MODIFICACIONES SE PRESENTAN DESTACADAS EN AMARILLO

Superintendencia de Bancos e Instituciones Financieras Chile

CIRCULAR

Bancos N°

Santiago,

RECOPILACIÓN ACTUALIZADA DE NORMAS. Capítulo 1-13

Lineamientos y buenas prácticas para la gestión de la *Ciberseguridad*.

La evolución de la industria financiera, particularmente la incorporación de las tecnologías de la información en la forma de generar, procesar y administrar sus activos de información, involucran nuevos riesgos que afectan a los procesos intrínsecos del negocio de la institución. En este ámbito la *Ciberseguridad*, concepto que comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta, es fundamental para evitar los efectos adversos de sus riesgos y amenazas inherentes sobre la seguridad de la información y la continuidad del negocio.

En dicho contexto, el presente cambio normativo establece diversos aspectos para la gestión de la seguridad de los activos de información sujetos a riesgo en el ciberespacio que serán parte de la evaluación de gestión establecida en el Capítulo 1-13 de la Recopilación Actualizada de Normas, específicamente la letra C) del numeral 3.2 del Título II sobre la Administración del Riesgo Operacional.

Por otra parte, esta normativa también considera la necesidad de generar una base de incidentes de *Ciberseguridad* bajo un estándar común, que tiene por objeto establecer un lenguaje y nivel de información mínimo y homogéneo en la industria.

Como consecuencia de los cambios señalados, se introducen los siguientes ajustes al Capítulo 1-13 de la referida Recopilación:

a) Se intercala lo siguiente como cuarto párrafo de la letra C) del numeral 3.2 del título II:

> "Asimismo, es esencial que las instituciones cuenten con una clara definición, caracterización e identificación de los principales activos de información y de la infraestructura física que soporta y resguarda la seguridad de los mismos. En este ámbito, las entidades también deben gestionar la seguridad de sus activos de información expuestos a riesgos en el ciberespacio, entendido este como el entorno que permite la interacción lógica, es decir no física, mediante la conexión de redes tecnológicas.".

b) Se complementa la situación descrita en la duodécima viñeta del párrafo séptimo de la letra C) del numeral 3.2 del título II, agregando a continuación del punto aparte, que pasa a ser punto seguido, lo siguiente: "Asimismo, la entidad ha dispuesto de estructuras dedicadas a la gestión de la *Ciberseguridad* que al menos contemplan los aspectos descritos en el Anexo N° 3 de este Capítulo".

c) Se introduce el nuevo Anexo N° 3, que contiene los lineamientos de gestión que deben ser considerados en el ámbito de la *Ciberseguridad* y establece la necesidad de generar y mantener una base de incidentes sobre la materia, bajo las condiciones que allí se describen.

Se acompañan las siguientes hojas del Capítulo 1-13 de la Recopilación Actualizada de Normas: hojas N°s 13 a 17 y la que contiene su nuevo Anexo N° 3.

Saludo atentamente a Ud.,

ERIC PARRADO HERRERA
Superintendente de Bancos e Instituciones Financieras

CAPÍTULO 1-13

CLASIFICACIÓN DE GESTIÓN Y SOLVENCIA

El presente Capítulo contiene las disposiciones relativas a la clasificación que de los bancos, según su solvencia y gestión, debe mantener en forma permanente esta Superintendencia, de acuerdo con lo establecido en el Título V de la Ley General de Bancos. Adicionalmente, en el Capítulo se incorporan los aspectos esenciales de gestión del capital incluidos en el nuevo acuerdo de Basilea (Basilea II).

I. CLASIFICACION DE LOS BANCOS.

1. Categorías.

Conforme a lo establecido en el Título V de la Ley General de Bancos, esta Superintendencia debe mantener clasificadas a los bancos, según su gestión y solvencia, en una de las siguientes categorías:

Categoría I: Incluye a los bancos clasificados en nivel A de solvencia y nivel A de gestión.

Categoría II: Incluye a los bancos clasificados en nivel A de solvencia y nivel B de gestión, en nivel B de solvencia y en nivel A de gestión, o en nivel B de solvencia y nivel B de gestión.

Categoría III: Incluye a los bancos clasificados en nivel B de solvencia y por dos o más veces consecutivas en nivel B de gestión. Asimismo, estarán en esta categoría las instituciones que se encuentren clasificadas en nivel A o B de solvencia y en nivel C de gestión.

Categoría IV: Incluye a los bancos que se encuentren clasificados en nivel A o B de solvencia y, por dos o más veces consecutivas, en nivel C de gestión.

Categoría V: Incluye a los bancos que se encuentren clasificados en nivel C de solvencia, cualquiera sea su nivel de gestión.

Las reglas antes mencionadas se resumen en el cuadro del Anexo N° 1 de este Capítulo.

2. Permanencia de la clasificación.

La clasificación de un banco rige a partir de la fecha en que ella sea comunicada por esta Superintendencia y hasta la fecha en que reciba una nueva comunicación en ese sentido.

Para este efecto, se informarán a cada banco los cambios en su nivel de gestión y en su nivel de solvencia, en las oportunidades que en cada caso corresponda, según lo indicado en los numerales 3.2 y 4.2 de este título.

3. Clasificación de gestión.

3.1. Niveles de gestión.

De acuerdo con la ley, los niveles de gestión deben determinarse según lo siguiente:

Nivel A: Bancos no clasificados en los niveles B o C.

Nivel B: Instituciones que reflejan debilidades relacionadas con los controles internos, sistemas de información para la toma de decisiones, seguimiento oportuno de los riesgos, clasificación privada de riesgo y capacidad para enfrentar escenarios de contingencia. Las debilidades de que se trate deben ser corregidas durante el período que preceda al de la próxima calificación, para evitar un deterioro paulatino de la solidez del banco. También deben considerarse las sanciones aplicadas a la empresa, salvo las que se encuentren con reclamación pendiente.

Nivel C: Instituciones que presenten deficiencias significativas en alguno de los factores señalados en el Nivel anterior, cuya corrección debe ser efectuada con la mayor prontitud para evitar un menoscabo relevante en su estabilidad.

3.2. Oportunidad de la clasificación de gestión.

La clasificación de un banco según gestión, se realizará a lo menos una vez en cada año calendario.

Conforme a lo dispuesto en la ley, el nivel de gestión asignado será notificado a la respectiva institución por esta Superintendencia dentro de los cinco días siguientes a la fecha en que la clasificación se resuelva.

En la notificación se indicarán los fundamentos que determinaron la asignación del nivel de gestión y la clasificación que, consecuentemente, le corresponde al banco de acuerdo con lo indicado en el N° 1 de este título, la que regirá a contar de la fecha de esa comunicación.

La asignación del nivel de gestión de un banco se basará en la evaluación practicada por este Organismo que se describe en el título II de este Capítulo.

4. Clasificación de solvencia.

4.1. Niveles de solvencia.

De acuerdo con la ley, los niveles de solvencia señalados en el N° 1 de este título, se determinan según la relación que registren los bancos entre su patrimonio efectivo, deducidas las pérdidas acumuladas en el ejercicio, y la suma de los activos ponderados por riesgo netos de las provisiones exigidas. Corresponde el Nivel A de solvencia, cuando esa relación sea igual o superior al 10%; el Nivel B, cuando esa relación sea igual o superior al 8% e inferior al 10%; y, el Nivel C, cuando tal relación sea inferior al 8%.

El patrimonio efectivo y los activos ponderados por riesgo se calcularán según lo previsto en el Capítulo 12-1 de esta Recopilación.

Si bien la evaluación de solvencia tiene su correspondencia en lo establecido en el Capítulo 12-1 de esta Recopilación, resulta claro que los indicadores de solvencia también reflejan el adecuado uso de los recursos patrimoniales aportados por los accionistas para llevar a cabo las actividades del banco. Esto significa, entre otros aspectos, que debe existir una concordancia entre el nivel de capital que debe ser mantenido, en un contexto de mediano y largo plazo, y la gestión llevada a cabo por la administración para optimizar el uso de los recursos. Esa concordancia entre el nivel de capital y la gestión se ve plasmada en la estrategia de negocios que aborda y los riesgos que asume, en particular frente a escenarios de estrés. En suma, los niveles de patrimonio, así como su composición entre capital primario y secundario (capital básico y patrimonio efectivo) también deben obedecer a un análisis de sus necesidades en un contexto de mediano y largo plazo, lo cual, en definitiva, debiera quedar manifestado en la planificación de sus actividades.

