

Lima, 02 de abril de 2009

CIRCULAR N° G- 139 -2009

Ref.: Gestión de la continuidad del
negocio

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones aprobado por el Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas supervisadas, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance

Artículo 1°.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones

Artículo 2°.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

- a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
- b. Grupos de interés: Personas u organizaciones que se ven impactadas por las operaciones de una empresa. Ejemplos: clientes, socios del negocio, empleados, proveedores, accionistas, entidades gubernamentales, entre otros.
- c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
- d. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

- e. Periodo máximo tolerable de interrupción: Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.
- f. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- g. Riesgo: La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.
- h. Riesgo operacional: La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.
- i. Tiempo objetivo de recuperación: Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

Gestión de la continuidad del negocio

Artículo 3°.- La gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Las empresas deben realizar una gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

Responsabilidad del Directorio

Artículo 4°.- El Directorio es responsable de establecer una adecuada gestión de la continuidad del negocio. Entre sus responsabilidades específicas están:

- a. Aprobar una política general que defina el alcance, principios y guías que orienten la gestión de la continuidad del negocio.
- b. Aprobar los recursos necesarios para el adecuado desarrollo de la gestión de la continuidad del negocio, a fin de contar con la infraestructura, metodología y personal apropiados.
- c. Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de la continuidad del negocio.

Responsabilidad de la Gerencia

Artículo 5°.- La gerencia general tiene la responsabilidad de implementar la gestión de la continuidad del negocio conforme a las disposiciones del Directorio. La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades relacionadas con la gestión de la continuidad del negocio.

Responsabilidad de la Unidad de Riesgos

Artículo 6°.- La Unidad de Riesgos deberá asegurarse que la gestión de la continuidad del negocio que realice la empresa sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Función de continuidad del negocio

Artículo 7º.- Las empresas deberán contar con una 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 empresa, incluyendo la asignación de roles y responsabilidades;
- b. Velar por una gestión de la continuidad del negocio competente;
- c. Informar a la gerencia general y al comité de riesgos los aspectos relevantes de la gestión de la continuidad del negocio para una oportuna toma de decisiones.

En función a su tamaño y complejidad de operaciones y servicios, esta función será desempeñada por una unidad especializada o asignada a otra unidad de la empresa.

Fases de la gestión de la continuidad del negocio

Artículo 8º.- Las empresas deberán desarrollar como mínimo las siguientes fases como parte de la gestión de la continuidad del negocio:

8.1. Entendimiento de la organización

Esta fase consiste en conocer los objetivos y metas de la empresa; identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.

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

- a. Análisis de impacto: Consiste en determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios de la empresa. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la empresa, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, debe establecerse el período máximo tolerable de interrupción por cada uno de estos procesos.

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: Consiste en identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deberá seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos que enfrenta la empresa.

La empresa debe definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

8.2. Selección de la estrategia de continuidad

En esta fase, se determinan las estrategias de continuidad que permitirán mantener las actividades y procesos de negocio luego de ocurrido un evento de interrupción de operaciones.

Debe desarrollarse, como mínimo, la siguiente actividad:



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

- a. Evaluación y selección de estrategias de continuidad por proceso: Se refiere a seleccionar las estrategias que permitirán mantener la continuidad de los procesos que soportan los principales productos y servicios de la empresa, dentro del tiempo objetivo de recuperación, definido para cada proceso. Las estrategias de continuidad deben tomar en cuenta los siguientes aspectos, 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.

8.3. Desarrollo e implementación de la estrategia de continuidad

En esta fase, se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta flexible y escalable 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 empresas deberán implementar dos tipos de planes:

- a. Plan de Gestión de Crisis: Consiste en preparar a la empresa 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
 - Interacción con los medios de comunicación
 - Comunicación con los grupos de interés
 - Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno)
- b. Plan(es) de Continuidad del Negocio: Tiene(n) como objetivo dotar a la empresa de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos. Debe(n) considerar, como mínimo, los siguientes aspectos:
- Propósito y alcance
 - Roles y responsabilidades
 - Criterios de invocación y activación
 - Responsable de su actualización
 - Planes de acción para reanudar los procesos conforme a la estrategia seleccionada.
 - Requerimiento de recursos
 - Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, entre otros)

Se deben desarrollar planes específicos considerando, por lo menos, los siguientes:

Plan de Emergencia: Plan que tiene como objetivo salvaguardar la integridad física del personal.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Plan de Recuperación de los servicios de tecnología de información: Plan que busca inicialmente restaurar los servicios de tecnología de información dentro de los parámetros establecidos, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

8.4. Pruebas y actualización

Los planes de continuidad del negocio deberán ser probados cuando menos una vez al año. A continuación se detallan las actividades mínimas que deben ser aplicadas en esta fase:

- a. Ejecución de pruebas: El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones. Esta información debería ser usada para mejorar los planes de continuidad del negocio en forma oportuna. Pueden aplicarse diferentes tipos de prueba, desde las pruebas de escritorio hasta las simulaciones completas de escenarios de interrupción de operaciones.

Las empresas deberán asegurarse que sus principales proveedores de servicios cuenten con planes de continuidad y que éstos cumplan con lo señalado en el presente numeral.

- b. Actualización de los planes: Las empresas deben definir políticas y procedimientos para la actualización de los planes de gestión de la continuidad del negocio, de tal manera que cualquier cambio que impacte a la empresa (ya sea interno o externo) sea revisado en relación con la continuidad del negocio.

8.5. Integrar la gestión de la continuidad del negocio a la cultura organizacional

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

- a. Evaluación del grado de conocimiento sobre la gestión de continuidad: Tiene como objetivo determinar el nivel de conocimiento actual y esperado sobre la gestión de continuidad del negocio, los procedimientos implementados, las tareas específicas señaladas en los planes de continuidad, entre otros aspectos.
- b. Desarrollo y mejora de la cultura de continuidad: Diseñar e implementar planes de capacitación y entrenamiento, a fin de cubrir las deficiencias encontradas en la actividad previa.
- c. Monitoreo permanente: Revisar periódicamente el nivel de entendimiento de la gestión de continuidad del negocio a fin de identificar requerimientos adicionales.

Documentación Sustentatoria

Artículo 9°.- Las empresas deberán mantener a disposición de la Superintendencia la documentación necesaria que permita sustentar el desarrollo de cada una de las fases y actividades descritas en el artículo anterior.

Los principales aspectos de la gestión de la continuidad del negocio, incluyendo el programa de pruebas de los planes de continuidad, serán reportados a través del aplicativo IG-ROp en el plazo establecido en el Reglamento para la Gestión del Riesgo Operacional.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Cambios significativos

Artículo 10°.- Las empresas analizarán 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, entre otros.

Auditoría Interna

Artículo 11°.- La Unidad de Auditoría Interna evaluará el cumplimiento de lo dispuesto en la presente norma de acuerdo a su plan de trabajo.

Plan de Adecuación

Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las empresas deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la empresa respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Vigencia y Plazo de Adecuación

Artículo 13°.- La presente Circular entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010. A partir de dicha fecha, queda derogado el artículo 83° del Título III del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones, referido a Gestión Empresarial.

Atentamente,

FELIPE TAM FOX

Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones