Resolución SMV Nº 027-2016-SMV/01

Lima, 15 de septiembre de 2016

VISTOS:

El Expediente N° 2016030999, los Informes Conjuntos N°s 620 y 712-2016-SMV/06/12/13 del 10 de agosto y 12 de septiembre de 2016, respectivamente, emitidos por la Oficina de Asesoría Jurídica, la Superintendencia Adjunta de Investigación y Desarrollo y la Superintendencia Adjunta de Riesgos, así como, el proyecto de Reglamento de Gestión del Riesgo Operacional (en adelante, el PROYECTO);

CONSIDERANDO:

Que, conforme a lo dispuesto en el literal a) del artículo 1° del Texto Único Concordado de la Ley Orgánica de la Superintendencia del Mercado de Valores - SMV, aprobado mediante Decreto Ley N° 26126 y modificado por la Ley de Fortalecimiento de la Supervisión del Mercado de Valores, Ley N° 29782, la Superintendencia del Mercado de Valores - SMV está facultada para dictar las normas legales que regulen materias del mercado de valores;

Que, de acuerdo con el literal b) del artículo 5° de la precitada norma, el Directorio de la SMV tiene por atribución aprobar la normativa del mercado de valores, así como aquella a que deben sujetarse las personas naturales y jurídicas sometidas a su supervisión;

Que, el artículo 16-B de la Ley del Mercado de Valores - LMV, aprobada por Decreto Legislativo N° 861, establece que las personas jurídicas autorizadas por la SMV deberán constituir un Sistema de Administración de Riesgos de acuerdo con las normas que establezca la SMV;

Que, el 20 de diciembre de 2015, se publicó en el Diario Oficial El Peruano el Reglamento de Gestión Integral de Riesgos aprobado mediante Resolución SMV N° 037-2015-SMV/01, el cual establece criterios mínimos para que las Entidades a las que la SMV otorga autorización de funcionamiento desarrollen de manera adecuada su gestión integral de riesgos;

Que, bajo el referido marco, es necesario aprobar disposiciones complementarias a efectos de regular con detalle y de manera independiente diversos aspectos asociados con la gestión de los riesgos inherentes a los que se encuentran expuestas dichas Entidades, tales como riesgo operacional, de mercado, crédito, liquidez, entre otros;

Que, se requiere establecer lineamientos, criterios y parámetros generales que la Entidad debe observar en el diseño, desarrollo y aplicación de su gestión del riesgo operacional, de acuerdo con el tamaño, volumen de transacciones y complejidad de las operaciones que realizan; a modo de garantizar el correcto desarrollo de las operaciones por parte de las entidades supervisadas por la SMV, teniendo presente que la administración de este riesgo se está convirtiendo en una característica importante en la gestión integral de riesgos de los mercados financieros modernos;

Que, el uso extendido de soluciones y plataformas tecnológicas en los mercados de valores ha permitido ampliar la capacidad, velocidad y precisión de diversas operaciones que se pueden realizar en los mercados globales, pero, a su vez ,plantean diversos riesgos, por lo que resulta necesario, como parte de

una adecuada gestión del riesgo operacional, establecer para las Entidades que la SMV otorga autorización de funcionamiento, lineamientos para el desarrollo de sus sistemas de gestión de seguridad de información y gestión de continuidad del negocio, para que estos sean desarrollados de manera adecuada;

Que, el PROYECTO fue difundido en el Diario Oficial El Peruano y puesto en consulta ciudadana en el Portal del Mercado de Valores de la SMV por quince (15) días calendario, conforme lo dispuso la Resolución SMV Nº 022-2016-SMV/01, publicada el 17 de agosto de 2016; y,

Estando a lo dispuesto por el literal a) del artículo 1°, el literal b) del artículo 5 del Texto Único Concordado de la Ley Orgánica de la Superintendencia del Mercado de Valores – SMV, aprobado por el Decreto Ley N° 26126 y sus modificatorias, el artículo 7 de la Ley del Mercado de Valores, Decreto Legislativo N° 861 y sus modificatorias, así como a lo acordado por el Directorio en su sesión del 14 de septiembre de 2016;

SE RESUELVE:

Artículo 1°.- Aprobar el Reglamento de Gestión del Riesgo Operacional, el mismo que consta de dieciocho (18) artículos, tres (3) disposiciones complementarias finales, dos (2) disposiciones complementarias transitorias y un (01) Anexo, los que a continuación se detallan:

REGLAMENTO DE GESTIÓN DEL RIESGO OPERACIONAL

TÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.- AMBITO DE APLICACIÓN

Las disposiciones del presente Reglamento son aplicables a las Entidades a las que la Superintendencia de Mercado de Valores - SMV otorga autorización de funcionamiento.

ARTÍCULO 2.- DEFINICIONES

Para la aplicación del presente Reglamento se considerarán las siguientes definiciones:

a) Confidencialidad: La información debe mantenerse en reserva, pudiendo ser accesible únicamente a aquellos usuarios que se encuentren debidamente autorizados, capacitados y supervisados.

b) Disponibilidad: La información debe ser accesible a los usuarios autorizados cuando sea requerida.

c) Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d) Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

e) Integridad: La información debe ser completa, exacta y veraz.

f) Periodo máximo tolerable de interrupción: Es el periodo, determinado por la Entidad, luego del cual la viabilidad de la Entidad sería afectada seriamente, si un producto o servicio en particular no es reanudado.

g) Proveedor principal: Es aquel que, de interrumpir sus operaciones afectaría de manera importante la continuidad del negocio de la Entidad. Es, además, aquel con el que se tiene una subcontratación significativa, que incluye a los proveedores de servicios públicos como: telecomunicaciones, energía, entre otros.

h) Reglamento: El Reglamento de Gestión del Riego Operacional.

i) Reglamento de Gestión Integral de Riesgos: El Reglamento de Gestión Integral de Riesgos, aprobado por Resolución SMV N° 037-2015-SMV/01.

j) Subcontratación significativa: Es aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo a la Entidad, al afectar sus ingresos, solvencia o continuidad del negocio de manera importante.

k) Tiempo objetivo de recuperación: Es el tiempo establecido por la Entidad para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

Asimismo, serán de aplicación las definiciones contenidas en el Reglamento de Gestión Integral de Riesgos.

En adelante, los términos antes mencionados podrán emplearse en forma singular o plural, sin que ello implique un cambio en su significado. Salvo mención en contrario, la referencia a artículos determinados debe entenderse efectuada a los correspondientes del presente Reglamento.

ARTÍCULO 3.- FINALIDAD

El presente Reglamento establece lineamientos, criterios y parámetros generales que la Entidad debe observar en el diseño, desarrollo y aplicación de su gestión del riesgo operacional, de acuerdo con el tamaño, volumen de transacciones y complejidad de las operaciones que realizan.

Como parte de una adecuada gestión del riesgo operacional, las Entidades deben implementar un sistema de gestión de seguridad de la información y gestión de la continuidad del negocio.

TÍTULO II

GESTIÓN DEL RIESGO OPERACIONAL

ARTÍCULO 4.- RIESGO OPERACIONAL

El riesgo operacional es la posibilidad de ocurrencia de pérdidas originadas por procesos inadecuados, errores del personal, fallas tecnológicas o por eventos externos. El riesgo operacional incluye el riesgo legal.

No constituye riesgo operacional el riesgo estratégico y el de reputación.

ARTÍCULO 5.- FACTORES DE RIESGO OPERACIONAL

La Entidad debe considerar los siguientes factores de riesgo operacional:

a) **Personal:** La Entidad debe gestionar los riesgos asociados a su personal como: la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo,

paralizaciones, apropiación de información sensible, alta rotación, concentración de funciones, entre otros.

b) **Procesos internos:** La Entidad debe gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios. Estos riesgos están relacionados con el diseño inapropiado de los procesos, políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia del desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

c) **Tecnología:** La Entidad debe 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, errores en el diseño e implementación de los sistemas, problemas de calidad de la información y lograr que la información sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

d) **Eventos externos:** La Entidad debe gestionar los riesgos de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la entidad que pueden alterar el desarrollo de sus actividades. Se deben tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos.

ARTÍCULO 6.- EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Las Entidades deben identificar los eventos de pérdida por riesgo operacional, pudiendo agruparlos de la siguiente manera:

a) **Fraude interno**.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas internas en las que se encuentran implicados empleados de la Entidad, y que tiene como fin obtener un beneficio ilícito.

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

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

d) **Prácticas relacionadas con los clientes, los productos y el negocio**.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes o generadas por la deficiencia en el producto o servicio.

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

f) **Interrupción del negocio por fallas en la tecnología de información**.- Pérdidas derivadas de interrupciones en el negocio y de fallas en los sistemas.

g) **Deficiencia en la 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, tales como proveedores, clientes, entre otros.

En el Anexo se presentan algunos ejemplos de tipos de eventos de pérdida por riesgo operacional de acuerdo con la agrupación establecida en el presente artículo.

ARTÍCULO 7.- METODOLOGÍA

La metodología que elabore la Entidad para la gestión del riesgo operacional, la que comprende la gestión de la seguridad de la información y gestión de la continuidad del negocio, deberá considerar los elementos señalados en el artículo 5 del Reglamento de Gestión Integral de Riesgos. Asimismo, deberá cumplir con lo siguiente:

a) La metodología debe ser aprobada por el Directorio u órgano equivalente, e implementada en toda la Entidad en forma consistente.

b) La Entidad debe asignar recursos suficientes para aplicar su metodología en sus operaciones y en los procesos de control y de apoyo.

c) La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la Entidad.

d) La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.

e) Debe establecerse procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional.

