LIBRO I.- NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO

TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005)

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en el capítulo I "De la gestión integral y control de riesgos", las instituciones controladas observarán las disposiciones del presente capítulo.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

2.1 **Alta gerencia.-** La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

2.2 **Evento de riesgo operativo.-** Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 **Factor de riesgo operativo.-** Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

2.4 **Proceso.-** Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

2.5 **Insumo.-** Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

2.6 **Proceso crítico.-** Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.7 **Actividad.-** Es el conjunto de tareas;

2.8 **Tarea.-** Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

2.9 **Procedimiento .-** Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

2.10 Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

2.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

2.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones;

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

2.15 Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

2.16 Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

2.17 Instalaciones.- Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información;

2.18 Responsable de la información.- Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.24 Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

2.25 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;

2.26 Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

2.27 Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

2.28 Encriptación.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

2.29 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. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación;

2.30 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 financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento;

2.31 Plan de reanudación.- Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema;

2.32 Plan de recuperación.- Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución;

2.33 Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

2.34 Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores; y,

2.35 Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no

han sido claramente estipuladas. (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.35 del artículo 2.

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 4.- Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí,:

4.1 Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

4.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

4.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

4.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

4.2 Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dichos procesos corresponden a:

4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

4.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

4.2.3 **Los procesos de desvinculación.-** Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

4.3 **Tecnología de información.-** Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar 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.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Dichas políticas, procesos y procedimientos se referirán a:

4.3.1 Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;

4.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;

4.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;

4.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

4.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

4.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

4.3.3 Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

4.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

4.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información

contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

4.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

4.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

4.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

4.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

4.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

4.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

4.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;

4.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

4.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

4.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;

4.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,

4.3.4.12 Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

4.3.5 Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

4.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;

4.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;

4.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,

4.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

4.3.6 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

4.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

4.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;

4.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,

4.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

4.3.7 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

4.4 **Eventos externos.-** En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 5.- En el marco de la administración integral de riesgos, establecido en la sección II "Administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio.

El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.

ARTÍCULO 6.- Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de información adecuada.

ARTÍCULO 7.- Con la finalidad de que las instituciones controladas administren adecuadamente el riesgo operativo es necesario que agrupen sus procesos por líneas de negocio, de acuerdo con una metodología establecida de manera formal y por escrito, para lo cual deberán observar los siguientes lineamientos:

7.1 Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos le corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar; y,

7.2 Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o

proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo.

ARTÍCULO 8.- Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

Los tipos de eventos son los siguientes:

8.1 Fraude interno;

8.2 Fraude externo;

8.3 Prácticas laborales y seguridad del ambiente de trabajo;

8.4 Prácticas relacionadas con los clientes, los productos y el negocio;

8.5 Daños a los activos físicos;

8.6 Interrupción del negocio por fallas en la tecnología de información; y,

8.7 Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

En el anexo No. 1 se incluyen algunos casos de eventos de riesgo operativo, agrupados por tipo de evento, fallas o insuficiencias que podrían presentarse en las instituciones controladas y su relación con los factores de riesgo operativo.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

ARTICULO 9.- Dentro del proceso de identificación al que se refiere el artículo anterior, las instituciones deben adicionalmente determinar de manera puntual las fallas o insuficiencias de orden legal, de tal manera que les proporcione una visión clara sobre su exposición al riesgo legal, debiendo tener como referencia para el efecto los tipos de evento de riesgo operativo indicados en dicho artículo.

Las fallas o insuficiencias de orden legal deben ser establecidas por las instituciones de acuerdo con su propia percepción y perfil de riesgos, pero deben enfocar por lo menos los siguientes campos: actos societarios; gestión de crédito; operaciones del giro financiero; actividades complementarias no financieras; y, cumplimiento legal y normativo, entendiéndolos dentro de las siguientes conceptualizaciones:

9.1 **Actos societarios**.- Son todos aquellos procesos jurídicos que debe realizar la institución en orden a ejecutar y perfeccionar las decisiones de la junta general de accionistas o asamblea general de socios o representantes, según sea del caso, y del directorio o cuerpo colegiado que haga sus veces, necesarios para el desenvolvimiento societario de la institución del sistema financiero, atenta su naturaleza jurídica;

