SUPERINTENDENCIA DE PENSIONES

Año del Fortalecimiento del Estado Social y Democrático de Derecho

RESOLUCIÓN 340-12 SOBRE SISTEMA INTEGRAL DE LA EVALUACIÓN DE LAS ADMINISTRADORAS DE FONDOS DE PENSIONES BASADO EN RIESGO OPERATIVO. SUSTITUYE LA RESOLUCIÓN 297-09

CONSIDERANDO: Que el literal c) del Artículo 108 de la Ley 87-01 que crea el Sistema Dominicano de Seguridad Social, faculta a la Superintendencia de Pensiones, en lo adelante Superintendencia a supervisar, controlar, monitorear y evaluar las operaciones financieras de las Administradoras de Fondos de Pensiones, en lo adelante las Administradoras y verificar la existencia de los sistemas de contabilidad independientes;

CONSIDERANDO: Que el Artículo 128 del Reglamento de Pensiones le atribuye a la Superintendencia llevar a cabo labores permanentes de vigilancia sobre los procesos operativos y financieros a las entidades supervisadas;

CONSIDERANDO: Que es interés de la Superintendencia que las Administradoras, la Tesorería de la Seguridad Social, en lo adelante TSS, y la Empresa Procesadora de la Base de Datos, en lo adelante EPBD, implementen los lineamientos necesarios para el funcionamiento adecuado de la administración de riesgos;

VISTA: La Ley 87-01 que crea el Sistema Dominicano de Seguridad Social, promulgada el 9 de mayo del 2001 y sus modificaciones;

VISTO: El Reglamento de Pensiones aprobado mediante el Decreto 969-02 del Poder Ejecutivo de fecha diecinueve (19) de diciembre de 2002;

VISTOS: Los artículos 117, 118 y 119 del Reglamento de Pensiones;

VISTA: La Resolución 27-03 de fecha 11 de enero de 2003 y sus modificaciones, que establece el Manual de Cuentas para las AFP;

VISTA: La Resolución 240-05, de fecha 6 de junio de 2005, sobre mecanismos de control interno a ser implementados por las Administradoras de Fondos de Pensiones (AFP);

VISTA: La Resolución 297-09, de fecha 11 de diciembre de 2009, sobre Sistema Integral de la Evaluación de las Administradoras de Fondos de Pensiones, basado en Riesgo Operativo;

VISTA: La Resolución 307-10, de fecha 01 de septiembre de 2010, sobre Registros de Auditores Externos;

SUPERINTENDENCIA DE PENSIONES

Año del Fortalecimiento del Estado Social y Democrático de Derecho

La Superintendencia de Pensiones en virtud de las atribuciones que le confiere la Ley

RESUELVE:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto
Establecer los lineamientos generales y las normas mínimas que deben ser aplicadas por las Administradoras de Fondos de Pensiones, en lo adelante las Administradoras, Tesorería de la Seguridad Social y la Empresa Procesadora de Base de Datos para la identificación, medición, administración, mitigación y divulgación del riesgo operativo a que están expuestas, así como contar con una estructura organizacional que facilite el cumplimiento de estas tareas.

Artículo 2. Ámbito de aplicación
La presente resolución es aplicable a las entidades que se identifican a continuación:

a) Administradoras de Fondos de Pensiones
b) Empresa Procesadora de Base de Datos (EPBD)
c) Tesorería de la Seguridad Social (TSS)
d) Aquellas entidades que administren fondos de pensiones, abiertos o cerrados, sean estatales o privados, en virtud de leyes especiales, a través de Cuentas de Capitalización Individual, Sistema de Reparto y fondos complementarios.

Artículo 3. Definiciones
Para la aplicación de la presente resolución, los términos indicados a continuación tendrán los significados siguientes:

Administración de riesgos: Es el procedimiento mediante el cual las entidades identifican, miden, evalúan, monitorean y controlan los riesgos inherentes al negocio, con el objeto de conocer el grado de exposición a que están expuestas en el desarrollo de sus operaciones y definir los mecanismos de mitigación y control para proteger los recursos propios y de terceros que se encuentran bajo su control y administración.

Alta gerencia: La integran el presidente y los vicepresidentes, gerentes generales o cargos afines, responsables de ejecutar las disposiciones del Consejo de Administración u órgano equivalente, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada entidad.

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas): Es un marco de gobierno de Tecnología de la Información (TI) que permite el desarrollo de políticas y buenas prácticas para el control de TI en todas las partes de la organización.
Evento: Acontecimiento de un incidente interno o externo en un lugar particular y en un intervalo de tiempo determinado.

Evento de pérdida: Evento que genera pérdida a causa de un riesgo operativo.

Factores de riesgo: Son las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo a nivel de la actividad o líneas de negocios.

ITIL (Infraestructura de Bibliotecas para Tecnología de Información): Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de alta calidad de tecnología de la información.

ISO (Organización Internacional para la Estandarización):
Organización internacional para la estandarización de normas relativas a productos y seguridad para las empresas u organizaciones a nivel internacional.

Otras entidades supervisadas por la Superintendencia: Aquellas entidades que administren fondos de pensiones, abiertos o cerrados, sean estatales o privados, en virtud de leyes especiales, a través de Cuentas de Capitalización Individual, Sistema de Reparto y fondos complementarios. Dentro de estas entidades se incluyen la Tesorería de la Seguridad Social y la Empresa Procesadora de Base de Datos.

Perfil de riesgo: Es el grado de riesgo que tiene una entidad en un período de tiempo de acuerdo con la frecuencia y severidad de los riesgos identificados.

Pérdida: Cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

Pista de auditoría: Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.

Plan de contingencia: Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado.

Plan de continuidad: Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación.

Procedimiento: Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de los cuales se asegura el cumplimiento de una función operativa.

Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

Proceso crítico: Proceso indispensable para la continuidad del negocio y las operaciones de la entidad, y cuya falta de identificación o aplicación deficiente puede generar un impacto financiero negativo.

Riesgo: Es la posibilidad que se produzca un hecho que genere pérdidas que afecte los resultados y/o el patrimonio y la solvencia de las entidades identificadas en el Artículo 2.

Riesgo inherente: Es el riesgo que por su naturaleza no se puede separar de la situación donde existe. Es el riesgo propio de cada actividad, sin tener en cuenta el efecto de las medidas adoptadas para su mitigación y control.