ARTÍCULO 8.- BASE DE DATOS DE EVENTOS DE PÉRDIDA

La gestión del riesgo operacional constituye un proceso continuo y permanente, siendo necesario que la Entidad elabore bases de datos para cumplir, al menos, los siguientes criterios:

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

b) El monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos será de S/ 3 000.00 (tres mil y 00/100 soles). No obstante, la Entidad podrá establecer un monto mínimo inferior al indicado en función del tamaño, volumen de transacciones y complejidad de sus operaciones.

   El Superintendente del Mercado de Valores podrá modificar el monto señalado en el párrafo anterior y/o establecer montos diferenciados.

c) Registrar la siguiente información referida al evento y a las pérdidas asociadas:

   - Código de identificación del evento (asignado por la entidad, registro sistemático).
   - Tipo de evento de pérdida (según tipos de eventos señalados en el Anexo del presente Reglamento).
   - Operaciones
   - Descripción del evento.
   - Proceso o área a la que pertenece el evento.
   - Fecha de ocurrencia o de inicio del evento.
   - 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 y tipo de cambio y tipo de cobertura aplicada.
   - Monto total recuperado, moneda y tipo de cambio.

- Cuenta(s) contable(s) asociadas, de ser el caso.

En el caso de eventos con pérdidas múltiples, la Entidad puede registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

La Entidad podrá registrar información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

La Entidad establecerá criterios objetivos para asignar los eventos de pérdida a los tipos de eventos señalados en el Anexo, así como a las operaciones de la Entidad, los que deberá documentar.

La Base de Datos de Eventos de Pérdida estará a disposición de la SMV, a su requerimiento para los fines de supervisión y control.

TÍTULO III

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 9.- SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Entidad debe implementar un sistema de gestión de la seguridad de la información, orientado a garantizar como mínimo la integridad, confidencialidad y disponibilidad de la información mediante la adecuada combinación de políticas, procedimientos, controles, estructura organizacional y herramientas informáticas especializadas.

Para ello, deberá como mínimo realizar las siguientes actividades:

a) Definición de una política de seguridad de información aprobada por el Directorio u órgano equivalente.

b) Definición e implementación de una metodología de gestión de seguridad de la información, conforme a lo establecido en el artículo 7 del Reglamento, y que guarde consistencia con la gestión integral de riesgos de la Entidad.

c) Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la Entidad, para la correcta gestión de la seguridad de la información, así como mantener una suficiente evidencia de auditoría.

ARTÍCULO 10.- FUNCIÓN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Entidad debe contar con una estructura organizacional que le permita implementar y mantener el sistema de gestión de la seguridad de información, para lo cual deberá:

a) Asegurar el cumplimiento de la política, los procedimientos y la metodología de seguridad de información elaborada por la Entidad, incluyendo además la asignación de roles y responsabilidades;

b) Coordinar y monitorear la implementación de los controles de seguridad de información;

c) Desarrollar actividades de concientización y entrenamiento en seguridad de información, así como la operatividad para informar sobre incidentes;

d) Evaluar de forma continua los eventos asociados a una posible falla en la política de seguridad, en los controles o una situación previamente desconocida relevante para la seguridad y recomendar acciones apropiadas;

e) Desarrollar planes de comunicación para determinar responsabilidades en la toma de decisiones, así como las políticas y procedimientos para divulgar potenciales vulnerabilidades;

f) Dirigir y promover que el personal contribuya con la efectividad del sistema de gestión de seguridad de la información; y,

g) Reportar al Directorio u órgano equivalente o al Comité de Riesgos, según su organización, sobre el desempeño del sistema de gestión de la seguridad de la información con la periodicidad que determine la Entidad, la que no podrá ser mayor a un año.

La Entidad deberá realizar la función de gestión de la seguridad de la información, de acuerdo con el tamaño, volumen de transacciones y complejidad de las operaciones que realizan.

ARTÍCULO 11.- CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

La Entidad deberá considerar, de acuerdo con su tamaño, volumen de transacciones y complejidad de sus operaciones, la implementación de los controles generales, que se indican a continuación:

1. **Seguridad lógica:**
   a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
   b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
   c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
   d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
   e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
   f) Controles especiales sobre usuarios remotos y computación móvil.