9.2 **Gestión de crédito**.- Es el conjunto de actividades que debe ejecutar la institución del sistema financiero relacionadas con el otorgamiento de operaciones crediticias. Se inicia con la recepción de la solicitud de crédito y termina con la recuperación del valor prestado, sus intereses y comisiones. Incluye la gestión de recuperación de cartera tanto judicial como extrajudicial, la misma que debe proseguir aún cuando la operación crediticia hubiere sido castigada;

9.3 **Operaciones del giro financiero**.- Es el conjunto de actividades o procesos que realiza la institución del sistema financiero para la ejecución de operaciones propias del giro financiero, distintas a la gestión de crédito;

9.4 **Actividades complementarias de las operaciones del giro financiero**.- Es el conjunto de actividades o procesos que debe ejecutar la institución del sistema financiero que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social; y,

9.5 **Cumplimiento legal y normativo.-** Es el proceso mediante el cual la institución del sistema financiero controla que sus actividades y sus operaciones se ajusten a las disposiciones legales y normativas vigentes, así como la capacidad de adecuarse rápida y efectivamente a nuevas disposiciones legales y normativas. (artículo incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 10.- Una vez identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos.

La identificación antes indicada permitirá al directorio u organismo que haga sus veces y a la alta gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 11.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que adicionalmente las instituciones controladas conformen bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones controladas consideren necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo. (artículo renumerado y reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 12.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las instituciones controladas cuenten con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 13.- El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente.

La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 14.- Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Los reportes deberán contener al menos lo siguiente:

14.1 Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificados por líneas de negocio;

14.2 Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,

14.3 Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 15.- Las instituciones controladas 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. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Las instituciones controladas deberán establecer un proceso de administración de la continuidad de los negocios, que comprenda los siguientes aspectos claves:

15.1 Definición de una estrategia de continuidad de los negocios en línea con los objetivos institucionales;

15.2 Identificación de los procesos críticos del negocio, aún en los provistos por terceros;

15.3 Identificación de los riesgos por fallas en la tecnología de información;

15.4 Análisis que identifique los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan;

15.5 Evaluación de los riesgos para determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros;

15.6 Elaboración del plan de continuidad del negocio para someterlo a la aprobación del directorio u organismo que haga sus veces;

15.7 Realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios; y,

15.8 Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos.

ARTÍCULO 16.- Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las operaciones. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Los planes de contingencia y de continuidad deberán incluir, al menos, lo siguiente:

16.1 Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente;

16.2 Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución;

16.3 Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente;

16.4 Cronograma y procedimientos de prueba y mantenimiento del plan; y,

16.5 Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 17.- Las responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, el directorio u organismo que haga sus veces tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

17.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;

17.2 Aprobar las disposiciones relativas a los procesos establecidos en el numeral 4.1 del artículo 4;

17.3 Aprobar las políticas, procesos y procedimientos para la administración del capital humano conforme con los lineamientos establecidos en el numeral 4.2 del artículo 4;

17.4 Aprobar las políticas y procedimientos de tecnología de información establecidos en el numeral 4.3 del artículo 4; y,

17.5 Aprobar los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV de este capítulo.

ARTÍCULO 18.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, el comité de administración integral de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

18.1 Evaluar y proponer al directorio u organismo que haga sus veces las políticas y el proceso de administración del riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;

18.2 Evaluar las políticas y procedimientos de procesos, personas y tecnología de información y someterlas a aprobación del directorio u organismo que haga sus veces;

18.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;

18.4 Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV del este capítulo; asegurar la aplicabilidad; y, cumplimiento de los mismos; y,

18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

ARTICULO 19.- Las funciones y responsabilidades de la unidad de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

19.1 Diseñar las políticas y el proceso de administración del riesgo operativo;

19.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;

19.3 Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de información, especialmente aquellas relacionadas con la seguridad de la información; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

19.4 Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como

proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio; y, (reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

19.5 Analizar, monitorear y evaluar los procedimientos de orden legal de la institución; y, en coordinación con las áreas legales, emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

SECCIÓN VI.- DISPOSICIONES GENERALES

ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidas las integrantes de un grupo financiero, las instituciones controladas deberán observar lo siguiente: (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

20.1 Contar con políticas, procesos y procedimientos efectivos que aseguren una adecuada selección y calificación de los proveedores, tales como:

20.1.1 Evaluación de la experiencia pertinente;

20.1.2 Desempeño de los proveedores en relación con los competidores;

20.1.3 Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;

20.1.4 Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;

20.1.5 Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;

20.1.6 Capacidad logística del proveedor incluyendo las instalaciones y recursos; y,

20.1.7 La reputación comercial del proveedor en la sociedad.

20.2 Contratos debidamente suscritos y legalizados que contengan cláusulas que detallen, entre otros, los niveles mínimos de servicio acordado; las penalizaciones por incumplimiento; y, que prevean facilidades para la revisión y seguimiento del servicio prestado, ya sea, por la unidad de auditoría interna u otra área que la entidad designe, así como, por parte de los auditores externos o de la Superintendencia de Bancos y Seguros; y,

20.3 Contar con proveedores alternos que tengan la capacidad de prestar el servicio.

ARTÍCULO 21.- El manual que contempla el esquema de administración integral de riesgos, de que trata el artículo 15 del capítulo I "De la gestión integral y control de riesgos, incluirá la administración del riesgo operativo. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 22.- La Superintendencia de Bancos y Seguros podrá disponer la adopción de medidas adicionales a las previstas en el presente capítulo, con el propósito de atenuar la exposición al riesgo operativo que enfrenten las instituciones controladas. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, la Superintendencia de Bancos y Seguros podrá requerir a las instituciones controladas, la información que considere necesaria para una adecuada supervisión del riesgo operativo.

ARTÍCULO 23.- En caso de incumplimiento de las disposiciones contenidas en este capítulo, la Superintendencia de Bancos y Seguros aplicará las sanciones correspondientes de conformidad con lo establecido en el capítulo I "Normas para la aplicación de sanciones pecuniarias", del título XVI. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTICULO 24.- Los casos de duda y los no contemplados en el presente capítulo, serán resueltos por Junta Bancaria o el Superintendente de Bancos y Seguros, según el caso. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

SECCIÓN VII.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las instituciones controladas presentarán a la Superintendencia de Bancos y Seguros, hasta el 30 de abril del 2006, su diagnóstico y el proyecto de implementación de las disposiciones contenidas en este capítulo, para una administración adecuada del riesgo operativo. El proyecto, debidamente aprobado por el directorio u organismo que haga sus veces, incluirá un cronograma detallado de las actividades que las instituciones controladas realizarán para su cumplimiento, señalando el responsable de cada una de ellas.

Para el caso de las cooperativas de ahorro y crédito que realizan intermediación financiera con el público, el plazo para la presentación del diagnóstico y proyecto de implementación será hasta el 31 de octubre del 2006.

SEGUNDA.- La implementación de las disposiciones previstas en este capítulo no podrá exceder de los siguientes plazos:

1.1 Para grupos financieros; y, para los bancos o sociedades financieras que no forman parte de un grupo financiero, las compañías de arrendamiento mercantil, las compañías emisoras y administradoras de tarjetas de crédito, las corporaciones de desarrollo de mercado secundario de hipotecas, las instituciones financieras públicas, hasta el 31 de octubre del 2008; y,

1.2 Para las cooperativas de ahorro y crédito que realizan intermediación con el público y las asociaciones mutualistas de ahorro y crédito para la vivienda, hasta el 31 de octubre del 2009. Esta fecha podrá ser modificada por el Superintendente de Bancos y Seguros, considerando el tamaño de la institución, la estructura organizacional, la cobertura geográfica y la complejidad de sus operaciones.

TERCERA.- El cumplimiento de las disposiciones constantes en el presente capítulo por parte de las instituciones del sistema financiero, deberá realizarse dentro de los plazos previstos en la disposición transitoria segunda, para cuyo efecto deberán ajustar sus planes de implementación de la norma de gestión de riesgo operativo, remitidos al organismo de control. (incluida con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ANEXO No.1

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO

LINEAS DE NEGOCIO:

TIPOS DE EVENTOS	FALLAS O INSUFICIENCIAS	FACTORES DE RIESGO DE OPERATIVO	NUMERO DE VECES (FRECUENCIA)	EFECTO CUANTITATIVO PERDIDA PRODUCIDA
FRAUDE INTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Operaciones no reveladas adecuadamente	Mal diseño de proceso	Procesos		
Operaciones no registradas intencionalmente	Inadecuada selección de personal	Personas		
Inadecuada utilización de información confidencial	Ausencia de control en los perfiles de usuario	Tecnología de Información		
Apropiación indebida de activos	Inadecuada segregación de funciones	Personas		
Falsificación	Inexistencia de controles	Procesos		
Destrucción maliciosa de activos	Inadecuadas medidas de seguridad	Procesos		
Evasión de impuestos	Falta de ética	Personas		
Robo	Inadecuada segregación de funciones	Personas		
FRAUDE EXTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Robo	Falta de seguridades físicas	Procesos		
Emisión de cheques sin fondos	Inadecuada capacitación del Personal	Personas		
Perjuicios por intrusión o ataque de terceros	Falta de seguridades en la teconología de información para prevenir ataques de terceros	Tecnología de Información		
Falsificación	Falta de seguridades de la tecnología de información	Tecnología de Información		
PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Reclamos por compensación e indemnización al personal	Inadecuada contratación del personal	Procesos		
Violación de las normas de salud o seguridad	Falta de difusión y comunicación de políticas	Personas		
Todo tipo de discriminación	Inadecuada política de administración de personal	Personas		
PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Mal manejo de la información confidencial de clientes	Falta de defininición de políticas y procedimientos	Procesos		
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación	Falta de defininición de políticas	Personas		
Actividades no autorizadas	Incursión en nuevas actividades sin considerar riesgos	Procesos		
Abuso de información privilegiada a favor de la institución	Falta de ética	Personas		
DAÑOS A LOS ACTIVOS FÍSICOS PROVOCADOS POR				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Terrorismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Vandalismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Pérdidas por desastres naturales	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Fallas en el software	Deficiencia en el proceso de desarrollo y/o implantación	Tecnología de Información		
Fallas en el hadware	Falta de previsión de la capacidad de los recursos para el volumen de operaciones. Falta de mantenimiento preventivo de los servidores centrales	Tecnología de Información		
Problemas de telecomunicación	Caída en los enlaces de telecomunicaciones	Tecnología de Información		
Cortes en los servicios públicos	Falta de planes de contingencia	Eventos externos		
DEFICIENCIAS EN LA EJECUCIÓN DE PROCESOS, EN EL PROCESAMIENTO DE OPERACIONES Y EN LAS RELACIONES CON PROVEEDORES Y OTROS EXTERNOS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Errores en el ingreso de los datos	Falta de controles de ingreso de datos en las aplicaciones	Tecnología de Información		
Falla en la administración de colaterales	Inadecuada segregación de funciones	Procesos		
Documentación legal incompleta	Falta de verificación del área legal	Procesos		
Acceso no aprobado a las cuentas de clientes	Proceso no definido	Procesos		
Disputa con los proveedores	Deficiencias en la contratación	Procesos		
Incumplimiento en la entrega de la información hacia terceros	Falta de controles en el proceso de envio de información	Procesos		

NOTAS:

1.- En el presente Anexo constan ejemplos de eventos agrupados por tipo, los cuales consideran los lineamientos establecidos por el Comité de Basilea

2.- Los eventos que se produjeren que no esté alineados a los tipos de eventos especificados en este Anexo, deberán constar bajo la denominación "información no alineada, concepto bajo el cual constarán únicamente por excepción.

3.- Frecuencia, se refiere al número de veces que se repite cada evento