NPB4-50

El Consejo Directivo de la Superintendencia del Sistema Financiero, en uso de la potestad que le confiere el literal k) del artículo 10 de la Ley Orgánica de la Superintendencia del Sistema Financiero y para dar cumplimiento a los artículos 63 e inciso final del artículo 66 de la Ley de Bancos, al literal a) del artículo 24 de la Ley de Sociedades de Seguros y a los artículos 41 y 155 de la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito, acuerda emitir las:

NORMAS PARA LA GESTIÓN DEL RIESGO OPERACIONAL DE LAS ENTIDADES FINANCIERAS

CAPÍTULO I
OBJETO Y SUJETOS OBLIGADOS

Objeto

Art. 1.- El objeto de las presentes Normas es proporcionar lineamientos mínimos para una adecuada gestión del riesgo operacional y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para la gestión del riesgo, acordes con la naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones.

Se entiende por riesgo operacional la posibilidad de incurrir en pérdidas debido a fallas en los procesos, de las personas, en los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal que consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros.

Estas Normas complementan a las disposiciones establecidas en las Normas para la Gestión Integral de Riesgos de las Entidades Financieras (NPB4-47) y las Normas de Gobierno Corporativo para las Entidades Financieras (NPB4-48).

Sujetos

Art. 2.- Los sujetos obligados al cumplimiento de las presentes Normas son: (2)

a) Los bancos constituidos en El Salvador, sus oficinas en el extranjero y sus subsidiarias; (2)

b) Las sucursales y oficinas de bancos extranjeros establecidos en el país en lo pertinente; (2)

c) Las sociedades de seguros, sus sucursales en el extranjero; (2)

d) Las sucursales de sociedades de seguros extranjeras establecidas en el país en lo pertinente; (2)

e) Los bancos cooperativos, las sociedades de ahorro y crédito y las federaciones reguladas por la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito; (2)

f) El Banco Hipotecario de El Salvador, S.A.; (2)

g) El Fondo Social para la Vivienda y el Fondo Nacional de Vivienda Popular, en lo que no contradiga a sus leyes de creación ni a lo dispuesto por la Corte de Cuentas; (2)

h) El Banco de Fomento Agropecuario, en lo que no contradiga a su ley de creación ni a lo dispuesto por la Corte de Cuentas e; (2)

i) El Banco de Desarrollo de El Salvador, en lo que no contradiga a su ley de creación ni a lo dispuesto por la Corte de Cuentas. (2)

En las presentes Normas, con los vocablos genéricos "entidad o entidades", "Superintendencia" y "Junta Directiva", se designan respectivamente a los sujetos obligados al cumplimiento de estas Normas, a la Superintendencia del Sistema Financiero y a la Junta Directiva o Consejo de Administración de los sujetos obligados en los casos que corresponda.

CAPÍTULO II
FACTORES Y EVENTOS DE RIESGO OPERACIONAL

Factores de riesgo

Art. 3.- Las entidades deben gestionar los diferentes factores generadores de riesgo operacional, siendo éstos los siguientes:

a) **Procesos:** Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades deben contar con procesos documentados, definidos y actualizados permanentemente, que pueden ser agrupados en procesos estratégicos y operativos.

Las entidades deben gestionar apropiadamente los riesgos asociados a dichos procesos, con énfasis en las fallas o debilidades que presenten, dado que éstas pueden tener como consecuencia el desarrollo deficiente de las operaciones.

b) **Personas:** Las entidades deben establecer políticas, procesos y procedimientos que procuren una adecuada planificación y administración del capital humano, que incluyan el proceso de contratación, permanencia y desvinculación del personal.

Asimismo, deben establecer mecanismos preventivos que permitan identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros, asociadas al personal, vinculado directa o indirectamente a la entidad; de tal modo que se minimice la posibilidad de pérdidas económicas.