2. **Seguridad de personal:**
   a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
   b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.
   c) Concientización y entrenamiento.
   d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad de la información.
   e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

3. **Seguridad física y ambiental:**
   a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la Entidad.
   b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

4. **Inventario de activos y clasificación de la información:**
   a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
   b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la Entidad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5. **Administración de las operaciones y comunicaciones:**
   a) Procedimientos documentados para la operación de los sistemas.
   b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
   c) Separación de funciones para reducir el riesgo de error o fraude.
   d) Separación de los ambientes de desarrollo, pruebas y producción.
   e) Monitoreo del servicio brindado por terceros.
   f) Administración de la capacidad de procesamiento.
   g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
   h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
   i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
   j) Seguridad sobre canales electrónicos.
   k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

6. **Adquisición, desarrollo y mantenimiento de sistemas informáticos:**
   Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

   a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
   b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
   c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
   d) Controlar el acceso a las librerías de programas fuente.
   e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
   f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la Entidad.

7. **Procedimientos de respaldo:**
   a) Procedimientos de respaldos regulares y validados con la periodicidad que determine la Entidad. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la Entidad.
   b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

8. **Gestión de incidentes de seguridad de información:**

   Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, la Entidad deberá considerar los siguientes aspectos:

   a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.

   b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

9. **Cumplimiento normativo:**

   La Entidad deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

10. **Privacidad de la información:**

    La Entidad debe adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

ARTÍCULO 12.- AUDITORÍA EXTERNA

La Auditoría Externa deberá evaluar de manera independiente el cumplimiento de los procedimientos utilizados para la Gestión de Seguridad de la Información realizada por la Entidad.

TITULO IV

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

ARTÍCULO 13.- SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La Entidad debe implementar un sistema de gestión de la continuidad del negocio mediante el conjunto detallado de acciones que describan los procedimientos, los sistemas y los recursos necesarios para retornar y continuar las operaciones en caso de interrupción. Tendrá como objetivo principal brindar respuestas efectivas para que la operatividad del negocio continúe de una manera razonable, ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en sus operaciones.

Para ello deberá como mínimo realizar las siguientes actividades:

a) Definición de una política de continuidad del negocio aprobada por el Directorio u órgano equivalente.
b) Definición e implementación de una metodología de gestión de continuidad del negocio, conforme a lo establecido en el artículo 7 del Reglamento, y que guarde consistencia con la gestión integral de riesgos de la Entidad.
c) Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la Entidad para la correcta gestión de la continuidad del negocio, así como mantener una suficiente evidencia de auditoría.

ARTÍCULO 14.- FUNCIÓN DE CONTINUIDAD DEL NEGOCIO

La Entidad deberá contar con una estructura organizacional que le permita cumplir adecuadamente la función de continuidad del negocio, la cual tendrá a su cargo las siguientes responsabilidades:

a) Proponer las políticas, procedimientos y metodología apropiados para la gestión de la continuidad del negocio en la Entidad, incluyendo la asignación de roles y responsabilidades;

b) Desarrollar actividades de concientización y entrenamiento de continuidad del negocio, así como la operatividad para informar sobre incidentes;

c) Evaluar los incidentes de continuidad del negocio de forma continua y recomendar acciones apropiadas;

d) Desarrollar planes de comunicación para determinar responsabilidades en la toma de decisiones, así como las políticas y procedimientos para divulgar potenciales vulnerabilidades; y,

e) Reportar al Directorio u órgano equivalente o al Comité de Riesgos, según su organización, sobre el desempeño del sistema de gestión de la continuidad del negocio para una oportuna toma de decisiones con la periodicidad que determine la Entidad, la que no podrá ser mayor a un año.

La Entidad deberá realizar la función de gestión de continuidad del negocio de acuerdo con el tamaño, volumen de transacciones y complejidad de las operaciones que realice.

ARTÍCULO 15.- FASES DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La Entidad deberá desarrollar, de acuerdo con su tamaño, volumen de transacciones y complejidad de sus operaciones, las siguientes fases como parte de la gestión de la continuidad del negocio:

1. Entendimiento de la organización y el contexto

La Entidad debe conocer y documentar sus objetivos y metas; identificar los principales procesos, productos, servicios, proveedores y todas las partes interesadas, así como las actividades, recursos requeridos y los requerimientos legales y/o regulatorios que son de su aplicación. Asimismo, debe conocer las relaciones entre las políticas de continuidad del negocio y los objetivos de la organización y otras políticas incluyendo la estrategia de gestión integral de riesgos y el apetito por riesgo de la organización.

La Entidad debe conocer, además, los factores internos y externos que crean incertidumbre y evaluar los riesgos que podrían causar la interrupción de dichas actividades, así como el impacto que podría tener dicha interrupción.