4.2. Oportunidad de la clasificación de solvencia.

Dado que los niveles de solvencia son conocidos mensualmente, en caso de que en banco deba cambiarse dicha clasificación, esta Superintendencia se lo notificará dentro del mes siguiente a aquel a que se refiere la información que refleja el nuevo nivel.

En esa comunicación se dejará constancia de la categoría que por la clasificación de gestión y solvencia le corresponde al banco de acuerdo con las reglas mencionadas en el N° 1 de este título, considerando el cambio en el nivel de solvencia a que se refiere este numeral.

II. EVALUACION DE LA GESTION DE LOS BANCOS.

1. Orientación general de la evaluación de la gestión según lo previsto en la ley.

De acuerdo con lo establecido en el artículo 62 de la Ley General de Bancos, las observaciones que emanen de la evaluación de esta Superintendencia deben tener relación con los controles internos, sistemas de información para toma de decisiones, seguimiento oportuno de los riesgos, clasificación privada de riesgos y capacidad para enfrentar escenarios de contingencia. La importancia relativa de las debilidades asociadas a uno o más de esos conceptos genéricos de distinta especie, se relacionan en la ley con la clasificación en los niveles B o C de gestión, debiéndose considerar también, para efectos de la clasificación, las sanciones aplicadas a la empresa que no se encuentren con reclamación pendiente. Según la ley, son debilidades propias de una clasificación en el Nivel B de gestión, aquellas deficiencias que deben ser corregidas antes de la próxima clasificación para evitar un deterioro paulatino en la solidez de un banco, en tanto que son debilidades que obligan a clasificar en el Nivel C, aquéllas que acarrean un menoscabo relevante para la estabilidad de la empresa y que, por lo tanto, requieren de correcciones con la mayor prontitud.

De lo indicado se desprende que la evaluación de esta Superintendencia debe apuntar al examen de las debilidades que perturban o pueden perturbar la solidez o estabilidad de los bancos en el corto o largo plazo.

En ese contexto, el enfoque de esta Superintendencia para esa evaluación, no puede sino concordar con principios de sana administración para el resguardo de la estabilidad o buena marcha de la empresa, donde el Directorio y la alta administración de cada entidad evaluada velen por una gestión eficaz de todos los riesgos importantes que asume o enfrenta en su caso, y que sus objetivos y planes estratégicos se basen en apreciaciones debidamente fundamentadas de su entorno y recursos.

Junto con lo anterior, este Organismo también considerará como factores esenciales para la clasificación, la adhesión a la normativa por parte del banco evaluado y el debido cumplimiento de los compromisos que haya asumido con esta Superintendencia y con otros organismos reguladores en lo que corresponda.

2. Proceso de evaluación.

La evaluación de una entidad se realizará a través de diversas visitas de inspección, como asimismo mediante el análisis de información acerca del banco evaluado y de reuniones para estar al corriente de acontecimientos que inciden o pueden incidir en la marcha normal de la institución.

En todo caso, antes de realizar el proceso de clasificación de la gestión a que se refiere el numeral 3.2 del título I de este Capítulo, se efectuará una visita final, en la cual se harán las tareas necesarias para completar la evaluación y obtener las conclusiones definitivas respecto a la situación de la empresa.

Conforme a lo previsto en la ley, en la evaluación se considerarán los informes de los evaluadores privados que se refieran a debilidades atinentes a la gestión.

Respecto a las demás opiniones independientes que provengan de un examen de aspectos inherentes a la gestión de un banco, se tendrán en consideración, en la medida en que revelen debilidades importantes que toquen el contexto de la evaluación de esta Superintendencia, los informes de las auditorías externas, como asimismo, en el caso de bancos que tengan sucursales o filiales en el exterior, la información entregada por los organismos reguladores de los países anfitriones.

3. Descripción del alcance de la evaluación.

El Directorio, en tanto órgano colegiado encargado de la administración del banco, tiene un rol preponderante respecto de cada una de las materias sujetas a la evaluación de esta Superintendencia y que se precisan en el numeral 3.2 siguiente, en los términos que se detallan a continuación:

3.1. Gobierno corporativo y el rol del Directorio

Para efectos del presente Capítulo, se entenderá que el gobierno corporativo es el conjunto de instancias, directrices y prácticas institucionales que influyen en el proceso de toma de decisiones del banco, contribuyendo entre otras a la creación sustentable de valor, en un marco de transparencia y de una adecuada gestión y control de los riesgos.

El Directorio es el principal articulador de su gobierno corporativo y de una gestión prudente de los riesgos que enfrenta la entidad. En ese contexto, resulta fundamental que la labor estratégica del Directorio, orientada a la fijación de políticas y evaluación de su cumplimiento, se mantenga separada de las funciones propias de los gerentes u otras instancias en las que delega su implementación definitiva.

Respecto de las instituciones bancarias que no mantengan Directorio en Chile, como sucede con las sucursales de bancos extranjeros, el cumplimiento de los lineamientos constitutivos de un buen gobierno corporativo señalados en este Capítulo alcanza a las instancias que hagan sus veces en la sucursal o en la casa matriz, según corresponda a su estructura organizacional. En estos casos, los aspectos de buen gobierno corporativo se verifican a través de las políticas, prácticas y procedimientos determinados por la sociedad matriz a nivel global o regional, según corresponda.

3.1.1 Elementos de un buen gobierno corporativo.

Las siguientes materias son consideradas inherentes a un buen gobierno corporativo y repercuten en una buena gestión de las materias que son objeto de evaluación, según lo indicado en el numeral 3.2 siguiente, por lo que serán vistas y ponderadas de acuerdo a las características propias de cada banco:

a) Establecimiento de objetivos estratégicos, valores corporativos, líneas de responsabilidad, monitoreo y rendición de cuentas.

Esta Superintendencia considera que el Directorio, de acuerdo al mandato legal que establece su competencia, debe definir y aprobar tanto los objetivos como el plan estratégico de la institución, promoviendo una gestión del capital de mediano y largo plazo acorde con el perfil de riesgo que haya definido, considerando a su vez una debida protección a los intereses de los accionistas y del público en general.

Para cumplir con tales responsabilidades, el Directorio debe ser capaz de establecer y sancionar los valores corporativos que identifican al banco y complementan sus objetivos estratégicos, considerando también las líneas de responsabilidad necesarias para asegurar su adecuada implementación.

En la evaluación de las distintas dimensiones que abarcan las materias mencionadas, se considerarán situaciones como las que se describen a continuación:

- La entidad mantiene políticas formalmente establecidas para la administración de los distintos riesgos que se tratan en el numeral 3.2 siguiente. Dichas políticas son aprobadas por el Directorio, procurando que sean consistentes con el plan estratégico y los valores institucionales.

- Los valores corporativos están recogidos en un código o manual, que abordan aspectos tales como los principios institucionales, los imperativos de conducta para sus empleados, las reglas sobre posibles conflictos de interés y la manera como son prevenidos y solucionados, entre otros.

- La implementación del plan estratégico y los valores corporativos es realizada por personal designado para dichos efectos, quienes a su vez informan y rinden cuenta al Directorio de manera periódica, con el objeto de monitorearlos y evaluar posibles cambios.

- El Directorio establece líneas claras de responsabilidad, para asegurar que los objetivos estratégicos y valores corporativos sean divulgados mediante mecanismos formales, establecidos por él mismo o por la instancia a la cual delega tal responsabilidad, de manera de lograr su oportuno y cabal entendimiento y aplicación al interior de la institución.