La vinculación directa es aquélla que está basada en un contrato interno de trabajo, de acuerdo a la legislación laboral respectiva. La vinculación indirecta está referida a aquellas personas que tienen una relación jurídica con la entidad para la prestación de determinados servicios, diferente de aquélla que se origina de un contrato interno de trabajo.

c) **Tecnología de información:** Las entidades deben gestionar los riesgos asociados a la tecnología de información, entre otros, los 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 la calidad de la información y una adecuada inversión en tecnología.

d) **Acontecimientos externos:** Las entidades deben gestionar los riesgos asociados a acontecimientos externos ajenos al control de la entidad que pudiesen alterar el desarrollo normal de sus actividades, relacionados a fallas en los servicios críticos provistos por terceros, contingencias legales, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

Eventos de riesgo operacional

Art. 4.- Los eventos de riesgo operacional son aquellas situaciones que afectan el normal desarrollo de las operaciones de la entidad, los cuales incluyen los incidentes ocurridos y eventos potenciales que pudieren generar pérdidas económicas y pueden o no afectar el estado de resultados, siendo estos los siguientes:

a) Fraude interno;
b) Fraude externo;
c) Relaciones laborales y seguridad en el puesto de trabajo;
d) Clientes, productos y prácticas de negocio;
e) Daños en activos materiales;
f) Interrupción del negocio y fallas en los sistemas, y
g) Ejecución, entrega y gestión de procesos.

CAPÍTULO III
GESTION DEL RIESGO OPERACIONAL

Sistema de organización

Art. 5.- Las entidades deben establecer una estructura organizacional o funcional adecuada a su modelo de negocios y apropiadamente segregada, que delimite claramente funciones y responsabilidades, así como los niveles de dependencia e interrelación que les corresponden a cada una de las áreas involucradas en la realización de actividades relativas al riesgo operacional.

Todos estos aspectos deben estar contemplados en el manual respectivo, aprobado por la Junta Directiva de la entidad.

Junta Directiva

Art. 6.- La Junta Directiva de la entidad es el Órgano directamente responsable de la gestión del riesgo operacional, por lo que debe:

a) Aprobar las estrategias, políticas, manuales y planes de continuidad del negocio de la entidad para la gestión del riesgo operacional, y asegurarse que la Alta Gerencia los implemente efectivamente;
b) Asignar y aprobar los recursos necesarios para implementar y mantener en funcionamiento la gestión del riesgo operacional en forma efectiva y eficiente, y
c) Asegurarse de que Auditoría Interna verifique la existencia y el cumplimiento del esquema de gestión del riesgo operacional.

Comité de Riesgos

Art. 7.- El Comité de Riesgos es el encargado de velar por una sana gestión del riesgo operacional de la entidad, por lo que debe:

a) Evaluar, revisar y proponer para aprobación de la Junta Directiva las estrategias, políticas, manuales y planes de continuidad del negocio de gestión del riesgo operacional;
b) Supervisar que la gestión del riesgo operacional sea efectiva y que los eventos de riesgos sean consistentemente identificados, evaluados, mitigados y monitoreados;
c) Proponer los mecanismos para la implementación de las acciones correctivas requeridas en caso de que existan desviaciones con respecto al nivel de tolerancia al riesgo operacional;
d) Aprobar las metodologías de gestión del riesgo operacional; y
e) Apoyar la labor de la Unidad de Gestión de Riesgos en la implementación de la gestión de riesgo operacional.

Alta Gerencia

Art. 8.- La Alta Gerencia es la responsable de la implementación de la gestión del riesgo operacional, de las estrategias, políticas, manuales y planes de continuidad del negocio, autorizados por la Junta Directiva.

Unidad de Riesgos

Art. 9.- La Unidad de Riesgos es la encargada de implementar la metodología de gestión de riesgo operacional, por lo que deberá:

a) Diseñar y someter a la aprobación de la Junta Directiva, a través del Comité de Riesgos, las estrategias, políticas, manuales y planes de continuidad del negocio para la gestión del riesgo operacional;
b) Diseñar y someter a la aprobación del Comité de Riesgos la metodología para la gestión del riesgo operacional;
c) Apoyar y asistir a las demás unidades de gestión para la implementación de la metodología del riesgo operacional;
d) Elaborar una opinión sobre el riesgo de nuevos productos o servicios, previo a su lanzamiento; así como también ante cambios importantes en el ambiente operacional o informático, y
e) Reportar oportunamente y de forma completa y detallada las fallas en los diferentes factores de riesgo operacional a la Junta Directiva a través del Comité de Riesgos.

Auditoría Interna

Art. 10.- La Auditoría Interna debe evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional y dar seguimiento al cumplimiento del plan de trabajo de la Unidad de Riesgo, lo que involucra todo lo dispuesto en las presentes Normas.

Etapas de la gestión

Art. 11- Para la gestión del riesgo operacional las entidades deben contar con un proceso continúo y documentado para:

a) **Identificación:** Las entidades deben establecer un proceso de identificación de todos sus eventos de riesgos operacionales agrupándolos de acuerdo a lo establecido en el Anexo No. 1, de tal forma que les permita establecer su mapa de riesgo operacional.

   Asimismo, en el caso de los bancos, bancos cooperativos y sociedades de ahorro y crédito, es conveniente que la identificación de los eventos puedan agruparse, adicionalmente, de acuerdo a las líneas de negocio que la entidad mantiene, tal como se amplía en el Anexo No. 2, y para las sociedades de seguro, tal como se detalla en el Anexo No. 3.

b) **Medición:** Las entidades deben estimar o cuantificar el riesgo operacional considerando la probabilidad de ocurrencia y el impacto económico en los resultados de la entidad. Esta cuantificación es esencial para la entidad porque en función a ellas se establecen las medidas de control y mitigación que buscan minimizar pérdidas por este riesgo.

   Las metodologías y herramientas para estimar o cuantificar el riesgo operacional deben estar de conformidad con el tamaño, naturaleza de los niveles de riesgos asumidos por la entidad y volumen de sus operaciones.

c) **Control y mitigación:** Se refiere a las acciones o mecanismos de cobertura y control implementados por la entidad con la finalidad de prevenir o reducir los efectos negativos en caso de materializarse los eventos adversos de riesgo operacional.

   Debe establecerse un plan de acción para implementar medidas que busquen mitigar los eventos de riesgo identificados. Este plan debe detallar las acciones a implementar, el plazo estimado de ejecución y los responsables directos de dicha ejecución.

d) **Monitoreo y comunicación:** Las entidades deben dar seguimiento sistemático y oportuno a los eventos de riesgo operacional, así como a los resultados de las acciones adoptadas.

   El seguimiento deberá asegurar una revisión periódica y la generación de información suficiente para apoyar los procesos de toma de decisiones.

   Las entidades deben realizar un monitoreo permanente de su mapa de riesgos y exposición a pérdidas por riesgo operacional, debiendo cumplir como mínimo con los siguientes aspectos:

   i. Desarrollar procesos de seguimiento efectivo y permanente que permitan la rápida detección y corrección de las deficiencias;
   ii. Establecer indicadores que evidencien potenciales riesgos operacionales;
   iii. Asegurar que los controles internos establecidos se encuentren funcionando en forma efectiva y eficiente; y
   iv. Asegurar que los riesgos residuales se encuentren bajo el nivel de tolerancia establecido por cada entidad.

   La entidad debe contar con sistemas de información gerencial y bases de datos estadísticas que posibiliten la generación de información oportuna, confiable, consistente

y homogénea para los reportes periódicos a la Junta Directiva, Comité de Riesgos y/o Alta Gerencia, así como a otros interesados responsables de la toma de decisiones en la gestión del riesgo operacional.

Políticas

Art. 12.- Las entidades deben contar con políticas para definir el marco de gestión del riesgo operacional, que les permita reducir su vulnerabilidad y pérdidas por dicho riesgo e impulsar a nivel de toda la organización la cultura de prevención y control de este riesgo, asegurando el cumplimiento de las normas internas y externas relacionadas al mismo.

Las políticas de gestión del riesgo operacional deben considerar, entre otros aspectos, la categorización de eventos de pérdida, las funciones y responsabilidades en la gestión del riesgo operacional, criterios de identificación, medición, control, mitigación y sistemas de información para la gestión del riesgo operacional

Manual de gestión de riesgo operacional

Art. 13.- Las entidades deben contar con un manual de gestión de riesgo operacional que agrupe las políticas de gestión de este riesgo, las funciones y responsabilidades de las áreas involucradas, la metodología, los procesos asociados y la periodicidad con la que se debe informar a la Junta Directiva y a la Alta Gerencia sobre la exposición al riesgo operacional.

CAPÍTULO IV
DISPOSICIONES GENERALES

Prestación de servicios por terceros

Art. 14.- Las entidades deben establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los servicios críticos brindados por terceros, es decir aquellos que puedan interrumpir el normal desarrollo de las operaciones, definidos en las políticas de cada entidad.

La prestación de servicios debe formalizarse mediante contratos firmados, que incluya el alcance del servicio y defina claramente las responsabilidades del proveedor y de la entidad. Asimismo, deben incluir una cláusula que obligue al proveedor a documentar los servicios brindados y le garantice el establecimiento de planes de contingencia y de continuidad del servicio brindado. Además, deben incluirse cláusulas que faciliten una adecuada revisión de la respectiva prestación de servicios por parte de las mismas entidades o eventualmente de la Superintendencia y de otros organismos supervisores.

Independientemente que determinados servicios sean realizados por terceras partes, las entidades sujetas a estas Normas son las responsables de asegurar el cumplimiento de las disposiciones que le son aplicables.

Las entidades deben contar con un control centralizado de todos los servicios prestados por terceros que como mínimo debe contener el nombre del proveedor, el tipo de servicio, el monto del contrato, contraparte dentro de la entidad y su vigencia. Dicho control debe estar a disposición de la Superintendencia en el momento que ésta lo requiera.

Riesgo legal

Art. 15.- Además de lo establecido en estas Normas, para el caso del riesgo legal, las entidades deben establecer como mínimo políticas y controles específicos, de manera que, previo a la celebración de contratos, actos jurídicos u operaciones que realizan, se analice la validez jurídica y se procure la adecuada verificación legal. Asimismo, dichas políticas y procedimientos deben contener aspectos relativos a la conservación ordenada, completa, íntegra y oportuna de la información y documentación que soporta las operaciones de la entidad.

Plan de continuidad del negocio y de seguridad de la información

Art. 16.- Las entidades deben implementar un sistema de gestión de continuidad del negocio en caso de interrupciones que incluya planes de contingencia, análisis de impacto en el negocio, plan de recuperación de desastres y planes de gestión del incidente, que aseguren la operatividad normal del negocio ante la ocurrencia de eventos adversos.

Los planes de continuidad del negocio deben considerar como mínimo lo siguiente:

a) La identificación de eventos que ponen en riesgo la continuidad del negocio, las actividades a realizar para superarlos, las alternativas de operación y el retorno a las actividades normales;
b) La definición de los roles y responsables de implementarlos;
c) La realización de las pruebas necesarias para confirmar su eficacia y eficiencia, al menos una vez al año; y
d) La divulgación del plan a todos los miembros de la entidad.

Asimismo, las entidades deben contar con un sistema de gestión de seguridad de la información que les garantice su disponibilidad, integridad y confidencialidad.

Metodologías para la gestión del riesgo operacional

Art. 17.- Las entidades deben definir la metodología que utilizarán para gestionar el riesgo operacional, la que debe estar adecuadamente documentada e implementada en toda la entidad en forma consistente, para lo cual deben asignar los recursos suficientes para su aplicación.

CAPÍTULO V
REQUERIMIENTO DE INFORMACION

Bases de datos

Art. 18.- Las entidades deben conformar una base de datos centralizada que permita registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operacional. Éstos deben ser clasificados por factores, determinando la frecuencia del evento y el efecto producido, debiendo contener como mínimo los campos que se detallan en el Anexo No. 4 y remitirlo por medios electrónicos o de la forma que la Superintendencia lo determine.

Informe anual

Art. 19.- Las entidades deben presentar a la Superintendencia, dentro de los primeros ciento veinte (120) días calendario siguientes al cierre de cada ejercicio anual, un informe relativo a las acciones realizadas para el control y la evaluación del riesgo operacional que enfrenta la entidad, por procesos y/o unidad de negocios y de apoyo. El informe deberá contener como mínimo lo siguiente:

a) La definición de la estrategia utilizada para la gestión del riesgo operacional;
b) El detalle de la metodología empleada para la gestión del riesgo operacional;
c) Identificación y evaluación de los riesgos operacionales de eventos críticos ocurridos durante el año, por proceso y/o unidad de negocio y de apoyo; y el detalle de las medidas adoptadas para administrarlos;
d) Detalle de los ejecutivos responsables de las actividades de control de riesgo de los eventos críticos ocurridos durante el año; y
e) Plan de Actividades a desarrollar por la Unidad de Riesgos, relacionado con la gestión del riesgo operacional.

Remisión de base de datos

Art. 20.- Las entidades deben enviar a la Superintendencia, de forma anual y a más tardar el treinta y uno de enero de cada año, los eventos contenidos en las "Bases de datos" a que hacen mención las presentes Normas, iniciando con la base de datos del año dos mil trece, remitiéndolo por medios electrónicos o de la forma que la Superintendencia lo determine. (1)

Remisión de Manual de Gestión de Riesgo Operacional

Art. 21.- Las entidades deberán remitir en forma electrónica a la Superintendencia, a más tardar el uno de agosto de dos mil doce, el Manual de Gestión de Riesgo Operacional a que hacen mención las presentes Normas; asimismo, deberán remitir el Manual cada vez que realicen cambios al mismo.

CAPÍTULO VI
DISPOSICIONES TRANSITORIAS Y VIGENCIA

Transitorio

Art. 22.- Para cumplir con las disposiciones de estas Normas, las entidades deben presentar a la Superintendencia un Plan de Actividades, dentro de los seis meses siguientes a su vigencia. Una vez presentado, las entidades deben iniciar y completar su ejecución dentro de un plazo máximo de seis meses, contados a partir de la presentación del mismo.

Lo no previsto

Art. 23.- Lo no previsto en las presentes Normas será resuelto por el Consejo Directivo de la Superintendencia.

Vigencia

Art. 24.- Las presentes Normas entrarán en vigencia a partir del uno de agosto de dos mil once.

(Normas aprobadas por el Consejo Directivo de la Superintendencia del Sistema Financiero, en sesión No. CD-22/11, de fecha 29 de junio de 2011)

(1) Modificaciones Aprobadas por el Comité de Normas del Banco Central de Reserva de El Salvador, en Sesión No. CN-02/2012 de fecha 3 de febrero de 2012, con vigencia a partir del día 9 de marzo de dos mil doce.

(2) Modificaciones Aprobadas por el Comité de Normas del Banco Central de Reserva de El Salvador, en Sesión No. CN-05/2012 de fecha 27 de abril de 2012, con vigencia a partir del día 14 de mayo de dos mil doce.

ANEXO N° 1

TIPOS DE EVENTOS POR RIESGO OPERACIONAL

Tipo de evento (Nivel 1)	**Definición**	**Tipo de evento (Nivel 2)**	**Ejemplos**
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la entidad.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas económicas), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
Relaciones 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 reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Clientes, productos y prácticas de negocios	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), infringir la privacidad de información sobre clientes minoristas, infringir la privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la entidad), lavado de dinero.
		Productos defectuosos	Defectos del producto (no autorizado, etc.), error de los modelos.
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.	Desastres y otros acontecimientos	Desastres naturales, pérdidas causadas por personas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
Ejecución, entrega y gestión de	Pérdidas derivadas de errores en el procesamiento de operaciones o en	Recepción, ejecución y mantenimiento de	Errores de introducción de datos, mantenimiento o descarga,

procesos	la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	operaciones	incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo .
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos.
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

ANEXO No.2

DETALLE DE LÍNEAS DE NEGOCIO

Nivel 1	Nivel 2	Grupos de Actividades
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titularización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de Administraciones locales / públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda.
	Creación de Mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minorista, servicios bancarios, fideicomisos.
	Banca privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y asesoramiento de inversión.
	Servicios de tarjetas	Tarjetas de empresas / comerciales, de marca privada y minoristas.
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoraje, arrendamiento financiero, préstamos, garantías, letras de cambio.
Pago y liquidación	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Certificados de depósitos, operaciones para préstamo de títulos valores.
	Agencia para empresas	Agentes de emisiones de deudas y pagos.
	Fideicomisos de empresas	Comisiones de confianza y otros servicios
Administración de activos	Administración discrecional de fondos	Minoristas, institucionales, cerrados, abiertos, participaciones accionariales.
	Administración no discrecional de fondos	Minoristas, institucionales, de capital fijo, de capital variable.
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo.

ANEXO No. 3

DETALLE DE LÍNEAS DE NEGOCIOS DE SOCIEDADES DE SEGUROS.

Nivel 1	Nivel 2	Grupos de actividades
Seguros de Personas	Seguros de Vida	Vida individual de largo plazo, vida individual de corto plazo, colectivos y otros planes
	Seguros Previsionales rentas y pensiones	Renta de invalidez y sobrevivencia, sepelio, otras rentas y pensiones
	Seguros de Accidentes y enfermedades	Salud y hospitalización, accidentes personales, accidentes viajes aéreos y escolares
Seguros de Daños o Generales	Incendios y Líneas Aliadas	Incendios, Tormentas, Terremotos, Huracanes, Granizo.
	Automotores	Automotores particulares, automotores colectivos, motocicletas, transporte colectivo,
	Seguros Generales	Rotura de cristales, transporte marítimo, transporte aéreo, marítimos cascos, aviación, robo y hurto, fidelidad, seguro de banco, todo riesgo contratistas, rotura de maquinaria, montaje contra todo riesgo, todo riesgo electrónico, calderas, ganadero agrícola, crédito interno y misceláneo.
Fianzas	Fidelidad	Fidelidad
	Garantía	Licitación y oferta, fiel cumplimiento, buena calidad, buena obra, fianza de responsabilidad civil, fianza de construcción, otras fianzas
	Motoristas	Motorista

ANEXO No.4

TABLA DE CONTENIDO DE LA BASE DE DATOS DE REGISTRO DE EVENTOS

1	Referencia	Código interno que identifique el evento en forma secuencial.
2	Factor de riesgo operacional	De acuerdo a la clasificación establecida en Capítulo II de estas Normas.
3	Tipo de evento de pérdida	Identifica el tipo de pérdida, de acuerdo con la clasificación del Anexo No. 1.
4	Líneas de negocio	Identificación de la línea de negocio que origino el evento**,** siendo las principales para el caso de bancos, bancos cooperativos y sociedades de ahorro y crédito las detalladas en Anexo No.2. Para las Sociedades de Seguro, las principales líneas de negocios, se detallan en Anexo No.3.
5	Descripción del evento	Descripción detallada del evento. Canal de servicio o atención al cliente (cuando aplica) Zona geográfica.
6	Fecha de inicio del evento	Fecha en que se inicia el evento. Día, mes, año.
7	Fecha de finalización del evento	Fecha en que finaliza el evento. Día, mes, año.
8	Fecha del descubrimiento	Fecha en que se descubre el evento. Día, mes, año.
9	Fecha de contabilización	Fecha en que se registra contablemente la pérdida económica por el evento. Día, mes, año, hora.
10	Monto	El monto a que asciende la pérdida, cuantificación económica de la ocurrencia del evento de riesgo operacional y los gastos derivados de su atención.
11	Divisa	Moneda extranjera en la que se materializa el evento.
12	Cuentas contables afectadas	Identifica las cuentas del Catalogo de Cuentas afectadas.
13	Proceso	Identifica el proceso afectado.
14	Valor total recuperado	El valor total recuperado por la acción directa de la entidad. Incluye los montos recuperados por seguros.
15	Valor recuperado por seguros	Corresponde al valor recuperado por la cobertura a través de un seguro.
16	Producto o servicio afectado	Identifica el producto o servicio afectado por el evento de riesgo operacional.
17	Cuantificación de la severidad del daño	Monto a que asciende la pérdida (neta de cualquier mitigante o recuperación)

Para la creación del registro de eventos de riesgo operacional las entidades podrán utilizar, además de los campos descritos anteriormente, otros que se consideren relevantes.

Las entidades que consideren que las bases de datos de eventos de riesgo operacional sean insuficientes para cuantificar el riesgo operacional, podrán optar por la utilización de bases de datos de fuentes externas, siempre que dichas bases de datos sean normalizadas y adecuadas a las bases de datos internas de la entidad.

GLOSARIO DE TERMINOS

a) Evento de riesgo operacional: Es un suceso o serie de sucesos, de origen interno o externo, que puede o no derivar en pérdidas financieras para la entidad.

b) Factor de riesgo operacional: Es la causa primaria o el origen de un evento operacional.

c) Línea de negocio: Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios para atender un segmento de mercado objetivo.

d) Mapa de riesgos: Es una herramienta que permite presentar una panorámica de los riesgos a los que está expuesta la entidad; independiente de la forma de su presentación, en el que se identifican y se ubican las áreas/actividades/activos (procesos) que podrían verse afectados durante la ocurrencia de un evento adverso. Permite ver las amenazas y medir la magnitud de cada riesgo (probabilidad e impacto económico). Son un instrumento gráfico de gestión de los riesgos que permite comparar los riesgos por su importancia relativa así como en conjunto, permitiendo a la entidad establecer niveles aceptables de riesgo.

e) Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

f) Proceso: Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el usuario, sea interno o externo.

g) Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

h) Riesgo residual: Nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han instrumentado los controles pertinentes para su tratamiento. En todo caso exige un permanente monitoreo para observar su evolución.