Las actividades mínimas a desarrollar durante esta fase son las siguientes:

a) **Análisis de impacto:**

Es el proceso formal de evaluación del impacto (financiero, jurídico y regulatorio) que tendría una interrupción de los procesos que soportan las principales operaciones de la Entidad y determinar las prioridades de continuidad y objetivos de recuperación. Para ello, deben considerarse aspectos como: la identificación de actividades que soportan la provisión de servicios, daños a la viabilidad financiera de la empresa, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. De acuerdo con ello debe establecerse el período máximo tolerable de

interrupción, así como los objetivos de recuperación por cada uno de estos procesos.

Debe incluir, además, la identificación y evaluación de los riesgos relacionados con los procesos operativos y servicios de procesamiento y transmisión de datos contratados con proveedores de procesos identificados como críticos.

El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.

b) **Evaluación de riesgos**:

Es el proceso mediante el cual sistemáticamente se identifica, analiza y evalúan los riesgos que podrían causar una interrupción del negocio. Para ello, deberá aplicarse la metodología aprobada que debe ser consistente con aquella que se utilice para la evaluación de los demás riesgos que enfrenta la Entidad. Además, debe definir y priorizar las actividades y procesos, sistemas, información, personal, activos, proveedores y otros recursos que soporten sus actividades y que requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos. Asimismo, debe identificar los tratamientos correspondientes para los objetivos de continuidad del negocio de acuerdo con el apetito al riesgo de la organización, conservando la información documentada de los resultados del proceso de evaluación de la continuidad del negocio.

c) **Requerimientos legales y regulatorios**:

La organización debe implementar y mantener un procedimiento para identificar, tener acceso y evaluar los requerimientos legales y regulatorios que le sean aplicables relativos a la continuidad de sus operaciones, así como las partes involucradas y asegurarse que estos requerimientos sean tomados en cuenta en la gestión de la continuidad del negocio.

2. Planificación

a) **Acciones para abordar los riesgos y oportunidades**

En esta etapa, deberán considerar lo abarcado en el numeral anterior y el entendimiento de las necesidades y expectativas de las partes interesadas para así determinar los riesgos y oportunidades que necesitan ser cubiertos. Para ello, la Entidad debe planificar las acciones que tomará para abordar sus riesgos y oportunidades, así como la manera en cómo se integrarán e implementarán las acciones en los procesos de gestión de la continuidad del negocio y la evaluación de la eficacia de estas acciones.

b) **Objetivos de continuidad del negocio y planes para lograrlos**

La Entidad debe asegurarse que los objetivos de la continuidad del negocio, se cumplan, sean medibles y consistentes con sus políticas, así como con las exigencias legales y regulatorias aplicables y los resultados de la evaluación de riesgos y su tratamiento.

Para lograr sus objetivos la Entidad deberá determinar a los responsables, los planes de acción, los recursos que requerirán, cuándo estará completado y cómo evaluará los resultados.

3. Soporte

a) **Recursos:** La Entidad debe determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de la continuidad del negocio.

b) **Competencia:** Es necesario determinar las competencias necesarias de las personas que trabajan en la Entidad que inciden el desempeño del sistema de seguridad de la información, asegurando su competencia y, cuando corresponda, tomar acciones para adquirir capacidades necesarias y evaluar la efectividad de las acciones tomadas, manteniendo la información documentada como evidencia de dichas competencias.

c) **Sensibilización:** El personal que trabaja en la Entidad debe estar al tanto de la política de gestión de continuidad del negocio, la contribución de la eficacia del sistema de gestión de continuidad del negocio, las implicaciones de no cumplir con los requerimientos de la gestión de continuidad del negocio y el rol del personal durante un evento de interrupción de operaciones.

d) **Comunicación:** La Entidad deberá determinar la necesidad de la comunicación interna y externa sobre el sistema de gestión de continuidad del negocio hacia las partes interesadas y empleados dentro de la organización, asegurando la disponibilidad de los medios de comunicación durante un evento de interrupción de operaciones.

4. Información documentada

El sistema de gestión de la continuidad del negocio de la Entidad debe incluir la información documentada de los aspectos requeridos en el presente Reglamento y toda aquella información que considere pertinente para la gestión de la continuidad del negocio y debe contar con controles para asegurar su disponibilidad y uso apropiado , así como estar debidamente protegida.

