EMPLEADOS AFECTADOS
En este campo se debe completar con el número de empleados que fueron afectados por el incidente que se reporta.

SERVICIOS AFECTADOS
En este campo se deben informar en detalle los servicios afectados por el incidente.

NÚMERO DE TRANSACCIONES AFECTADAS
En este campo se debe completar el número de transacciones que fueron afectadas por el incidente que se reporta.

MEDIDAS ADOPTADAS
En este campo se deben informar en detalle las acciones realizadas por la entidad para superar el incidente.

NOMBRE Y CARGO DE PERSONAS DE CONTACTO
Corresponden a las personas que informan el incidente y sus cargos.

TELÉFONO DE CONTACTO
Se debe señalar en este campo el teléfono celular de las personas de contacto.

FECHA Y HORA DE TÉRMINO DEL INCIDENTE
Este campo se incluirá cuando se cierra el incidente. Se debe completar la fecha (DD/MM/AAAA)
y la hora (HH:MM:SS) en que éste finalizó.

ANEXO N° 3: REPORTE DE PÉRDIDAS OPERACIONALES

A través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar al último día hábil de junio y diciembre de cada año el detalle de todos los eventos que materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento. Además, se deberán reportar los montos de gastos y recuperaciones asociados a pérdidas operacionales asociados a un mismo evento.

INFORMACION	DETALLE
Número de identificación del incidente asignado por la CMF	
Fecha de descubrimiento	
Fecha de contabilización	
Tipo de monto	
Tipo de gasto	
Tipo de recuperación	
Monto	
Nombre y cargo del informante	

NUMERO DE IDENTIFICACIÓN DEL INCIDENTE ASIGNADO POR LA CMF
Corresponde al código que identifica en forma unívoca el incidente reportado, asignado por la CMF cuando se reportó el inicio del incidente a través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

FECHA DE DESCUBRIMIENTO
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se identificó el evento de pérdida.

FECHA DE CONTABILIZACIÓN
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se imputa contablemente la pérdida o recupero en los estados financieros.

TIPO DE MONTO
Seleccionar el código que identifica el tipo de monto a reportar, de acuerdo con la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE MONTO
1	Pérdida (cargos directos en los estados de resultados)
2	Gastos (costos incurridos internos o externos con relación directa al evento operacional)
3	Recuperación

TIPO DE GASTO
Seleccionar el código que identifica el principal tipo de gasto asociado al evento de pérdida, ya sea interno o externo directamente atribuible al evento operacional, de acuerdo con la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE GASTO
1	Legales
2	Proveedores
3	Asesorías
4	Internos
5	Otros
9	No aplica (debe reportarse cuando el campo "TIPO DE MONTO" toma valores 1 o 3)

TIPO DE RECUPERACIÓN
Seleccione el código asociado a las causas de la recuperación operacional, de acuerdo con la siguiente codificación que se desplegará en este campo:

CODIGO	TIPO DE RECUPERACIÓN
1	Compañías de seguros
2	Acciones judiciales
3	Otros (liberación de provisión)
4	No aplica

MONTO
Corresponde al monto de las pérdidas, gastos o recuperaciones que deben reportarse en la fecha en la que se contabilicen.

NOMBRE Y CARGO DEL INFORMANTE
Corresponde a la persona que informa el incidente y su cargo.