Riesgo legal: Es la posibilidad que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una de las entidades identificadas en el Artículo 2. Estas pueden ser derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones, así como por el incumplimiento no intencional de las leyes y/o normas aplicables.

Riesgo operativo: Es la posibilidad de sufrir pérdidas debido al incumplimiento de políticas y procedimientos necesarios en la operación del negocio, a la falta de adecuación o a fallos de los procesos y controles internos, personas o sistemas internos, o bien a causa de acontecimientos externos.

Seguridad de la información: Son los mecanismos establecidos para garantizar la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

Sistema de administración de riesgos: Es el sistema orientado a identificar, medir, evaluar, monitorear y mitigar los riesgos de la entidad.

Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que este desarrolle o ejecute un proceso que podría ser realizado por la empresa contratante.

TI (Tecnología de Información): Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software (aplicaciones, sistemas operativos, sistemas de administración de bases de datos, etc.), redes, multimedia, servicios asociados, entre otros.

CAPÍTULO II

LINEAMIENTOS PARA ESTABLECIMIENTO DE POLÍTICAS Y PROCEDIMIENTOS

Artículo 4. Las Administradoras y las otras entidades supervisadas por la Superintendencia, diseñarán un proceso de evaluación y administración del riesgo que le permita identificar, medir, controlar/mitigar y monitorear sus exposiciones al riesgo operativo en el desarrollo de sus negocios y operaciones, considerando para su implementación todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control.

Artículo 5. Las Administradoras y las otras entidades supervisadas por la Superintendencia, antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, deben asegurarse que el riesgo operativo inherente a los mismos esté sujeto a procedimientos adecuados de evaluación y control.

Artículo 6. Las Administradoras y las otras entidades supervisadas por la Superintendencia deben identificar los eventos de riesgo operativo agrupados por tipo y fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

Artículo 7. Identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la entidad, el Consejo de Administración u órgano equivalente, y la Alta Gerencia deben decidir si el riesgo se debe asumir, compartir, evitar o transferir, reduciendo sus consecuencias y efectos, para lo cual debe:

a) Revisar estrategias y políticas;
b) Actualizar o modificar procesos y procedimientos establecidos;
c) Implantar o modificar límites de riesgo;
d) Constituir, incrementar o modificar controles;
e) Implantar planes de contingencias y de continuidad del negocio;
f) Revisar términos de pólizas de seguro contratadas; y,
g) Contratar servicios provistos por terceros; u otros, según corresponda.

Artículo 8. Las Administradoras y las otras entidades supervisadas por la Superintendencia deben contar con la tecnología de información (TI) que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, segura y confiable; mitigar las interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Artículo 9. El proceso de evaluación de riesgo debe conducir a una buena selección de tecnología y control de su implementación, e incorporar las evaluaciones específicas para las responsabilidades funcionales, tales como: seguridad, continuidad de negocio, gestión de

suplidores, entre otras. Asimismo, deben evaluar las deficiencias de hardware, software, sistemas, aplicaciones y redes, errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas, vulnerabilidad en las redes, controles instalados, seguridad ante ataques intencionales o incidentes de irrupción y acciones fraudulentas, así como defectos en la recuperación de información.

Artículo 10. Las Administradoras y las otras entidades supervisadas por la Superintendencia deben asignar responsables que se encarguen de definir y autorizar de manera formal los accesos, cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos. Asimismo, las Administradoras y las otras entidades supervisadas deben definir políticas, procesos y procedimientos de tecnología de información bajo el estándar COBIT como gobierno de TI y puede ser combinado con otros estándares generalmente aceptados, que garanticen la ejecución de los criterios de control interno relativos a eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la entidad.

Artículo 11. Las Administradoras y las otras entidades supervisadas por la Superintendencia deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.

CAPÍTULO III

FACTORES Y EVENTOS DE RIESGO OPERATIVO

Artículo 12. Factores que originan el riesgo operativo

a) Procesos internos

Las Administradoras y las otras entidades supervisadas por la Superintendencia deben observar los criterios indicados a continuación para un control efectivo de los riesgos asociados a los procesos internos.

i) Gestionar los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de conformidad con la presente norma, en lo relativo al diseño inapropiado de los procesos críticos o las políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

ii) Contar con políticas documentadas y formalizadas relativas al diseño, control, actualización y seguimiento de los procesos.

iii) Definir y delimitar las funciones que eviten tareas cuya combinación de competencias en una sola persona pudiese permitir la realización y/o ocultamiento de fraudes, errores, omisiones u otros eventos de riegos.
iv) Identificar sus procesos y subprocesos críticos.

v) Elaborar y mantener permanentemente actualizados los mapas de procesos de la entidad.

b) Personas
Para asegurar una adecuada planificación y administración del personal, las Administradoras y las otras entidades supervisadas por la Superintendencia deben:

i) Establecer políticas, procesos y procedimientos para gestionar los riesgos asociados al personal de la entidad, en lo relativo a la capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de activos.

ii) Evaluar y definir las necesidades de recursos humanos con las competencias idóneas para el desempeño de sus funciones tomando en cuenta la experiencia profesional, formación académica, sus valores, actitudes y habilidades personales.

iii) Mantener información actualizada del personal de la entidad relativa, a la formación académica, desempeño laboral, capacitación, procedimiento de contratación y motivo de desvinculación.

c) Tecnología de información
Las Administradoras y las otras entidades supervisadas por la Superintendencia deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como problemas de calidad de información, y la inadecuada inversión en tecnología.

d) Eventos externos
Las Administradoras y las otras entidades supervisadas por la Superintendencia deben gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados a fallas en los servicios públicos, fallas en los servicios provistos por terceros, la ocurrencia de desastres naturales, contingencias legales, atentados y actos delictivos, entre otros factores.

Artículo 13. Eventos de riesgo operativo
Los eventos de pérdida por riesgo operativo deben ser agrupados de la manera descrita a continuación:

a) Fraude interno. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales

en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

b) **Fraude externo**. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c) **Prácticas laborales y seguridad en el puesto de trabajo**. Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d) **Clientes, productos y prácticas empresariales**. Pérdidas derivadas del incumplimiento, ya sea de carácter involuntario o negligente, de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o pérdidas derivadas de la naturaleza o diseño de un producto.

e) **Daños a los activos físicos.** Pérdidas derivadas de daños o perjuicios a los activos materiales de la entidad, como consecuencia de desastres naturales u otros acontecimientos.

f) **Pérdidas derivadas de interrupción del negocio y fallos en los sistemas.**

g) **Ejecución, entrega y gestión de procesos.** Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

CAPÍTULO IV

ROLES Y RESPONSABILIDADES

DEL CONSEJO DE ADMINISTRACIÓN U ÓRGANOS EQUIVALENTES

Artículo 14. El Consejo de Administración u órgano equivalente de las Administradoras y de las otras entidades supervisadas por la Superintendencia, respectivamente, tendrá las responsabilidades siguientes:

a) Definir la política general de la gestión de riesgo operativo de la entidad.

b) Integrar en sus decisiones la información proveniente del Sistema de administración del Riesgo Operativo de la entidad, revisarla al menos semestralmente e informar al respecto en su informe anual a la Asamblea de Accionistas.

c) Aprobar el Manual de Políticas y Procedimientos para la administración del riesgo operativo, el cual debe contener las políticas para el análisis y control del riesgo, así como los niveles de tolerancia, exposición al riesgo y medidas de mitigación. Una vez que dicho manual sea aprobado por el Consejo de Administración, las Administradoras y las otras entidades supervisadas por la Superintendencia deben remitirlo a la Superintendencia en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura, junto al acta de aprobación por parte del Consejo, en original y debidamente sellada y registrada.

d) Designar a uno de sus miembros como Presidente del Comité de Riesgo Operativo y autorizar los demás miembros del mismo. De igual manera, contratar a un experto independiente en materia de evaluación de riesgo operativo, quien será parte integrante de dicho comité y asesor de la Unidad de Riesgo Operativo.

e) Aprobar el conjunto de normas y directrices necesarias para la administración de los riesgos operativos asociados a los procesos ejecutados por las entidades correspondientes. Del mismo modo, debe aprobar la metodología que establezca los mecanismos para medir y controlar los riesgos operativos en la entidad y generar indicadores por cada tipo de riesgo previa opinión del experto independiente y del Comité de Riesgo Operativo.

f) Asignar los recursos necesarios a fin de contar con la infraestructura, metodología y personal apropiados para la gestión adecuada del riesgo operativo;

Párrafo I: Toda modificación que se efectúe al manual de políticas y procedimientos para el control del riesgo operativo de las Administradoras, otras entidades supervisadas por la Superintendencia, debe ser remitido y aprobado por el Consejo de Administración de cada entidad. Asimismo, debe remitir a la Superintendencia de Pensiones una copia de las modificaciones realizadas en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura.

DE LA GERENCIA

Artículo 15. Responsabilidades de la Gerencia

La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operativo conforme a las disposiciones del Consejo de Administración u órgano equivalente de las Administradoras, u otras entidades supervisadas por la Superintendencia.

Cada unidad técnica o de apoyo tiene la responsabilidad de gestionar el riesgo operativo en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

DEL COMITÉ DE RIESGO OPERATIVO

Artículo 16. El Comité de Riesgo Operativo de las Administradoras, u otras entidades supervisadas por la Superintendencia, la TSS y la EPBD es el órgano con funciones y propósitos específicos en la materia, que tiene como objeto la administración de los riesgos operativos a que se encuentra expuesta la entidad. Dicho Comité debe ser integrado, sin suplencia, por:

a) Un miembro del Consejo de Administración, designado para presidirlo;
b) Un experto independiente;
c) El Comisario de Cuentas;
d) El Director General de la Administradora o de otra entidad supervisada por la Superintendencia, el Director General de la Procesadora de la Base de Datos o el Tesorero de la Seguridad Social o Titular, según corresponda.
e) El auditor interno; y
f) El titular de la Unidad de Administración Riesgo Operativo.

Párrafo I: El Comité de Riesgo Operativo debe sesionar al menos bimestralmente. Todas las sesiones y acuerdos del Comité de Riesgo Operativo deben constar en actas debidamente firmadas por todos y cada uno de los integrantes presentes en la sesión correspondiente.

Párrafo II: Cuando sea necesario, los responsables de la ejecución de los procesos críticos en las entidades detalladas en el Artículo 2, deben ser convocados a las sesiones del Comité del Riesgo Operativo, en las cuales participarán con voz, pero sin voto.

Artículo 17. Las responsabilidades del Comité de Riesgo Operativo de las Administradoras, u otras entidades supervisadas por la Superintendencia, la TSS y la EPBD son:

a) Proponer para aprobación del Consejo de Administración u órgano equivalente de la entidad, los niveles de tolerancia al riesgo, y los criterios de responsabilidad de información, por tipo de riesgo, de acuerdo con lo establecido en la presente resolución;

b) Coordinar y participar en la elaboración y permanente actualización del Manual de Políticas y procedimientos para la administración del riesgo operativo y someterlo a la autorización del Consejo de Administración u órgano equivalente;

c) Establecer el mapa de procesos, incluyendo el detalle de subprocesos, actividades, tareas, funcionarios identificados por área y puesto, los elementos tecnológicos sobre los que se ejecutan y sus controles, codificando los mismos.

d) Determinar el mecanismo para medir los costos de cada fase del proceso, incluyendo los elementos humanos, materiales, tecnológicos que en él participan, así como los costos de las incidencias y pérdidas monetarias que resulten de la materialización de riesgos operativos.

e) En todos los casos en que la evaluación del riesgo se base en juicio experto, establecer al menos tres umbrales de probabilidad de ocurrencia y tres de grados de severidad o impacto, especificando las razones para definir las fronteras entre dichos umbrales.

f) Establecer la metodología para crear una base de datos de eventos de pérdidas operativas históricas que identifique el proceso, actividad, tarea y valor de la incidencia o pérdida generada por la materialización de un riesgo operativo, la causa que lo propició y la medida de mitigación adoptada. Esto debe registrarse por cada evento, y la información sólo podrá ser borrada de dicha base de datos con apego a la política definida por el Comité de Riesgo Operativo. Únicamente podrán escribir en la base de datos de eventos de pérdidas operativas, los agentes autorizados por la Unidad de Administración de Riesgo Operativo.

g) Aprobar y revisar, al menos una vez al año, la metodología, modelos, sistemas de medición, parámetros y escenarios, para identificar, medir, monitorear, controlar e informar los distintos tipos de riesgo operativo a que se encuentran expuestas las entidades.

h) Informar al Consejo de Administración u órgano equivalente los eventos de excesos sobre los niveles de tolerancia a los riesgos, así como el impacto financiero que enfrentaría la entidad derivado de la materialización de los mismos;

i) Informar al Consejo de Administración u órgano equivalente sobre las medidas correctivas implementadas, cuando el nivel observado de los riesgos operativos se acerque o exceda los niveles de tolerancia establecidos, así como cualquier otra medida representativa de mitigación que se tome en la materia;

j) Informar al Consejo de Administración u órgano equivalente el grado de cumplimiento de las políticas y procedimientos, así como el resultado de las evaluaciones del riesgo operativo;

k) Crear los subcomités que se consideren convenientes para el cumplimiento de las presentes disposiciones;

l) Establecer políticas de aplicación para el desarrollo de una cultura de administración y mitigación de riesgo operativo entre los empleados de las entidades.