5. Determinación y selección de la estrategia de continuidad

Las estrategias de continuidad permitirán mantener las actividades y procesos del negocio luego de ocurrido un evento de interrupción de operaciones basadas en el análisis del impacto del negocio, la evaluación de riesgos, requerimientos legales y regulatorios aplicables y acorde con su nivel de apetito por el riesgo, para lo cual deben desarrollarse, como mínimo, las siguientes actividades:

a) Evaluación y selección de estrategias de continuidad por proceso: La Entidad debe destinar los recursos requeridos para seleccionar y priorizar las estrategias que permitirán mantener la continuidad de los procesos que soportan los principales productos y servicios de la Entidad, dentro del tiempo objetivo de recuperación, definido para cada proceso. Las estrategias de continuidad deben tomar en cuenta los siguientes aspectos no limitativos, según sea aplicable para cada proceso:
   - Seguridad del personal.
   - Habilidades y conocimientos asociados al proceso.
   - Instalaciones alternas de trabajo.
   - Infraestructura alterna de tecnología de información que soporte el proceso.
   - Seguridad de la información.
   - Equipamiento necesario para el proceso.

b) Evaluación y selección de estrategias de servicios críticos provistos por parte de terceros: La Entidad deberá realizar evaluaciones de las capacidades de recuperación ante la caída de actividades significativas subcontratadas.

La Entidad deberá considerar medidas preventivas que permitan reducir la probabilidad de ocurrencia de daños, reducir el tiempo de recuperación y limitar el impacto hacia productos y servicios claves para la organización.

6. Desarrollo e implementación de los procedimientos de continuidad del negocio

Se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones.

Para este fin, las Entidades deberán implementar:

a) Organización para el reporte de incidentes: La Entidad deberá establecer, documentar e implementar procedimientos y una estructura de respuesta ante incidentes realizada por el personal con la responsabilidad, autoridad y competencia para gestionar el incidente y comunicar a las partes interesadas.

   En caso de ocurrencia de eventos de interrupción significativa de operaciones, esta deberá ser comunicada a la SMV al día siguiente hábil. Dicha comunicación incluirá una descripción general del evento ocurrido.

   Se entenderá como evento de interrupción significativa de operaciones lo siguiente:

   i. El menor entre cualquier evento que implique la suspensión de la atención a los clientes por un tiempo mayor al tiempo objetivo de recuperación establecido por la Entidad o cuatro (4) horas de interrupción; y/o
   ii. Todo evento que implique activar el Plan de Gestión de Crisis establecido en el presente Reglamento.

b) Protocolos de comunicación interna y externa: Deberán establecer, implementar y mantener procedimientos para detectar, monitorear, comunicar internamente, documentar y responder a las partes interesadas.

c) Plan de Gestión de Crisis: Consiste en preparar a la Entidad para enfrentar la fase aguda de un evento de interrupción de operaciones, incluso de aquellos no esperados. Debe incluir los siguientes aspectos:
   - Propósito y alcance.
   - Roles y responsabilidades.
   - Criterios de invocación y activación.
   - Responsable de su actualización.
   - Planes de acción.
   - Comunicaciones con el personal, familiares y contactos de emergencia.
   - Comunicación con los grupos de interés.
   - Establecimiento de un centro de cómputo (considerar al menos un sitio principal, y uno alterno).

d) Plan de Continuidad del Negocio: Tiene como objetivo dotar a la Entidad de la capacidad de mantener o, de ser el caso, recuperar los principales procesos de negocio dentro de los parámetros previamente establecidos. Debe documentar y considerar, como mínimo, los siguientes aspectos:

   - Propósito, alcance y objetivos.
   - Roles y responsabilidades.
   - Criterios de invocación y activación.
   - Responsable de su actualización.

- Requerimientos y procedimientos de comunicación en respuesta al incidente.
- Planes de acción para reanudar los procesos conforme a la estrategia y periodos predeterminados.
- Requerimiento de recursos.
- Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, entre otros).
- Plan de emergencia, que permita salvaguardar la integridad física del personal.
- Plan de recuperación de servicios de tecnología de información, que permita restaurar los servicios de tecnología de información dentro de los parámetros establecidos, con la posterior recuperación de las condiciones previas a su ocurrencia.

7. Pruebas y actualización

El plan de continuidad del negocio deberá ser probado cuando menos una vez al año y deberá asegurar la consistencia con sus objetivos de continuidad del negocio. A continuación se detallan las actividades mínimas que deben ser aplicadas en esta fase:

a) **Ejecución de pruebas**: Las pruebas deben ser consistentes con el alcance y objetivos de la gestión de continuidad del negocio, deberán estar basadas en escenarios adecuados y planificados con fines y objetivos definidos. Cada prueba debe tener un reporte que resuma los resultados alcanzados, recomendaciones y acciones para implementar las mejoras. Esta información deberá ser usada para mejorar los planes de continuidad del negocio en forma oportuna.

Las pruebas deben realizarse periódicamente y cuando existan cambios significativos en la organización o el ambiente en el que opera.

b) **Actualización de los planes**: La Entidad debe definir políticas, procedimientos y la oportunidad para la actualización de los planes de gestión de la continuidad del negocio, de tal manera que cualquier cambio, interno o externo, que le impacte, sea revisado en relación con la continuidad del negocio.