- Las actas levantadas en cada sesión del Directorio reflejan con claridad todos los asuntos tratados en cada reunión, tales como los acuerdos o compromisos tomados y el seguimiento de los mismos; los planes de acción y asignación de responsabilidades; así como el estado de avance de proyectos estratégicos, entre otros.

- El Directorio cuenta con el apoyo de diversos comités, acordes a la naturaleza y complejidad de las actividades del Banco, en los que participan uno o más integrantes del mismo y que le permiten tratar y monitorear aspectos específicos de su competencia.

b) Verificación del desempeño de la alta administración y cumplimiento con las políticas establecidas por el Directorio.

Para fines del presente Capítulo se entenderá que la alta administración está conformada tanto por aquellos individuos a quienes el Directorio ha encargado la responsabilidad de implementar el plan estratégico de la entidad y las políticas para gestión de los riesgos de que trata este Título, como también aquellos que pueden comprometer al Banco para tales efectos, dadas sus atribuciones.

La existencia de elementos como los que se describen a continuación, dan cuenta de que el Directorio verifica el cumplimiento de su mandato:

- El Directorio cuenta con políticas previamente definidas relativas a la selección, evaluación, remoción y sucesión de las distintas instancias que conforman la alta administración, acordes con la naturaleza particular de las mismas, las que son ajustadas y revaluadas en el tiempo.

- El Directorio procura el desarrollo de mecanismos formales para la evaluación de la alta administración, con el objeto de velar por la implementación y buen cumplimiento de sus políticas y decisiones. Para dicho fin el Directorio se informa periódicamente, en la oportunidad y a través de los medios que defina para tales efectos, de los resultados que generen dichos mecanismos.

- El Directorio cuenta con mecanismos de autoevaluación periódica, que le permiten identificar oportunidades de mejoramiento en su propia gestión.

- Existe una clara designación de responsabilidades y segregación de funciones al interior de la entidad, que permite una adecuada contraposición de intereses.

- Se promueve una cultura de rendición de cuentas, a través de canales que son conocidos y aprobados por el Directorio para tales efectos. Dichos canales permiten el flujo y respaldo de la información, de manera segura y fidedigna.

- Los sistemas de información habilitados para transparentar el funcionamiento de la entidad, especialmente en lo que respecta a la gestión de riesgos y la efectividad de sus mecanismos de control, consideran la presentación completa, periódica y oportuna de informes al Directorio.

c) Promoción de controles internos sólidos y de una auditoría efectiva.

Para garantizar una gestión prudente de la institución y de los riesgos sujetos a esta evaluación, el Directorio debe impulsar el establecimiento de procedimientos y sistemas de control interno, acordes con la naturaleza de las actividades desarrolladas por el banco y la complejidad de la estructura organizacional que las sustenta.

Para que la función de auditoría interna se desarrolle eficazmente y con la debida independencia, es indispensable que el compromiso del Directorio se plasme a través de la entrega de un marco de acción general, la definición de una estructura jerárquica adecuada y de una apropiada validación, tanto de las observaciones levantadas como de las acciones propuestas para superarlas.

Dicho nivel de compromiso también debe manifestarse a través del Comité de Auditoría, instancia responsable de entregar apoyo al Directorio en la evaluación constante de la calidad de los sistemas de control interno, el reforzamiento de la función de auditoría interna y la vinculación y coordinación con los auditores externos.

A continuación se describen algunos elementos que entregan indicios de una buena gestión y un adecuado involucramiento del Directorio en las materias antes descritas:

- El Directorio ha definido y utiliza indicadores de gestión, que le permiten hacer seguimiento de los asuntos claves de la institución, en ámbitos tales como el financiero, operacional, regulatorio y de capital humano.

- El Directorio del banco ha definido formalmente lo que constituye el rol de la función de auditoría interna, explicitando sus objetivos y alcances, su posición dentro de la entidad, su organización, atribuciones, responsabilidades y relaciones con otras áreas de control. En este contexto, el Directorio promueve la suficiencia y calidad de los recursos materiales y humanos disponibles para ejercer su función.

- El Directorio de la entidad aprueba el plan de auditoría anual y recibe información periódica sobre su grado de cumplimiento.

d) Mecanismo de divulgación de información

La disponibilidad de información completa, fidedigna y oportuna es una condición indispensable para la adecuada gestión del banco, por lo que el Directorio debe establecer los contenidos mínimos que considere adecuados y tomar las medidas que estime necesarias para su divulgación en las instancias pertinentes, tanto al interior como exterior de la entidad, ejerciendo el control de su cumplimiento.

Parte de la información a divulgar deberá comprender aspectos de interés público, tales como los definidos en el Título V del Capítulo 1-4 de esta Recopilación, que permitan a los accionistas y a las demás partes interesadas tener un conocimiento adecuado de la entidad, de sus políticas y de los principios que la rigen, definidos por el mismo Directorio.

3.2. Administración y control de los riesgos y otras materias sujetas a evaluación.

En los literales siguientes se describe brevemente la orientación de la evaluación, considerando para el efecto las siguientes agrupaciones de materias:

A) Administración del riesgo de crédito y gestión global del proceso de crédito.

B) Gestión del riesgo financiero y operaciones de tesorería.

C) Administración del riesgo operacional.

D) Administración de los riesgos de exposiciones en el exterior y control sobre las inversiones en sociedades.

E) Prevención del lavado de activos y del financiamiento del terrorismo.

F) Administración de la estrategia de negocios y gestión del capital.

G) Gestión de la calidad de atención a los usuarios y transparencia de información.

H) Gestión de la función de auditoría interna y rol del comité de auditoría.

Las materias indicadas en las letras A), B), C), D) y E) se relacionan principalmente con el seguimiento oportuno de los riesgos. Las señaladas en las letras F) y G) están relacionadas especialmente con la capacidad para enfrentar escenarios de contingencia y, finalmente, la mencionada en la letra H) guarda relación con el control interno. Respecto a los sistemas de información para la toma de decisiones a que se refiere la ley, ellos están presentes, en general, en todas las materias.

A) Administración del riesgo de crédito y gestión global del proceso de crédito.

La evaluación comprende el examen de la gestión del riesgo de crédito y de los factores de riesgo del proceso de crédito, que va desde la definición del mercado objetivo hasta la recuperación de los préstamos.

En la evaluación interesa, en primer lugar, la compatibilidad entre las políticas y procedimientos establecidos por la entidad, con respecto al volumen y complejidad de sus operaciones y su estrategia comercial. Junto con ello, se examinará la manera en que se han establecido las políticas y la forma en que el Directorio participa en su aprobación y supervisa su cumplimiento, como asimismo la calidad y efectividad de los controles orientados a asegurar el cumplimiento de las políticas y procedimientos inherentes a las colocaciones.

Serán también materia de examen la suficiencia y eficacia de las segregaciones funcionales, especialmente las que deben existir entre las áreas comerciales y aquellas encargadas de la función de administración del riesgo y de auditoría interna. En esto es esencial, por una parte, que la administración del riesgo de crédito sea una contraparte efectiva de las áreas tomadoras de riesgo y, por otra, que la posición independiente de la función de auditoría interna permita una adecuada cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.

En lo que toca a la administración del riesgo de crédito, se evaluarán los mecanismos y técnicas de detección, acotamiento y reconocimiento oportuno de los riesgos que asume la entidad en el desarrollo de sus actividades de crédito. En este ámbito, es clave la capacidad de la entidad para mantener permanentemente bien clasificada su cartera, su dominio sobre los factores de riesgo asociados a sus operaciones y su disposición para reconocer en forma oportuna en sus resultados los riesgos individuales de crédito a que está expuesta, como también su capacidad para limitar los riesgos de concentración de la cartera en general.

Asociado a lo anterior, constituye también un aspecto relevante de la evaluación, el examen de la cobertura y profundidad de la información acerca de los deudores, tanto aquella referida a su comportamiento de pago, incluyendo la adecuada administración de su cuenta corriente en el banco, como a sus condiciones financieras generales.

En relación con lo descrito precedentemente, una buena gestión puede manifestarse, por ejemplo, en circunstancias tales como:

- La entidad mantiene políticas para la administración de los riesgos aprobadas por el Directorio, que atienden la importancia de los riesgos considerando el volumen y complejidad de las operaciones, las proyecciones de crecimiento y el desarrollo de nuevos negocios.

- Las políticas aprobadas para la administración de los riesgos consideran especialmente la identificación, cuantificación, limitación y control de las grandes exposiciones en clientes, grupos o sectores económicos.

- La estructura de límites, tanto en lo que toca al riesgo individual de las operaciones como al riesgo de portafolio, es consecuente con un nivel tolerable de exposición al riesgo según sus condiciones financieras generales.

- Las políticas y procedimientos relacionados con la administración de los riesgos son conocidos y respetados por todo el personal involucrado. Asimismo, los procedimientos establecidos para las distintas etapas del proceso de crédito, están arraigados en el banco.

- La entidad cuenta con mecanismos que le permiten una medición y seguimiento oportuno del riesgo asumido, plenamente compatibles con el volumen y complejidad de las operaciones.

- Las operaciones con partes relacionadas se sujetan a criterios prudenciales de administración del riesgo y se otorgan en las mismas condiciones que los demás créditos.

- La función de administración del riesgo de crédito se desarrolla en forma independiente de las áreas de negocio. Las opiniones emitidas por los responsables de esa función, son reconocidas y consideradas por los distintos niveles de la organización pertinentes.

- Los sistemas de información permiten hacer un seguimiento continuo de la exposición a los riesgos. Poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones.

- Las auditorías internas cubren con una adecuada identificación, cuantificación y priorización, los distintos riesgos relacionados con las colocaciones.

- La entidad mantiene sanas prácticas de administración financiera que comprenden la plena identificación, medición y control de todos los riesgos de sus clientes y de los productos que estos contratan y de aquellos que unilateralmente entrega el banco como, por ejemplo, en el caso de la aprobación de sobregiros no pactados. Estos se documentan adecuadamente, se constituyen los resguardos necesarios y se evalúa la continuidad del contrato de cuenta corriente cuando un cliente los ocasiona en forma reiterada.

B) Gestión del riesgo financiero y operaciones de tesorería.

La evaluación comprende el manejo de los riesgos de liquidez y precios (tasas de interés y tipos de cambio) y la gestión de las operaciones de tesorería financiera en general. El examen se centra en los elementos claves que aseguran una adecuada identificación, cuantificación, limitación y control de los riesgos.

En esta materia es particularmente importante el alcance de las políticas y la compenetración del Directorio en la aprobación de las mismas y en los riesgos asociados a nuevos productos u operaciones; la eficacia de los límites que acotan los riesgos en relación con la filosofía general de riesgo del banco y su situación financiera general; la forma en que la entidad está organizada para abordar integralmente la administración del riesgo financiero; la efectividad de los sistemas de vigilancia y de los métodos de ingeniería financiera utilizados; y, la fortaleza de los controles operativos.

De la evaluación merecen destacarse las actividades dirigidas a examinar: la eficacia de la separación funcional entre las áreas tomadoras de riesgo, de seguimiento o control y de operación, lo cual constituye un factor crítico de control; la compatibilidad entre las técnicas de administración de riesgo utilizadas y el nivel y complejidad de las operaciones que realiza el banco; la calidad de la información tanto estratégica como operativa; y, la efectividad de las auditorías internas.

A efectos ilustrativos, una buena gestión en relación con esta materia puede manifestarse en situaciones tales como:

- Los riesgos de las posiciones y negocios individualmente considerados, como asimismo el riesgo consolidado del banco, están acotados por límites aprobados por el Directorio, compatibles con las actividades, estrategias y objetivos de la empresa. Tanto para la aprobación de dichos límites como de las políticas que, en general, condicionan las operaciones de tesorería, al igual que para el seguimiento posterior de su cumplimiento y eficacia, el Directorio cuenta con la información necesaria para apreciar cabalmente la sustentación y los riesgos a que está expuesta la institución.

- La empresa está organizada para manejar los riesgos financieros en forma integral. La planificación, administración y control constituyen procesos asentados en los distintos niveles de la organización; y la alta administración cuenta con la información necesaria para la evaluación periódica de los mismos.

- La responsabilidad de la administración de activos y pasivos depende de alguna de las instancias que conforman la alta administración, cuya función permite acotar el riesgo a niveles razonables, manteniendo políticas y estrategias financieras consecuentes con los lineamientos de exposición al riesgo sancionados por el Directorio y con las estrategias comerciales del banco.

- Los nuevos productos, en forma previa a su lanzamiento, son sometidos a un riguroso análisis de los riesgos involucrados.

- La evaluación y control de los riesgos se desarrolla con suficiente independencia de las áreas tomadoras de riesgo, contándose con personal especializado y soportes acordes con el alcance, tamaño y complejidad de las actividades del banco y con los riesgos que ésta asume.

- Las responsabilidades y atribuciones se encuentran claramente definidas, existiendo asignaciones de responsabilidades y niveles jerárquicos apropiados para las funciones claves de negociación, operación y control.

- El sistema de información para la toma de decisiones provee información oportuna y confiable para cautelar la exposición a los riesgos financieros. La información cubre apropiadamente los riesgos financieros y las diversas operaciones de tesorería, permitiendo a los usuarios tomar decisiones bien fundadas en relación con las posiciones y la gestión financiera.

- El banco cuenta con mecanismos para una adecuada identificación, cuantificación y limitación de los riesgos de liquidez y precio, acordes con el grado de refinamiento y complejidad de las transacciones y la naturaleza de los riesgos asumidos. Utiliza herramientas de ingeniería financiera compatibles con los riesgos que asume y mantiene procedimientos adecuados para enfrentar contingencias.

- La extensión y profundidad de las auditorías es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar el cumplimiento de las políticas, la eficacia de los procedimientos (de operación, control de riesgos, contables y legales) y los sistemas de información.

En todo caso, los criterios de evaluación de la política de administración de liquidez se basan en el cumplimiento de lo dispuesto en el Capítulo III.B.2.1 del Compendio de Normas Financieras del Banco Central de Chile y del Capítulo 12-20 de esta Recopilación. En lo que respecta a los riesgos de mercado tratados en el Capítulo III.B.2.2 de ese Compendio de Normas Financieras y en el Capítulo 12-21 de esta Recopilación, se entenderá que la política de administración de estos riesgos concuerda con los criterios mínimos de evaluación, cuando dicha política considere todos los aspectos señalados en el Anexo N° 2 de las presentes normas.

C) Administración del riesgo operacional.

Esta Superintendencia considera como marco referencial, la definición de riesgo operacional propuesta por el Comité de Basilea. Por lo tanto, se entenderá como tal el riesgo de pérdidas resultantes de una falta de adecuación o de una falla de los procesos, del personal y de los sistemas internos o bien por causa de acontecimientos externos.

En este contexto resultará de interés para la evaluación que sobre el referido riesgo hará la Superintendencia, el rol asumido por el Directorio y la aprobación que han dado a la estrategia a utilizar en su administración, entendiendo este riesgo como de una categoría distinta de los riesgos bancarios tradicionales.

Dicha estrategia, atendida la importancia relativa y el volumen de operaciones de la entidad, debe contemplar una definición clara de lo que considerará como riesgo operacional y establecer los principios para su identificación, evaluación, control y mitigación. En este sentido, si la exposición al riesgo es significativa, cobra relevancia la existencia de definiciones precisas de lo que se entenderá por pérdidas operacionales, ya sean esperadas o inesperadas, por cuanto los tratamientos de mitigación son diferentes en uno y otro caso.

Asimismo, es esencial que las instituciones cuenten con una clara definición, caracterización e identificación de los principales activos de información y de la infraestructura física que soporta y resguarda la seguridad de los mismos. En este ámbito, las entidades también deben gestionar la seguridad de sus activos de información expuestos a riesgos en el ciberespacio, entendido este como el entorno que permite la interacción lógica, es decir no física, mediante la conexión de redes tecnológicas.

En la evaluación que hará este Organismo, interesa observar la compatibilidad entre las políticas y procedimientos aprobados por el Directorio, con respecto al volumen, sofisticación y naturaleza de sus actividades. Asimismo, se examinará la manera en que se han establecido las políticas y la forma en que el Directorio de la empresa participa en su aprobación y supervisa su cumplimiento.

Será también materia de examen comprobar si la posición independiente de la función de auditoría interna permite una adecuada cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.

En ese sentido, revelan una buena gestión, por ejemplo, situaciones o hechos tales como:

- El Directorio procura el establecimiento de una definición de riesgo operacional y lo reconoce como un riesgo gestionable. Especial importancia tendrá la existencia de una función encargada de la administración de este tipo de riesgo.

- La entidad mantiene políticas para la administración de los riesgos operacionales aprobadas por el Directorio, que atienden la importancia relativa de los riesgos operacionales considerando el volumen y complejidad de las operaciones.

- La estrategia de administración del riesgo operacional definida por el banco, es consistente con el volumen y complejidad de sus actividades y considera el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad. Esta estrategia ha sido implementada a través de toda la organización bancaria, y todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración de este riesgo.

- La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en el banco (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.

- La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas. Asimismo, se asegura que antes de introducir nuevos productos, emprender nuevas actividades, o establecer nuevos procesos y sistemas, el riesgo operacional inherente a los mismos esté sujeto a procedimientos de evaluación.

- El banco ha integrado a sus actividades normales el monitoreo del riesgo operacional y ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.

- El banco es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.

- Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales. Poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones, de acuerdo a las necesidades propias de las distintas instancias organizacionales.

- El banco cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitoreos a las actividades de dichas partes.

- El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

- El banco cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.

- El banco cuenta con una estructura que permite administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad. Asimismo, la entidad ha dispuesto de estructuras dedicadas a la gestión de la *Ciberseguridad*, que al menos contemplan los aspectos descritos en el Anexo N° 3 de este Capítulo.

- El banco considera en sus planes de continuidad del negocio y contingencia, diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones y en ese sentido ha desarrollado una metodología formal que considera en sus etapas, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación, así como pruebas periódicas de tales estrategias.

- El banco ha implementado un proceso para controlar permanentemente la incorporación de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias de manera de reducir la frecuencia y severidad de los eventos de pérdida. Asimismo, el Directorio y la alta administración reciben reportes periódicos, con la información pertinente al rol que desempeñan.

- La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.

- La extensión y profundidad de las auditorías es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.

Sin perjuicio de lo anterior, en lo que se refiere específicamente a la gestión de la continuidad del negocio, la evaluación de esta Superintendencia cubrirá los aspectos que se detallan en el Capítulo 20-9 de esta Recopilación.

D) Administración de los riesgos de exposiciones en el exterior y control sobre las inversiones en sociedades.

La evaluación abarcará el control sobre las sucursales en el exterior, filiales y sociedades de apoyo al giro, ubicadas en el país o en el extranjero. Por otra parte, también incluye la gestión global de las operaciones de crédito hacia el exterior, las inversiones minoritarias en sociedades y las transacciones efectuadas en el extranjero, en general.

En lo que se refiere a la presencia de sucursales en el exterior, filiales y sociedades de apoyo al giro, interesa la suficiencia y efectividad del control ejercido por la matriz. Al respecto se espera un control permanente de las entidades, acorde con las peculiaridades del entorno en que ellas se desenvuelven y su grado de autonomía, que permita el seguimiento de su marcha y una reacción oportuna frente a factores perturbadores.

En la evaluación de la gestión global de los préstamos y operaciones en el exterior, incluidas aquellas efectuadas desde el exterior con terceros países, constituye un elemento clave el dominio que tiene el banco sobre el riesgo-país (riesgo soberano y de transferencia), y que pasa por un análisis permanente de la situación de los países en que compromete sus recursos y la fijación de límites en relación con la concentración de cartera en cada país.

Con respecto al riesgo de crédito, el enfoque de la evaluación no difiere del mencionado en la letra A) de este numeral 3.2. Por lo mismo, interesa particularmente la suficiencia de la información relativa a los deudores y al comportamiento de su entorno, y los criterios para la fijación de límites de crédito que atiendan a las características de los deudores y tipo de financiamiento.

Por otra parte, dado que en las operaciones con el exterior adquiere una relevancia especial el manejo del riesgo legal, merece destacarse también el examen de los procedimientos que permiten operar con un conocimiento fundado y oportuno de los efectos contractuales.

Al igual que en las otras materias antes descritas, la evaluación apunta asimismo a asegurarse de la eficacia de las auditorías internas. En el caso de las sucursales en el exterior, filiales y sociedades de apoyo al giro, tanto nacionales como en el exterior, es importante también, en este aspecto, la forma en que se cubre la función de auditoría.

Una gestión óptima en relación con lo señalado en este numeral, la mostrarían, por ejemplo, situaciones globales como las siguientes:

- El Directorio ejerce una supervisión efectiva sobre la alta administración, para asegurar que el banco maneja los riesgos de sus inversiones y operaciones internacionales en forma sana y segura.

- Las sucursales en el exterior, las filiales y sociedades de apoyo al giro en el país y en el extranjero, están sujetas a un control permanente y con medios que permiten tomar las medidas correctivas oportunas en caso de ser necesario, tanto en lo que se refiere a la marcha de los negocios, riesgos (patrimoniales y de reputación), rentabilidad y compromisos de capital, como en lo que se refiere a la verificación del cumplimiento de directrices o políticas de la matriz y, particularmente, para el caso de sucursales en el exterior del cumplimiento de las regulaciones de los países anfitriones.

- Las políticas para administrar el riesgo-país exigen una evaluación permanente de los países en los cuales se mantienen exposiciones y contemplan límites de exposición acordes con la situación financiera general del banco, debidamente aprobados y sujetos a seguimiento. Los procedimientos de evaluación del riesgo país contemplan el análisis por parte de profesionales independientes e idóneos, tanto de los factores económicos como de los políticos y sociales que en alguna medida podrían repercutir en el normal retorno de los flujos de las inversiones.

- Las estrategias comerciales en relación con las operaciones en el exterior, son compatibles con la capacidad del banco para efectuarlas bajo control de los riesgos. Las decisiones sobre nuevos negocios u operaciones con contrapartes radicadas en el exterior, son tomadas sobre la base de un análisis previo de todos los riesgos inherentes, cubriéndose en consecuencia, sistemáticamente, el riesgo país, el riesgo de crédito, el riesgo financiero, el riesgo legal y el riesgo operativo que derive de las peculiaridades de las operaciones.

- En el caso de las filiales, el banco ha establecido mecanismos que le permiten asegurarse de que las políticas relativas a riesgos, son consistentes con sus propias políticas. Asimismo, puede obtener mediciones consolidadas de los riesgos más relevantes, utilizando metodologías adecuadas a la escala y complejidad de los negocios llevados a cabo.

E) Prevención del lavado de activos y del financiamiento del terrorismo.

La evaluación comprende un análisis del rol que desempeña el Directorio sobre las actividades de prevención de lavado de activos y del financiamiento del terrorismo, así como también la existencia de un marco de políticas y procedimientos, los que deben ser acordes al tamaño y complejidad de las operaciones del banco y sus filiales.

Son también materia de revisión, los procedimientos eficaces sobre "conozca a su cliente", la presencia de un oficial de cumplimiento, la existencia de políticas relacionadas con selección de personal, la existencia de un código de conducta interno y de una función de auditoría independiente, responsable de evaluar periódicamente el cumplimiento de las políticas y procedimientos.

En este sentido, revelan una buena gestión, por ejemplo, situaciones o hechos como los siguientes:

- La entidad cuenta con políticas y procedimientos formalmente establecidos sobre "conozca a su cliente" ya sea para clientes permanentes u ocasionales, acordes al tamaño y complejidad de sus operaciones. Estas políticas al menos, contienen criterios de aceptación y de seguimiento proactivo de cuentas que permiten tener un adecuado conocimiento de los clientes y de las actividades que desarrollan.

- Las políticas y procedimientos fueron aprobados por el Directorio, el que a su vez, mantiene una vigilancia permanente sobre su cumplimiento y recibe información periódica sobre las revisiones que se efectúen para verificar su adherencia. A su vez, dicho marco de alineamiento se hace extensivo a las sociedades filiales y de apoyo al giro que corresponda.

- La entidad cuenta con procedimientos establecidos para conducir las relaciones con la banca corresponsal.

- La entidad cuenta con un manual de procedimientos formalizado para reconocer transacciones potencialmente sospechosas, el que es accesible a todo el personal involucrado y es permanentemente actualizado.

- La entidad cuenta con un oficial de cumplimiento con la jerarquía e independencia necesarias para desarrollar su función y con los recursos humanos y tecnológicos adecuados.

- Dependiendo del tamaño de la organización, se ha instaurado un comité de alto nivel encargado de revisar políticas y procedimientos, evaluar su cumplimiento y decidir sobre casos que requieren atención especial.

- Existe un proceso de capacitación formal y periódico con el objeto de difundir las políticas y procedimientos a todo el personal de la entidad. El proceso de capacitación es diferenciado de acuerdo a la función que desempeña cada cual.

- Se cuenta con normas de selección de personal y de conducta con clientes, con el objeto de prevenir la ocurrencia de operaciones de lavado de activos y financiamiento del terrorismo. Además se ha desarrollado un código de conducta del personal que contempla principios respecto de las relaciones que se deben mantener con los clientes del banco.

- La entidad ha desarrollado sistemas de detección de operaciones inusuales, los que son acordes al tamaño y complejidad de sus actividades. Además existen canales formales de información a instancias superiores, los que permiten que estas operaciones sean conocidas a tiempo por la instancia pertinente y puedan ser reportadas a la autoridad competente.

- La función de auditoría realiza actividades periódicas e independientes de aquellas desarrolladas por el oficial de cumplimiento, con el objeto de verificar la adherencia a las políticas y procedimientos del banco para la detección y seguimiento de esas operaciones ilícitas. Su rol también comprende el análisis de las políticas y procedimientos, los sistemas de control, los planes de capacitación del personal, entre otros.

F) Administración de la estrategia de negocios y gestión del capital.

La evaluación comprende el proceso global de diseño, formulación y seguimiento de la estrategia de negocios como también la elaboración y control de los planes desarrollados por el banco.

Será objeto de calificación la forma en que el banco administra el proceso de formulación de su estrategia de negocios, en lo que se refiere al manejo de los fundamentos e información que le otorgan un grado razonable de viabilidad como, asimismo, la manera en que las condiciones generales del entorno y de la entidad, particularmente en lo relativo a necesidades de capital, han sido incorporadas en su definición.

Debe tenerse presente, tal como se señaló en el numeral 4.1 del título I, que existe una estrecha relación entre los niveles de capital mantenidos por el banco y la estrategia de negocios. En rigor, el mero cumplimiento de los requisitos mínimos de capital establecidos en la ley constituye un acatamiento a las disposiciones normativas, pero no refleja necesariamente una gestión razonada de los requerimientos de capital idóneos a la estrategia de negocios de la entidad.

En este sentido, se examinará si el proceso de planificación tiene en cuenta el análisis de los requerimientos de capital actuales y futuros del banco con relación a sus objetivos estratégicos, así como respecto de la implementación de los procesos de gestión de riesgo y de sus controles internos, como base de una evaluación eficaz de la suficiencia de capital mantenido por la entidad.

Una buena gestión en relación con lo descrito puede manifestarse en lo siguiente:

- El Directorio comprende la naturaleza y el nivel del riesgo asumido por el banco y la forma en que este riesgo se corresponde con niveles de capital suficientes y con sus planes de negocios. En este sentido, el Directorio contempla la planificación del capital como un elemento fundamental para la definición, implementación y logro de los objetivos estratégicos.

- El análisis de los requerimientos de capital y los riesgos, son parte integral del proceso de formulación de la estrategia de negocios. En efecto, dicha estrategia recoge con claridad las necesidades de capital del banco y sus fundamentos, los aportes de capital previstos, el nivel y composición de capital deseable y las fuentes externas de capital, como también el nivel y perfil de riesgo proyectado para las distintas líneas de negocios.

- El banco realiza análisis permanentes del entorno económico y de sus condiciones internas, así como de su posición comparativa en el mercado, que le permiten mantener una estrategia bien fundada y sostenible.

- La estrategia de negocios ha sido integralmente plasmada en los planes y presupuestos operacionales, y adecuadamente transmitida a los niveles pertinentes. El Directorio manifiesta su plena concordancia respecto a la orientación, ejecución y a su concreción.

- La entidad cuenta con sistemas de información que permiten una supervisión efectiva sobre el cumplimiento de los planes de negocios, la naturaleza y cuantía de los riesgos, como también respecto de la adecuación de capital económico y regulatorio.

- La estrategia de negocios está sujeta a revisiones periódicas, bajo procedimientos que permiten acciones correctivas oportunas o redefiniciones de los objetivos o planes de acción. Esto contempla una evaluación rigurosa de los requerimientos de capital y la realización de pruebas de tensión que incorporan posibles acontecimientos o cambios en las condiciones de mercado que pudieran afectar negativamente al banco.

- El banco ha establecido metas, plazos y responsables del cumplimiento de los planes de negocios y se han asignado los recursos necesarios para ello.

G) Gestión de la calidad de atención a los usuarios y transparencia de información.

La buena calidad en la atención de los clientes así como la calidad de la información que les es divulgada, constituyen aspectos importantes de la imagen que los bancos proyectan y, por cierto, son concordantes con una adecuada gestión de la entidad.

La evaluación de esta materia contempla la existencia de políticas y procedimientos que consideren la adecuada atención de sus clientes, la administración de controversias y la entrega de información al público con los cobros que afectan a los productos y servicios ofrecidos por el banco.

Es también parte de este examen, comprobar si la función de auditoría es suficientemente independiente para permitir una adecuada cobertura y profundidad de las revisiones que se efectúen sobre la materia y la adopción oportuna de medidas correctivas por parte de las áreas auditadas.

A modo de ejemplo, revelan una buena gestión sobre la materia, los siguientes aspectos:

- Políticas y procedimientos formalmente establecidos de transparencia de la información referida a los atributos de los productos y sus tarifas, de modo que cumplan las condiciones necesarias para una adecuada toma de decisiones por parte de los clientes. Lo anterior comprende la información entregada tanto al inicio de la relación comercial con el cliente, como durante todo el período que dure la relación contractual con este.

- Políticas y procedimientos formalmente establecidos, que consideren aspectos tales como la gestión de los reclamos, la existencia de canales formales de recepción de reclamos, la atención de consultas y solicitudes del público, la existencia de código de buenas prácticas comerciales, la capacitación al personal, la entrega de normas y procedimientos para la administración de los fraudes y de otros hechos delictuosos.

- La existencia y funcionamiento de unidades especializadas que cuenten con las herramientas y los recursos humanos y tecnológicos adecuados al tamaño del banco para administrar eficientemente las consultas y los reclamos del público.

- La existencia de informes de gestión que permitan identificar los tipos de reclamos, consultas y solicitudes, los productos involucrados en las presentaciones, los canales de recepción y el cumplimiento de estándares de respuesta, los que periódicamente deben ser dados a conocer al Directorio o a quién haga sus veces.

- La participación del Directorio en la aprobación de políticas y procedimientos; y de alguna de las instancias de la alta administración, en la definición de estándares de calidad, resolución de controversias y promoción de acciones correctivas.

- La adecuada divulgación, cuando corresponda, de las políticas, procedimientos y estándares de calidad hacia las filiales y sociedades de apoyo del banco, y su posterior control.

- La presencia de la función de auditoría interna en la revisión del proceso de atención de clientes y administración de reclamos.

H) Gestión de la función de auditoría interna y rol del comité de auditoría.

La existencia de una sólida función de auditoría interna se caracteriza por entregar una opinión independiente respecto de la calidad de los sistemas de control interno y del cumplimiento de las políticas y procedimientos, de manera de identificar, medir y controlar razonablemente los riesgos presentes y potenciales que pueden existir.

A continuación se describen algunos elementos que constituyen una buena gestión en relación al rol de la auditoría interna:

- La función de auditoría, previamente definida por el Directorio, presenta independencia de las áreas que desarrollan la negociación, operación y control de los negocios, y cuenta con adecuados recursos humanos y tecnológicos para el logro de sus objetivos, en concordancia con el tamaño y complejidad de las operaciones del banco.

- Todos los procesos y áreas de mayor riesgo en el banco son examinados por la auditoría interna, al menos en forma anual.

- La función de auditoría posee un enfoque de carácter proactivo e integral, es decir, se incorporan en sus revisiones aspectos operativos, de riesgos y de gestión, entregando una opinión global de la unidad, producto o materia auditada.

- Los informes de auditoría se distribuyen adecuadamente, de manera que el Directorio tiene conocimiento oportuno del alcance y los resultados de los mismos. Los informes deben identificar claramente las causas y efectos de los problemas, de manera que se pueda dimensionar el nivel de exposición al riesgo, presente en las distintas unidades auditadas.

- La función de auditoría cuenta con un sistema de seguimiento formal que permite controlar el cumplimiento de los compromisos adquiridos por las distintas áreas auditadas. Los informes de seguimiento son distribuidos a las mismas instancias a las que se informaron las observaciones.

- Las observaciones emanadas de los informes de auditoría se traducen en acciones concretas por parte de la línea, que pueden ser evaluadas y que permitan corregir las debilidades.

- El área que ejerce las funciones de auditoría interna cuenta con programas de trabajo de las distintas materias que audita, los que deben tener un enfoque de riesgos.

- El Comité de Auditoría, cumple apropiadamente con aquellas funciones de carácter permanente y no permanente establecidas en el Capítulo 1-15 de esta Recopilación.

4. Metodología y resultado de evaluación.

La clasificación según gestión será fundamentada por este Organismo en la notificación mencionada en el numeral 3.2 del título I de este Capítulo. En dicha comunicación se darán a conocer los resultados de la evaluación, indicándose las debilidades que hayan sido determinantes en caso de calificarse en el nivel B o C. Esto no es óbice, claro está, para informar también acerca de aquellas deficiencias observadas que no hayan sido gravitantes para la clasificación, cualquiera sea el nivel de gestión en que el banco quede clasificado.

Los numerales precedentes contienen sólo una breve descripción del alcance de la evaluación, a fin de dar una idea acerca de la índole de los problemas o situaciones que pueden eventualmente repercutir en la clasificación final. La forma de agrupación de las materias en esos numerales, no constituye un elemento asociado a posibles ponderaciones de debilidades que pudieren observarse, y las circunstancias que en cada numeral se mencionan a modo de ejemplo de una buena gestión, no constituyen por si solo requisitos que deban cumplirse para una clasificación en el más alto nivel de gestión, sino que sólo tienen un carácter ilustrativo de la orientación implícita de la evaluación.

Sin perjuicio de lo anterior y para efectos de otorgar una calificación a las materias referidas con el seguimiento oportuno de los riesgos señaladas en el numeral 3.2 precedente, la Superintendencia utilizará la siguiente escala en la evaluación de las materias revisadas:

1 CUMPLIMIENTO: La entidad cumple integralmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. No existen deficiencias apreciables.

2 CUMPLIMIENTO MATERIAL: La entidad cumple en forma significativa con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Aun cuando se identifican algunas debilidades en procesos específicos de alguna función, ellas se pueden considerar acotadas, sin perjuicio de lo cual su corrección debe ser atendida por la entidad a objeto de alcanzar los más altos estándares de gestión de riesgos.

3 CUMPLIMIENTO INSATISFACTORIO: La entidad no cumple en forma razonable con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. Se identifican debilidades en los procesos que componen diversas funciones, entre las que se encuentran algunas relevantes. La corrección de estas debilidades debe ser efectuada con la mayor prontitud.

4 INCUMPLIMIENTO: La entidad incumple materialmente con las mejores prácticas y aplicación de sanos principios que caracterizan una adecuada gestión. La solución de sus debilidades se considera indispensable.

Como se comprenderá, las diversas circunstancias que podrían incidir en una clasificación desfavorable de las materias auditadas no son susceptibles de traducirse en situaciones hipotéticas que caractericen el tipo y gravedad de deficiencias probables.

Desde la perspectiva de la gestión global de un banco, las debilidades que pudiere presentar en las materias que se han mencionado pueden reflejar indirectamente debilidades en la cultura de riesgo de la institución evaluada. Aun cuando este último aspecto no se califica ni forma parte del fundamento de la clasificación, deberá ser tenido en cuenta por los propios bancos evaluados, como el elemento que determina, en definitiva, la calidad de su gestión.

Conviene tener en cuenta que aquellas materias relacionadas con la capacidad para enfrentar escenarios de contingencia y la relacionada con el control interno, si bien no son sujeto de calificación individual, dependiendo de la magnitud de las debilidades podrán afectar la clasificación final de la gestión del banco.

5. Evaluación de la gestión por la propia empresa.

Sin perjuicio de las revisiones que, de acuerdo a lo establecido en este Capítulo, realice esta Superintendencia, la administración del propio banco deberá analizar y pronunciarse, a lo menos una vez al año, acerca del desarrollo de su gestión.

El Directorio deberá conocer y pronunciarse sobre cada una de las materias señaladas en el numeral 3.2 de este título, lo que no excluye que considere e incluya igualmente otros aspectos relacionados con la gestión de la empresa.

En el caso de las sucursales de bancos extranjeros, cuya gestión dependa de directivas de su Casa Matriz, el Gerente General o la autoridad máxima de la oficina en Chile, remitirá el resultado de la mencionada evaluación así como las eventuales medidas que proponga, a los auditores internos del banco y a la autoridad jerárquica que corresponda. Los acuerdos que al respecto adopten las mencionadas autoridades serán comunicados a la sucursal en Chile, la que deberá darlos a conocer a esta Superintendencia.

Los bancos enviarán a este Organismo una copia del informe presentado al Directorio, junto con la copia del acta de la reunión en que éste tomó conocimiento y resolvió acerca de la gestión de la empresa, antes del 30 de septiembre de cada año. Para ese efecto, el informe se anexará, también en formato PDF "desprotegido", al acta que debe enviarse a través de la Extranet de esta Superintendencia según lo indicado en el Capítulo 1-4 de esta Recopilación. Al tratarse de una reunión celebrada en el mes de septiembre, el plazo antes indicado podrá extenderse al establecido para el envío del acta respectiva.

Las sucursales de bancos extranjeros entregarán a esta Superintendencia, antes del 30 de septiembre de cada año, la copia de la comunicación y de los antecedentes que sobre la materia haya informado el encargado de la sucursal en Chile, según lo indicado anteriormente y las resoluciones que al respecto haya acordado la Casa Matriz.

ANEXO N° 1

DEFINICIONES DE CATEGORIAS

(Artículo 60 Ley General de Bancos)

Clasificaciones vigentes		CATEGORIAS según el nivel de gestión anterior:		
Nivel de gestión	Nivel de solvencia	Nivel A (o sin clasificación)	Nivel B	Nivel C
A	**A**	**I**	**I**	**I**
A	**B**	**II**	**II**	**II**
B	**A**	**II**	**II**	**II**
B	**B**	**II**	**III**	**III**
C	**A**	**III**	**III**	**IV**
C	**B**	**III**	**III**	**IV**
Cualquiera	**C**	**V**	**V**	**V**

———————

ANEXO Nº 2

POLITICA DE ADMINISTRACION DE RIESGOS DE MERCADO

La política de administración de riesgos de mercado debe cubrir, a lo menos, lo siguiente:

- Identificación de las fuentes de riesgo de mercado que enfrenta el banco y sus filiales:
  - Relativos a la actividad de negociación.
  - Relativos a la actividad bancaria tradicional.

- Estrategias de la entidad frente a tales riesgos:
  - Estrategias de inversión en instrumentos financieros.
  - Estrategias en derivados.
  - Manejo de posición en moneda extranjera.
  - Gestión de activos y pasivos bancarios.
  - Estrategias de cobertura.

- Medición del riesgo de mercado:
  - Descripción y alcance de modelos utilizados:
    - Modelos para cuantificación del riesgo de tasa de interés del libro de negociación.
    - Modelos para cuantificación del riesgo de tasa de interés del libro de banca.
    - Modelos para cuantificación del riesgo de moneda.
    - Modelos para determinar riesgos de mercado en opciones.
  - Metodologías y criterios para la realización de pruebas retrospectivas.
  - Metodologías y criterios para la realización de pruebas de tensión.
  - Esquema operativo asociado a cada modelo.
  - Actividades destinadas a revaluar criterios, parámetros y supuestos incluidos en los modelos.

- Estructura de límites internos.
  - Fundamentos de la estructura de límites.
  - Periodicidad del control de límites.
  - Tratamiento de excepciones a los límites.
  - Actividades destinadas a verificar la consistencia de los límites.

- Esquema de reporte de los riesgos de mercado.
  - Tipos de informes.
  - Periodicidad.
  - Destinatarios.

- Responsabilidades respecto de las siguientes funciones:
  - Autorización de políticas.
  - Aplicación de políticas.
  - Revisión de suficiencia de la estructura de límites internos.
  - Monitoreo del estado de los límites.
  - Tratamiento de excepciones a las políticas definidas.
  - Generación y mantención de las herramientas utilizadas en la medición de los riesgos.
  - Cálculo de parámetros, definición de supuestos y escenarios.
  - Ejecución de las pruebas de tensión.
  - Realización de las pruebas retrospectivas.
  - Emisión de reportes a la alta administración.
  - Análisis del riesgo de mercado asociado al lanzamiento de nuevos productos.

- Rol de la función de auditoría interna.

_____

ANEXO Nº 3

GESTIÓN DE LA *CIBERSEGURIDAD*

Para efectos de lo dispuesto a continuación, se entiende que la *Ciberseguridad* es un concepto que comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, sobre la seguridad de la información y la continuidad del negocio de la institución.

I. GESTIÓN DE LA INFRAESTRUCTURA CRÍTICA DE *CIBERSEGURIDAD*

Una adecuada gestión de la infraestructura crítica en materias de *Ciberseguridad* requiere de un marco de gestión establecido por el Directorio, que contemple la estrategia de administración específica de este riesgo, el nivel de tolerancia, los roles y responsabilidades de los participantes, las metodologías a utilizar para su gestión en consideración a las mejores prácticas y al volumen y complejidad de sus actividad de negocio.

La gestión de la infraestructura crítica de *Ciberseguridad* es fundamental para el adecuado funcionamiento del sistema financiero, en el caso de eventuales ataques. Con este fin, se evaluará que las instituciones gestionen esta infraestructura considerando al menos los siguientes elementos:

a) La institución ha identificado la infraestructura crítica en términos de *Ciberseguridad*, esto es, aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio. Asimismo, identifica la infraestructura física, *hardware* y sistemas tecnológicos que almacenan, administran y soportan estos activos y que de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información.

b) La institución cuenta con una hoja de ruta que considere un listado de funciones básicas, metodologías y mejores prácticas como resultado de la definición de criticidad de su infraestructura.

c) La institución ha desarrollado e implementado los resguardos necesarios para proteger la infraestructura definida como crítica. La institución ha establecido las medidas de seguridad adecuadas para prever, detectar y gestionar oportunamente los eventos e incidencias que puedan afectar la *Ciberseguridad* de la infraestructura crítica.

d) La institución revisa regularmente sus políticas y procedimientos para prever la adopción oportuna de medidas ante escenarios de amenazas de *Ciberseguridad*.

e) La institución dispone de planes de recuperación de operaciones o procesos críticos, en forma oportuna y eficiente.

f) La institución promueve una cultura de riesgos en materia de *Ciberseguridad*, a través de procesos formales de difusión, capacitación y concientización de todos los empleados, entre otros.

II. BASE DE INCIDENTES DE *CIBERSEGURIDAD*

II.1 Condiciones mínimas para el desarrollo y mantención de una Base de Incidentes

La *Ciberseguridad* en las instituciones financieras es esencial para evitar los efectos adversos sobre su continuidad operacional, así como la seguridad de los activos que administran.

Al respecto, resulta relevante que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales relacionados con la *Ciberseguridad*.

A continuación se detallan algunos de los elementos que serán parte de la evaluación de gestión, respecto a la generación de la base de incidentes:

a) La entidad cuenta con una base de incidentes de *Ciberseguridad*, donde registra los eventos no planificados por la institución que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio e identificando de manera individual cada uno de estos incidentes.

b) La institución gestiona sus incidentes de *Ciberseguridad*, con el fin de detectar, investigar y generar acciones de mitigación del impacto de estos eventos, resguarda la confidencialidad, disponibilidad e integridad de sus activos de información.

c) El Directorio de la institución toma regularmente conocimiento de estos incidentes y se pronuncia sobre ellos al menos una vez al año, con el fin de mejorar su gestión y prevención.

d) La base de incidentes completa deberá mantenerse a disposición de esta Superintendencia para cuando sea requerida. La suficiencia de la base de incidentes es parte de las revisiones de la función de auditoría interna.

e) La institución realiza regularmente pruebas para detectar las amenazas y vulnerabilidades que pudieran existir en la infraestructura crítica de *Ciberseguridad*, tales como *pentesting* y/o *ethical hacking*.

II.2 Variables mínimas a considerar para la elaboración de la base de incidentes de *Ciberseguridad*

Identificación única del incidente.

Fecha del evento: fecha y hora del inicio del incidente.

Fecha del reporte: fecha y hora en la que el incidente es detectado.

Tipo de amenaza o vulnerabilidad: determinar la causa del incidente a partir del tipo de amenaza o vulnerabilidad que coloca en riesgos a los activos de información virtuales, de acuerdo a la clasificación presentada a continuación:

1. Falla producida en la estructura física que soporta el activo de información.
2. Falla en los accesos producto de una inadecuada definición, control o vulneración.
3. Acción de fuerzas de la naturaleza como incendios, terremotos, tormentas electromagnéticas, entre otros.
4. Terrorismo.
5. Fallas en los procesos, definición, control o vulneración.
6. Falla en los proveedores.
7. Inadecuada arquitectura tecnológica, definición, control o vulneración.
8. Prácticas inadecuadas de los usuarios internos de la organización.
9. Prácticas inadecuadas de los usuarios externos de la organización.
10. Falla en las redes de comunicaciones.

Fuente de la amenaza o vulnerabilidad: establecer si se trata de una causa externa o interna de la organización.

Descripción del incidente: breve descripción del incidente que permita entender las causas especificando el tipo de ataque (*ciberespionaje*, *phishing*, *malware*, denegación de servicio, entre otros) y especifique el tipo de amenaza o vulnerabilidad que lo produce.

Activos involucrados: especificación de los activos afectados, distinguiendo aquellos efectivamente vulnerados de los potencialmente en riesgo.

Tipo de productos o servicios involucrados: detallar cuando corresponda aquellos productos o servicios prestados por la institución que fueron afectados por el incidente, ya sea en su disponibilidad o funcionamiento.

Número de clientes afectados cuando corresponda.

Identificación de los proveedores (cuando corresponda).

Tiempo de resolución del incidente: medido en horas y minutos.

Costos de incidentes: costos asociados al incidente, entendidos como el valor de las pérdidas potenciales o reales.

Costos de mitigación y reparación: costos de eventuales medidas de mitigación y reparación asociados al incidente, sea que este se haya o no materializado.

Descripción de las acciones realizadas y áreas responsables de su implementación (cuando corresponda).

Estado del incidente: indicar para cada evento si los planes de acción para su corrección definitiva se encuentran implementados.