DE LA UNIDAD DE ADMINISTRACIÓN DE RIESGO OPERATIVO

Artículo 18. Unidad de Administración de Riesgo Operativo
Las Administradoras y las otras entidades supervisadas por la Superintendencia, deben contar con una Unidad de Administración de Riesgo Operativo responsable del control y mitigación de los riesgos operativos a los que se encuentran expuestas. Esta Unidad debe estar integrada dentro del

organigrama de cada una de las entidades mencionadas, con una función especializada de segundo nivel.

Artículo 19. Responsabilidad de Unidad de Administración de Riesgo Operativo
La Unidad de Administración del Riesgo Operativo, será responsable de:

a) Identificar, evaluar, medir y monitorear los distintos tipos de riesgo operativo a los que se encuentran expuestas las Administradoras y las otras entidades supervisadas por la Superintendencia, así como el impacto financiero que enfrentarían en caso de la materialización de los mismos, de acuerdo con el mecanismo de costo establecido por el Comité de Riesgo Operativo. Asimismo, debe informar al Comité de Riesgo Operativo los resultados de las evaluaciones, así como las medidas preventivas y correctivas implementadas o que deban implementarse, cuando el nivel observado de los riesgos operativos se acerque o exceda los niveles de tolerancia establecidos.

b) Clasificar, por procesos y subprocesos, actividades y tareas, los factores de riesgo operativo, los eventos de pérdida por cada tipo de factor de riesgo operativo y el área en la que se origine el mismo, resaltando el impacto de su materialización para la entidad. Estos eventos serán notificados a la Unidad por parte de quien los detecte a través del formulario correspondiente definido por la entidad.

c) Documentar e informar al Comité de Riesgo Operativo, inmediatamente se produzca cualquier desviación de los niveles de tolerancia de riesgo operativo, previamente establecidos por el Consejo de Administración, así como las causas que originaron dicha desviación, e informar las acciones correctivas necesarias recomendadas por los responsables de los procesos, ante los casos de desviación que se susciten.

d) Proponer políticas para la gestión del riesgo operativo.

e) Participar en la elaboración y permanente actualización del Manual de Políticas y Procedimientos para la administración del riesgo operativo.

Párrafo I. La Unidad debe registrar y almacenar los eventos de pérdida por riesgo operativo y de sistemas informáticos materializados en una Base de Datos de Eventos de Pérdidas única y especializada para estos fines, preservando la integridad del evento en cuestión, de acuerdo con los criterios de clasificación establecidos por el Comité de Riesgo. Asimismo, debe mantener esta base de datos con información histórica, la cual debe tener el registro sistemático de los diferentes eventos de pérdida, determinando la frecuencia con que se repite cada evento y el efecto cualitativo y cuantitativo de la pérdida producida, de acuerdo con el área de origen y la clasificación definida por el Comité de Riesgo Operativo, así como cualquier otra información que se considere necesaria y oportuna para estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo. En el caso de los riesgos cualitativos deben ser cuantificados por el

juicio del experto en la materia, que para los procesos críticos, se refiere al ejecutivo interno dueño del proceso.

Párrafo II. Cada área sustantiva del negocio tendrá un agente de riesgo operativo quien registrará e informará oportunamente a la Unidad, en los medios que esta disponga, de cualquier evento de pérdida. La Unidad debe apoyar y asistir a dichas áreas para la aplicación de la metodología de gestión de riesgos operativos.

Párrafo III. La Unidad debe remitir de forma continua y oportuna los reportes de información de control de riesgo a las áreas correspondientes de las Administradoras y otras entidades supervisadas por la Superintendencia, de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en el control del riesgo operativo y establecer o modificar políticas, procesos y procedimientos correspondientes, en los casos que se amerite.

Párrafo IV. Debe presentar al Comité de Riesgo Operativo un informe semestral donde la Unidad refleje el cumplimiento de las responsabilidades antes mencionadas.

Las Administradoras y las otras entidades supervisadas por la Superintendencia, deben presentar a la Superintendencia en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura, dentro de los treinta (30) días calendario siguientes al corte de cada año, un informe de evaluación de los riesgos operativos a que está expuesta la entidad por proceso crítico y área operativa y de apoyo, que refleje su perfil de riesgo.

CAPÍTULO V

DE LA AUDITORÍA

Artículo 20. Auditoría Interna

Auditoría Interna debe:

a) Velar por el cumplimiento de las políticas y procedimientos utilizados para la gestión de riesgo operativo.

b) Revisar la veracidad de todos los eventos registrados como pérdidas operativas, así como las medidas correctivas y sus consecuencias.

Artículo 21. Auditoría Externa

El informe sobre el sistema de control interno de cada una de las entidades del Artículo 2, elaborado por los auditores externos, debe incluir comentarios indicando si la entidad cuenta con políticas y procedimientos implementados para la gestión del riesgo operativo.

Artículo 22. Empresas Calificadoras de Riesgo

Las empresas calificadoras de riesgo deben tener en cuenta las políticas y procedimientos establecidos por la entidad para la gestión del riesgo operativo en el proceso de calificación de las entidades supervisadas.

CAPÍTULO VI

DE LAS POLÍTICAS, MANUALES Y PROCEDIMIENTOS

Artículo 23. Manual de gestión de riesgo operativo

Las Administradoras y las otras entidades supervisadas por la Superintendencia, deben contar con un manual de gestión del riesgo operativo que contemple al menos los aspectos siguientes:

a) Políticas para la gestión del riesgo operativo.

b) Funciones y responsabilidades asociadas con la gestión del riesgo operativo de la Alta Gerencia, el Comité de Riesgo Operativo, la Unidad de Administración Riesgo Operativo y las unidades de negocio y de apoyo.

c) Descripción de la metodología aplicada para la gestión del riesgo operativo.

d) Forma y periodicidad con la que se debe informar al Consejo de Administración, a la Alta Gerencia, al Comité de Riesgo Operativo, entre otros, sobre la exposición al riesgo operativo de la empresa y de cada unidad de negocio.

e) Proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que debe contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Las Administradoras y las otras entidades supervisadas por la Superintendencia deben remitir a la Superintendencia de Pensiones, dentro de un plazo no mayor a doce (12) meses después de la publicación de la presente Resolución, la totalidad de las políticas, los manuales y procedimientos correspondientes a los procesos y subprocesos descritos en este artículo, así como los mapas de procesos de los mismos de acuerdo con lo descrito en el Articulo 17, literales c) y d). A partir de esta fecha, las actualizaciones a dicha documentación deben ser enviadas a la Superintendencia una vez que sean aprobadas e indicar los plazos de implementación establecidos.

Procesos y subprocesos:

a) Las Administradoras

1. Afiliación y Traspasos
   - Asesoramiento y Atención al Público
   - Impresión y Distribución de Formularios de Afiliación y Traspaso
   - Gestión de Suscripción de Solicitudes de Afiliación y Traspaso
   - Resguardo y/o Recuperación de formularios de Afiliación y Traspaso

2. Dispersión de la Recaudación y Administración de Cuentas Individuales
   - Apertura y Cierre de la CCI
   - Confirmación de la Individualización, Dispersión de la Recaudación y Administración de Cuentas Individuales
   - Emisión y Envío de los Estados de Cuenta
   - Resguardo y/o Recuperación de la información relacionada con los procesos de Individualización, Dispersión de la Recaudación y Administración de las Cuentas Individuales

3. Inversiones
   - Definición de la Política de Inversión
   - Realización de Operaciones Financieras
   - Liquidación de Operaciones Financieras
   - Contabilización de Operaciones Financieras y Emisión del Informe Diario

4. Beneficios
   - Asesoramiento e Información al Beneficiario
   - Procedimientos y Plazos de Tramitación de las solicitudes de beneficios
   - Determinación de Derechos
   - Pago de Prestaciones

5. Sistemas y Tecnología
   - Gestión de la Continuidad Operativa
   - Gestión de la Seguridad de la Información
   - Aseguramiento de la Calidad
   - Desarrollo, implementación y mantenimiento de Sistemas
   - Gestión de los procesos operativos de tecnología
   - Resguardo y recuperación de la información

6. Selección y Capacitación de Personal
    - Capacidad Técnica
    - Experiencia
    - Conducta social

7. Designación de Atribuciones sobre el Negocio
    - Facultades Delegadas por el Consejo y Criterios
    - Facultades Delegadas por el Director General y Criterios
    - Facultades Delegadas por Otros Órganos y Criterios

8. Responsabilidades Compartidas
    - Responsabilidades mancomunadas para idénticos niveles de responsabilidad
    - Responsabilidades mancomunadas por jerarquía
    - Responsabilidades mancomunadas entre el Consejo y la Administración

9. Escalamiento de Información y Decisión
    - Aplicables a Adquisiciones de Activos
    - Aplicables a Ventas de Activos
    - Aplicables a Contratación de Fianzas, Seguros y Financiamiento
    - Decisiones Criticas del Negocio

- a) La DGJP

10. Traspasos
    - Asesoramiento y Atención al Público
    - Impresión y Distribución de Formularios de Afiliación y Traspaso
    - Gestión de Suscripción de Solicitudes de Afiliación y Traspaso
    - Resguardo y/o Recuperación de formularios de Afiliación y Traspaso

11. Beneficios
    - Asesoramiento e Información al Beneficiario
    - Procedimientos y Plazos de Tramitación de las solicitudes de beneficios
    - Determinación de Derechos
    - Pago de Prestaciones

12. Sistemas y Tecnología
    - Gestión de la Continuidad Operativa
    - Gestión de la Seguridad de la Información
    - Aseguramiento de la Calidad
    - Desarrollo, implementación y mantenimiento de Sistemas
    - Gestión de los procesos operativos de tecnología
    - Resguardo y recuperación de la información

13. Selección y Capacitación de Personal
    - Capacidad Técnica
    - Experiencia
    - Conducta social

14. Designación de Atribuciones sobre el Negocio
    - Facultades Delegadas por el Consejo y Criterios
    - Facultades Delegadas por el Director General y Criterios
    - Facultades Delegadas por Otros Órganos y Criterios

15. Responsabilidades Compartidas
    - Responsabilidades mancomunadas para idénticos niveles de responsabilidad
    - Responsabilidades mancomunadas por jerarquía
    - Responsabilidades mancomunadas entre el Consejo y la Administración

16. Escalamiento de Información y Decisión
    - Aplicables a Adquisiciones de Activos
    - Aplicables a Ventas de Activos
    - Aplicables a Contratación de Fianzas, Seguros y Financiamiento
    - Decisiones Criticas del Negocio

Párrafo: En adición a los procesos listados en este artículo, las Administradoras, la TSS y la EPBD deben remitir las políticas, los manuales, procedimientos y mapas de cualquier otro proceso relacionado, que estas consideren representativos de riesgo operativo.

Artículo 24. Base de Datos de Eventos de Pérdida

Las Administradoras, la TSS y la EPBD deben contar con una base de datos de los eventos de pérdida por riesgo operativo.

Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas, por lo cual la entidad debe estar en capacidad de agrupar las pérdidas ocurridas por evento.

La base de datos debe cumplir con los criterios mínimos siguientes:

a) Mantener un registro de los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.

b) Registrar, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código de identificación del evento.
- Tipo de evento de pérdida (según tipos de eventos señalados en el Artículo 13 de la presente Resolución).
- Proceso y tarea en el que se presentó el evento.
- Causa que lo propició (falla humana, del sistema, de las bases de datos o sus sistemas, del equipo o de cualquier otro elemento de soporte).
- Descripción detallada del evento.
- Fecha y hora de ocurrencia o de inicio del evento, en caso de estar disponible la hora.
- Fecha de descubrimiento del evento.
- Fecha de registro contable del evento.
- Monto(s) bruto(s) de la(s) pérdida(s), moneda y tipo de cambio.
- Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
- Monto total recuperado, moneda y tipo de cambio.
- Cuenta(s) contable(s) asociadas, en caso de que aplique.

c) En el caso de eventos con pérdidas múltiples, las Administradoras y las otras entidades supervisadas por la Superintendencia podrán registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

d) Por otro lado, debe registrarse la información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

e) Deben definirse y documentarse criterios objetivos para asignar los eventos de pérdida a los tipos de evento señalados en el Artículo 13 de la presente Resolución. Asimismo, deben definirse criterios específicos para aquellos casos en que un evento esté asociado a más de una línea de negocio.

f) Debe definirse un monto mínimo de pérdida a partir del cual debe contarse con un expediente físico o electrónico que contenga información adicional a la solicitada en el literal b) de este Artículo y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la entidad,

incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos. Dicho monto mínimo debe ser aprobado por el Comité de Riesgo Operativo.

g) La base de datos de eventos de pérdidas operativas de cada Administradora debe contar con un espejo en la Superintendencia de Pensiones.

h) La base de datos a que se refiere el presente artículo debe funcionar con aprobación de la Superintendencia a más tardar en un período de dos (2) años a partir de la emisión de la presente Resolución.

Artículo 25. Gestión de la continuidad del negocio y de la seguridad de la información.

Las Administradoras y las otras entidades supervisadas por la Superintendencia deben implementar un sistema de gestión de la continuidad del negocio que tenga como objetivo ejecutar respuestas efectivas para que la operatividad de su negocio continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la entidad.
Asimismo, las Administradoras y las otras entidades supervisadas por la Superintendencia deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Artículo 26. Subcontratación

Con el fin de gestionar los riesgos operativos asociados a la subcontratación, las Administradoras y las otras entidades supervisadas por la Superintendencia deben establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. Dichas políticas y procedimientos deben considerar:

a) El proceso de selección del proveedor del servicio, de acuerdo al marco legal vigente.
b) La elaboración del acuerdo de subcontratación, que establezca las responsabilidades de las partes.
c) La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación.
d) La implementación de un entorno de control efectivo.
e) Establecimiento de planes de continuidad

Los acuerdos de subcontratación deben formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, definir claramente las responsabilidades del proveedor y de la entidad e incluir una cláusula que permita a la Superintendencia la revisión de los procesos subcontratados al proveedor de servicios.

Dichos contratos deben incluir una cláusula que indique que la proveedora le asegurará a la entidad pistas de auditorías necesarias, de forma que existan pruebas para cualquier acción legal, y las mismas deben estar disponibles por el tiempo que exija la ley. Además, dichas cláusulas

deben establecer que la empresa proveedora garantice la disponibilidad de los servicios contratados.

La Superintendencia podrá objetar la tercerización del proceso cuando no se cumplan con las normativas vigentes establecidas por el Consejo Nacional de la Seguridad Social y por esta Superintendencia.

a) La Superintendencia podrá requerir a las Administradoras y a las otras entidades supervisadas por la Superintendencia todos los documentos necesarios para la supervisión de la evaluación del riesgo operativo.

b) La documentación debe ser remitida a la Superintendencia, en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura.

CAPÍTULO VII

TECNOLOGÍA DE INFORMACIÓN (TI)
OBJETIVOS DE CONTROL DE ALTO NIVEL DE TI

Artículo 27. Planificación y Organización. Las Administradoras y las otras entidades supervisadas por la Superintendencia deben contar con estrategias y tácticas de TI que contribuyan al logro de los objetivos del negocio. La visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas, para lo cual se requiere implementar una estructura organizacional y tecnológica apropiada, tomando en cuenta los aspectos siguientes:

a) Planificación Estratégica. Tener un plan estratégico de TI para administrar y dirigir los recursos de acuerdo con la estrategia del negocio y sus prioridades. El plan debe identificar las oportunidades y limitaciones de TI, evaluar el desempeño actual y determinar el nivel de inversión requerido. El presupuesto debe estar alineado con la estrategia, la cual debe ser ejecutada mediante planes y tareas específicas.

b) Arquitectura de la Información. Crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esa información. Esto debe incluir el desarrollo de un diccionario corporativo de datos que contenga las reglas de sintaxis utilizada en la entidad, el esquema de clasificación y los niveles de seguridad, responsabilidad sobre la integridad de los datos, la efectividad y control de la información compartida a lo largo de las aplicaciones.

c) Dirección tecnológica. Determinar la dirección hacia donde se orientará la tecnología para dar soporte al negocio, mediante la creación de un plan de infraestructura tecnológica que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer

en términos de productos, servicios y mecanismos de aplicación. Ese plan debe actualizarse de acuerdo a la variación de la estructura tecnológica y abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias.

d) **Procesos, organización y relaciones de TI.** La Tecnología de Información debe estar definida tomando en cuenta los requerimientos de personal, las funciones, delegación, autoridad, roles, responsabilidades y supervisión. Las mismas deben asegurar la transparencia y el control, así como el involucramiento de los altos ejecutivos y la gerencia del negocio. Deben existir procesos, políticas administrativas y procedimientos para todas las funciones, con atención específica en el control, aseguramiento de la calidad, administración de riesgos, seguridad de la información, propiedad de los datos, sistemas y la segregación de tareas.

e) **Administración de la inversión de TI.** Establecer un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios y prioridades dentro del presupuesto e identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias.

f) **Comunicación de las acciones y dirección de la gerencia.** Construir un marco de trabajo de control institucional para TI, definir y comunicar las políticas. Un programa de comunicación continua se debe implantar para articular la misión, los objetivos de servicio, las políticas y procedimientos, aprobados y apoyados por la dirección.

g) **Administración de los recursos humanos de TI.** Las entidades sujetas a supervisión deben contratar, mantener y motivar al personal para la creación y entrega de servicios de TI, mediante prácticas definidas y aprobadas que apoyen el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación.

h) **Administración de la calidad.** Construir y mantener un sistema de administración de la calidad, que incluya procesos y estándares probados de adquisición y desarrollo. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables

i) **Administración de proyectos.** Establecer programas y marco de controles administrativos de proyectos de TI que garanticen la correcta asignación de prioridades y la coordinación de esos proyectos. Además deben incluir un plan maestro con asignación de recursos, definición de entregables, aprobación de los usuarios, una guía de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y revisión post-implantación para garantizar la administración de los riesgos del proyecto y la entrega de valor al negocio.

Artículo 28. Adquisición e implementación. Las entidades supervisadas deben llevar a cabo las estrategias de TI mediante soluciones que necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, los cambios y mantenimientos de los sistemas existentes deben garantizar que las soluciones sigan satisfaciendo los objetivos del negocio, en cuanto a:

a) Adquisición de recursos de TI. Definir y ejecutar estándares, políticas y procedimientos para la adquisición, selección y arreglos contractuales con proveedores para garantizar que los recursos de TI se obtengan de manera legal, oportuna y rentable.

b) Administración del cambio. Los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previamente a la implementación y revisar contra los resultados planeados.

Artículo 29. Entrega y soporte. Las Administradoras y las otras entidades supervisadas por la Superintendencia, que provean servicios de TI, deben tomar en cuenta la prestación del servicio, administración de la seguridad y continuidad, el soporte del servicio a los usuarios y la administración de los datos y de las instalaciones operacionales. Específicamente, deben:

a) Administración de niveles de servicio. Contar con definiciones documentadas de los acuerdos de niveles de servicios de TI, que hagan posible una comunicación efectiva entre la gerencia de TI y los clientes del negocio respecto de los servicios requeridos. Además, deben monitorear el cumplimiento de los niveles de servicio para verificar la alineación entre los servicios de TI y los requerimientos del negocio.

b) Administración de servicios de terceros. Los acuerdos de servicios con terceras partes deben estar formalizados mediante contrato, donde se definan claramente los roles, responsabilidades y expectativas, así como la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.

c) Administración del desempeño y capacidad. El desempeño y capacidades de los recursos de TI deben ser monitoreados y revisados periódicamente. Además, anualmente debe realizarse el pronóstico de las necesidades futuras, basado en los requerimientos de carga de trabajo, almacenamiento y contingencias.

d) Continuidad de los servicios. Desarrollar, mantener y probar los planes de continuidad de TI, almacenar respaldos fuera de la instalación y entrenar al personal de forma periódica sobre los planes de continuidad y revisar anualmente la cobertura y necesidades de seguro para TI.

e) **Seguridad de los sistemas.** Mantener la integridad de la información y proteger los activos de TI, mediante un proceso de administración de seguridad. Este debe incluir el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. Además, deben realizar monitoreo de seguridad y pruebas periódicas, así como ejecutar las acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

f) **Entrenamiento a los usuarios.** Proveer una educación efectiva a todos los usuarios de sistemas de TI, para lo cual deben identificar las necesidades y elaborar un plan de entrenamiento para cada grupo de usuarios.

g) **Administración de la configuración.** Garantizar la integridad de las configuraciones de hardware y software, mediante el establecimiento y mantenimiento de un repositorio de configuraciones completo y preciso.

h) **Administración de problemas.** Manejar de forma efectiva la administración de problemas e incidentes. Este proceso requiere la identificación, clasificación, análisis de las causas desde su raíz, y la resolución de los mismos. Además, incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas.

i) **Administración de los datos.** Contar con una administración de datos que identifique de forma efectiva los requerimientos de datos. El proceso de administración de información también debe incluir el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios.

j) **Administración del ambiente físico.** Velar por la protección de los equipos de cómputo y del personal. Las instalaciones deben estar bien diseñadas y administradas. El proceso de administración del ambiente físico incluye la definición de los requerimientos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso.

Artículo 30. Monitoreo y Evaluación. Los procesos de TI tienen que evaluarse de forma regular en cuanto a su calidad y cumplimiento de los requerimientos de control. En ese sentido, las entidades deben establecer un programa de control interno efectivo para TI que incluya un proceso bien definido de monitoreo. Además, deben incluir las excepciones de control, resultados de las autoevaluaciones y revisiones por parte de auditores de sistemas.

Párrafo: Las áreas de auditoría interna de sistemas de información (ASI) y/o tecnología de información (ATI), incluyendo las contratadas de forma externa y las firmas de auditores externos que brinden estos servicios, deben contar con personal certificado en ASI y/o ATI, o por lo menos con una entidad reconocida internacionalmente.

CAPÍTULO VIII

DE LA METODOLOGÍA PARA LA AUTOEVALUACIÓN DE RIESGO OPERATIVO

Artículo 31. Metodología de autoevaluación

La autoevaluación de riesgo operativo debe incorporar las siguientes dimensiones analíticas, como componentes de la calificación final.

- Dimensión de Gestión de los Procesos Críticos, 55%
- Dimensión de Gestión Administrativa, 35%
- Dimensión de Desempeño de las AFP, 10%

En el caso de la TSS y de la DGJP, la autoevaluación de riesgo operativo debe incorporar las siguientes dimensiones analíticas, como componentes de la calificación final.

- Dimensión de Gestión de los Procesos Críticos, 60%
- Dimensión de Gestión Administrativa, 40%

Estos ponderadores pueden ser modificados siempre y cuando exista fundamentación técnica de un experto independiente y para aplicarse debe contar con la aprobación previa de la Superintendencia de Pensiones.

Párrafo I. La dimensión de gestión de los procesos críticos debe incorporar los procesos y subprocesos críticos siguientes:

a) Administradoras

- Afiliaciones y Traspasos, 10%
    - Asesoramiento y Atención al Público
    - Impresión y Distribución de Formularios de Afiliación y Traspaso
    - Gestión de Suscripción de Solicitudes de Afiliación y Traspaso
    - Resguardo y/o Recuperación de formularios de Afiliación y Traspaso

- Dispersión de la Recaudación y Administración de la CCI, 15%
    - Apertura y Cierre de CCI
    - Confirmación de la Individualización, Dispersión de la Recaudación y Administración de Cuentas Individuales
    - Emisión y Envío de los Estados de Cuenta,
    - Resguardo y/o Recuperación de la información relacionada con los procesos de Individualización, Dispersión de la Recaudación y Administración de las Cuentas Individuales

- Inversiones, 30%
    - Definición de la Política de Inversión
    - Realización de operaciones Financieras
    - Liquidación de Operaciones Financieras
    - Contabilización de Operaciones Financieras y Emisión del Informe Diario

- Beneficios, 30%
    - Asesoramiento e Información al Beneficiario
    - Procedimientos y Plazos de Tramitación de las solicitudes de beneficios
    - Determinación de Derechos
    - Pago de Prestaciones

- Sistemas y Tecnología, 15%
    - Gestión de la Continuidad Operativa
    - Gestión de la Seguridad de la Información
    - Aseguramiento de la Calidad

- Desarrollo, implementación y mantenimiento de Sistemas
- Gestión de los procesos operativos de tecnología
- Resguardo y recuperación de la información
- Planificación y Organización
- Adquisición e Implementación
- Entrega y Soporte
- Monitoreo y Evaluación

b) Tesorería de la Seguridad Social y la Empresa Procesadora de la Base de Datos (procesos y subprocesos relativos a los sistemas previsionales, Seguro de Vejez, Discapacidad y Sobrevivencia)

- Procesos detallados de cada producto del portafolio de servicios
- Políticas y procesos de administración plataformas tecnológicas
- Políticas y procesos de bases de datos y su arquitectura
- Políticas y procesos de comunicaciones
- Políticas y procesos de desarrollo de software
- Políticas y procesos de seguridad física y lógica
- Políticas de seguridad de la información
- Políticas de operación de tecnologías de información
- Políticas de mantenimiento
- Políticas de ciclo de vida de tecnologías de información
- Política de actualización y planeación tecnológica
- Políticas de calidad
- Políticas de servicio a clientes y de cumplimiento de niveles de servicio

- Políticas de cumplimiento normativo
- Políticas de continuidad y recuperación en casos de desastres

c) DGJP

- Traspasos, 5%
    - Asesoramiento y Atención al Público
    - Impresión y Distribución de Formularios de Afiliación y Traspaso
    - Gestión de Suscripción de Solicitudes de Afiliación y Traspaso
    - Resguardo y/o Recuperación de formularios de Afiliación y Traspaso

- Beneficios, 75%
    - Asesoramiento e Información al Beneficiario
    - Procedimientos y Plazos de Tramitación de las solicitudes de beneficios
    - Determinación de Derechos
    - Pago de Prestaciones

- Sistemas y Tecnología, 20%
    - Gestión de la Continuidad Operativa
    - Gestión de la Seguridad de la Información
    - Aseguramiento de la Calidad
    - Desarrollo, implementación y mantenimiento de Sistemas
    - Gestión de los procesos operativos de tecnología
    - Resguardo y recuperación de la información
    - Planificación y Organización
    - Adquisición e Implementación
    - Entrega y Soporte

- Monitoreo y Evaluación

Párrafo II. La dimensión de gestión administrativa de las Administradoras, la TSS y la EPBD debe incorporar los procesos y subprocesos críticos siguientes:

- Selección y Capacitación de Personal, 20%
  - Capacidad Técnica
  - Experiencia
  - Conducta Social
- Designación de Atribuciones sobre el Negocio, 30%
  - Facultades Delegadas por el Consejo y Criterios
  - Facultades Delegadas por el Director General y Criterios
  - Facultades Delegadas por Otros Órganos y Criterios
- Responsabilidades Compartidas, 30%
  - Responsabilidades compartidas para idénticos niveles de responsabilidad
  - Responsabilidades compartidas por jerarquía
  - Responsabilidades compartidas entre el Consejo y la Administración
- Escalamiento de Información y Decisión, 20%
  - Aplicables a Adquisiciones de Activos
  - Aplicables a Ventas de Activos
  - Aplicables a Contratación de Fianzas, Seguros y Financiamiento
  - Decisiones Criticas del Negocio

Párrafo III. Los aspectos mínimos a ser evaluados en la dimensión de desempeño son:

- Rentabilidad

- Solvencia
- Liquidez

CAPÍTULO IX

REQUERIMIENTOS DE INFORMACIÓN

Artículo 32. Informe a la Superintendencia
Las entidades citadas en el Artículo 2 de esta resolución deben presentar a la Superintendencia en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura, dentro de los treinta (30) días calendario siguientes al corte de cada año, un informe de evaluación del riesgo operativo que enfrenta la entidad por proceso y área operativa y de apoyo.

Párrafo I: Este informe debe incluir el informe anual de la Unidad de Administración de Riesgo Operativo donde refleja el cumplimiento de sus responsabilidades, así como el plan de trabajo a realizar durante el año siguiente.

Párrafo II: Asimismo, debe contemplar, por lo menos, la metodología empleada para el control de riesgo operativo y sus modificaciones, la identificación de los riesgos a que está expuesta y que enfrenta la entidad por cada proceso crítico y área operativa y de apoyo, la evaluación y valoración de los riesgos identificados, las medidas adoptadas para controlar el riesgo operativo materializado y sus consecuencias (refiriéndose por lo menos a los aspectos siguientes: evitar el riesgo, reducir su probabilidad de ocurrencia y sus consecuencias, transferir o retener el riesgo), plazos para su aplicación y responsables de ejecutarlas.

Artículo 33. Las entidades deben informar a la Superintendencia, anualmente, las consecuencias económicas, financieras y reputacionales que ellas enfrentarían derivadas de la materialización de los riesgos identificados.

Artículo 34. Información adicional
La Superintendencia podrá requerir a las entidades, toda la documentación e información adicional que considere necesaria para la supervisión de la evaluación del riesgo operativo.

Las entidades deben tener a disposición de la Superintendencia toda la documentación referida por la presente Resolución, los informes de auditoría y las revisiones realizadas por la casa matriz si aplica.

La documentación debe ser remitida a la Superintendencia, en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura.

Párrafo I: La Superintendencia podrá requerir a las entidades, la divulgación de información correspondiente a la gestión del riesgo operativo de forma que los usuarios puedan determinar si la entidad identifica, evalúa, monitorea y controla o mitiga efectivamente este riesgo.

Artículo 35. La autoevaluación de riesgo operativo debe aplicarse anualmente con corte al 31 de diciembre de cada año y remitida a la Superintendencia en formato físico y en dispositivo de almacenamiento electrónico, sólo lectura, durante los primeros treinta (30) días calendarios del año siguiente.

DISPOSICIONES TRANSITORIAS

Artículo 36. En un plazo no mayor de ciento veinte (120) días calendario, contado a partir de la fecha de publicación de la presente Resolución, las entidades citadas en el Artículo 2 deben remitir un plan para implementar las disposiciones establecidas en la misma. Este Plan incluirá el programa a ejecutar y las personas responsables, y debe estar debidamente aprobado por el Consejo de Administración u órgano equivalente de la entidad**.** El referido plan debe ser ejecutado y aplicado en un plazo no mayor de dieciocho (18) meses, contado a partir de la fecha de aprobación del plan para la implementación de las disposiciones establecidas en esta Resolución, con excepción de lo dispuesto en el literal h) del Artículo 24 de esta Resolución.

Dada en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los trece (13) días del mes de abril del año dos mil doce (2012).

Joaquín Gerónimo
Superintendente de Pensiones