8. Evaluación del desempeño: monitoreo, medición, análisis y evaluación

La Entidad debe evaluar qué procesos deben ser monitoreados, medidos, analizados y evaluados periódicamente. Dichos métodos deben asegurar la validez de los resultados y mantener debidamente documentada la evidencia de los resultados.

a) **Monitoreo permanente:** Debe monitorear en qué medida son satisfactorias las políticas, los objetivos y metas de la gestión de continuidad del negocio; los procesos, procedimientos y funciones que protegen las actividades críticas; así como el cumplimiento de las disposiciones del presente Reglamento. El registro de los resultados de medición y monitoreo deben facilitar la subsecuente acción correctiva.

b) **Evaluación de los procedimientos de continuidad del negocio:** La Entidad debe evaluar el desempeño y la efectividad de su sistema de gestión de continuidad del negocio y tomar las acciones que fueran necesarias. La Entidad debe conducir evaluaciones de los procedimientos de continuidad del negocio y la capacidad para asegurar su conveniencia, adecuación y eficacia continua. Dichas evaluaciones deben ser realizadas periódicamente.

9. Revisión de la gestión:

La Entidad debe revisar la gestión de continuidad del negocio y asegurar su conveniencia, suficiencia y efectividad continua considerando la situación actual, los cambios en factores internos y externos relevantes, los comentarios sobre el desempeño de su sistema de las partes interesadas, los resultados del ejercicio de la gestión de continuidad de negocios y el estado del plan de tratamiento del riesgo; así como las oportunidades para la mejora continua. Dicha revisión debe mantenerse documentada.

La Entidad deberá mejorar constantemente la conveniencia, adecuación y eficacia de la gestión de continuidad del negocio.

ARTÍCULO 16.- CAMBIOS SIGNIFICATIVOS

La Entidad analizará el impacto que tienen los cambios significativos sobre la continuidad del negocio.

Los cambios significativos podrán considerar entre otros: cambio de la infraestructura tecnológica que soporta los principales productos y/o servicios, fusión con otra empresa, implementación de un nuevo producto, cambio de un proveedor principal, cambio de oficina principal.

TÍTULO V

OTRAS DISPOSICIONES

ARTÍCULO 17.- SUBCONTRATACIÓN

La Entidad es responsable y debe verificar que se mantengan las características de seguridad de la información y condiciones de continuidad del negocio contempladas en el presente reglamento, incluso cuando ciertas funciones o procesos puedan ser objeto de una subcontratación.

Para toda subcontratación significativa, la Entidad deberá:

a) Asegurarse de que el procesamiento y la información objeto de la subcontratación se encuentren efectivamente separados en todo momento.

b) Desarrollar y aprobar un plan de continuidad respecto a los servicios contratados. La Entidad deberá verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas. Estos planes deben estar aprobados por la Entidad y encontrarse a disposición de la SMV.

c) Contar con un acuerdo de nivel de servicio con aquellas empresas subcontratadas, asegurando que los acuerdos o políticas de gestión de seguridad de la información y continuidad de negocios de la empresa subcontratada son apropiados y garanticen el cumplimiento de las disposiciones del presente Reglamento.

El Directorio u órgano equivalente, en última instancia, es responsable de la seguridad de la información y continuidad del negocio de la Entidad, incluso si las operaciones de negocios son subcontratadas.

ARTÍCULO 18.- CONSERVACION DE INFORMACION

Las Entidades deberán conservar la información de que trata el presente Reglamento por un plazo no menor de diez (10) años.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Como parte del informe anual requerido por el Reglamento de Gestión Integral de Riesgos, aprobado mediante Resolución SMV N° 037-2015-SMV/01, la Entidad deberá incluir información sobre los principales aspectos y resultados de la gestión del riesgo operacional, gestión de la seguridad de la información y gestión de la continuidad del negocio.

Dicha obligación será exigible tratándose de Entidades que formen parte de un conglomerado financiero respecto de la información correspondiente al 2018, debiendo presentar dicha información a más tardar el 31 de marzo de 2019. En el caso de Entidades que no formen parte de un conglomerado financiero, dicha obligación será exigible respecto de la información correspondiente al ejercicio 2019, debiendo presentar dicho informe a la SMV a más tardar el 31 de marzo de 2020.

SEGUNDA.- La SMV podrá requerir a la Entidad cualquier información que considere necesaria, en el ejercicio de sus acciones de supervisión y conforme a lo previsto en el presente Reglamento.

La Entidad deberá mantener a disposición de la SMV todos los documentos a que hace mención el presente Reglamento, así como la información de auditoría interna o revisiones realizadas por la matriz en caso de ser aplicable.

TERCERA.- Para todo lo no señalado en el presente Reglamento, será de aplicación el Reglamento de Gestión Integral de Riesgos, aprobado mediante Resolución SMV N° 037-2015-SMV/01. En particular, dicho reglamento será de aplicación para definir a los órganos y unidades responsables de la implementación y cumplimiento de la gestión del riesgo operacional, seguridad de la información, continuidad del negocio, auditoría interna, subcontratación, entre otros.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

PRIMERA.- Las Entidades que a la fecha de entrada en vigencia del presente Reglamento cuenten con planes de seguridad de la información y de continuidad de negocios en cumplimiento de una disposición específica, deberán adecuar dichos planes a lo establecido en el presente Reglamento a más tardar el 31 de enero de 2018.

SEGUNDA.- Para los fines de la aplicación del presente Reglamento, la Entidad deberá observar lo siguiente:

1.1 La Entidad que no forme parte de un conglomerado financiero deberá implementar la gestión del riesgo operacional y sus componentes en los términos previstos en el presente Reglamento, a más tardar el 31 de diciembre de 2018.

1.2 La Entidad que forme parte de un conglomerado financiero, deberá implementar la gestión del riesgo operacional y sus componentes en los términos previstos en el presente Reglamento, a más tardar el 31 de enero de 2018.

ANEXO

TIPOS DE EVENTOS DE PÉRDIDA 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 incumplir regulaciones, leyes o políticas internas en las que se encuentran implicados empleados de la entidad, y que tiene como fin obtener un beneficio ilícito.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), 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 un activo indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.	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 salud o seguridad en el trabajo, el pago de reclamos por daños personales, o casos relacionados con la diversidad o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Salud y seguridad en el trabajo	Casos relacionados con las normas de salud y seguridad en el trabajo; indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Prácticas relacionadas con los clientes, los productos y el	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes o generadas por la deficiencia en el producto o	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de

negocio	servicio.		la privacidad de información sobre clientes, quebrantamiento de 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, uso de información privilegiada, lavado de activos y financiamiento del terrorismo.
		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 físicos	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.	Desastres y otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio por fallas en la tecnología de información	Pérdidas derivadas de interrupciones en el negocio y de fallas en los sistemas.	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
Deficiencia en la ejecución, entrega y gestión de	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con	Recepción, ejecución y mantenimiento de operaciones	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades,

procesos	contrapartes, tales como proveedores, clientes, entre otros.		ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el *Delivery* vs. *Payment*).
		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.
		Pérdidas derivadas del incumplimiento de la normativa	De la normativa aplicable a la Entidad. De otras normas.
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

Artículo 2°.- Derogar las siguientes disposiciones:

a) El Título III, la Segunda Disposición Complementaria Final y el Anexo del Reglamento de Gestión Integral de Riesgos, aprobado mediante Resolución SMV N° 037-2015-SMV/01.
b) Las normas emitidas por esta Superintendencia que se opongan al presente Reglamento, así como aquellas que regulen la gestión de seguridad de la

información, la gestión de la continuidad del negocio y demás componentes del riesgo operacional, con excepción de la Resolución SMV N° 037-2015-SMV/01, la que se aplicará de manera supletoria en dichas materias.

Artículo 3°.- Modificar el inciso h) del artículo 6° del Reglamento de Gestión Integral de Riesgos, aprobado mediante Resolución SMV N° 037-2015-SMV/01, conforme al siguiente texto:

*"**ARTÍCULO 6.- MANUAL DE GESTIÓN INTEGRAL DE RIESGOS***

La Entidad debe contar con un Manual de Gestión Integral de Riesgos, que contendrá, como mínimo, además de los elementos señalados en el artículo precedente, los siguientes:

(…)

h) La metodología de Gestión de Riesgo Operacional.

(…)"

Artículo 4°.- La presente resolución entrará en vigencia el 1° de enero de 2018, salvo lo señalado en el inciso a) del artículo 2° y el artículo 3°, los cuales entrarán en vigencia al día siguiente de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 5°.- Publicar la presente resolución en el Diario Oficial El Peruano y en el Portal del Mercado de Valores de la Superintendencia del Mercado de Valores (www.smv.gob.pe).

Regístrese, comuníquese y publíquese.

Firmado por: ROCCA CARBAJAL Lilian Del Carmen (FAU2
Razón: RSMV 027-2016

Lilian Rocca Carbajal
Superintendente del Mercado de Valores

Firmado por: GIL VASQUEZ Liliana (FAU2013
Razón:

Firmado por: FALEN LARA Wilson Paul (FAU20131016396)
Razón:

Firmado por: RIVERO ZEVALLOS Carlos Fabian
Razón:

Firmado por: VARGAS PIÑA Julio Cesar (FAU
Razón: