CAPÍTULO 20-9

GESTION DE LA CONTINUIDAD DEL NEGOCIO.

El presente Capítulo establece un conjunto de lineamientos y buenas prácticas que deben ser consideradas por las entidades en la gestión de los riesgos de continuidad del negocio, atendiendo en todo caso el volumen y complejidad de sus operaciones. La debida adhesión de las entidades fiscalizadas a estos lineamientos y buenas prácticas será parte de la evaluación de gestión establecida en el Capítulo 1-13 de la RAN.

Por lo tanto, este Capítulo complementa lo señalado en la letra c) del numeral 3.2 del Título II del Capítulo 1-13 de esta Recopilación sobre la evaluación del riesgo operacional, como asimismo lo dispuesto en el Capítulo 20-7 en lo que se refiere a los riesgos que se asumen en la externalización de servicios.

En el Anexo adjunto se incluyen definiciones de conceptos utilizados en este documento.

I. ELEMENTOS GENERALES DE GESTIÓN.

En la evaluación de la gestión de la continuidad del negocio, un elemento fundamental corresponde al rol del Directorio en lo relativo a la aprobación de la estrategia institucional en esta materia. Asimismo, será importante verificar que la entidad dispone de metodologías para una adecuada identificación, cuantificación, evaluación y monitoreo de estos riesgos.

En ese sentido, revelan una buena gestión, por ejemplo, situaciones o hechos tales como:

- La entidad cuenta con una estrategia de administración de la continuidad del negocio aprobada por el Directorio, la que es concordante con el volumen y complejidad de las operaciones y la calidad de los servicios comprometidos.

- El Directorio ha dispuesto la existencia de una función de riesgos encargada del diseño y mantención de un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos que afectan la continuidad del negocio, así como también instancias colegiadas de alto nivel con atribuciones y competencias para gestionar esta materia.

- El Directorio ha aprobado una estructura de alto nivel para la administración de crisis, con atribuciones técnicas y del negocio para conocer y controlar cualquier interrupción de alto impacto que afecte a la entidad.

- El Directorio ha dispuesto un mecanismo que le permite informarse, periódica y adecuadamente, de la gestión de la entidad en materia de continuidad del negocio.

- La entidad mantiene políticas aprobadas por el Directorio para la administración de la continuidad del negocio, acordes con el volumen y complejidad de sus operaciones. Estas políticas son comunicadas a todas las partes interesadas y son revisadas al menos anualmente.

- Antes de introducir nuevos productos, emprender nuevas actividades o definir nuevos procesos y sistemas, la entidad se asegura de evaluar los riesgos de continuidad del negocio que se podrían estar asumiendo.

- La entidad ha desarrollado una metodología formal de evaluación de impacto del negocio (BIA), que considera los criterios necesarios para identificar los procesos de mayor criticidad y determinar los tiempos de recuperación objetivo (RTO) definidos por la entidad, este último con la aprobación de su Directorio. Asimismo, efectúa un análisis de los riesgos de continuidad del negocio de aquellos procesos identificados con mayor criticidad (RIA), a fin de mitigar su impacto o disminuir su probabilidad de ocurrencia. Dichos análisis son realizados al menos con periodicidad anual.

- La entidad considera como mínimo los escenarios de contingencia referidos a: la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder y/o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores. Además, de acuerdo con su propio perfil de riesgo, considera otros escenarios de contingencia que la puedan afectar. Todo lo anterior se encuentra debidamente formalizado en la respectiva política.

- Para aquellos procesos críticos la entidad tiene planes documentados de contingencia operativos y de recuperación ante desastres, que le permiten responder a la materialización de los escenarios de contingencia definidos, los que se actualizan al menos anualmente. Asimismo, cuenta con adecuados procedimientos para restaurar y volver a las actividades normales del negocio después de superada la contingencia.

- La entidad somete a prueba los planes de contingencia operativos y de recuperación ante desastres que soportan los procesos críticos en todos los escenarios previstos, a fin de asegurar su suficiencia y eficacia. Los ejercicios se realizan al menos con una periodicidad anual, de acuerdo con los tipos de pruebas definidos, procurando en todo caso avanzar constantemente hacia pruebas de mayor complejidad; por ejemplo, pruebas de escritorio, de simulación y de actividades críticas, entre otras. El resultado de estas pruebas se refleja en un informe que permite determinar con claridad el alcance, las condiciones en que se realiza cada ejercicio y los planes de corrección si corresponde.

- La entidad realiza pruebas, al menos con una periodicidad anual, al plan de recuperación de desastres (DRP) que simulen la indisponibilidad de sus sitios de procesamiento, tanto durante la ejecución de los procesos *online*, como durante la ejecución de los procesos *batch*. Las pruebas realizadas deben contar previamente con los análisis de riesgos respectivos, y la intensidad de ellas debe estar en función de los potenciales impactos en los clientes.

- Existe un proceso formal y sistemático de gestión frente a los incidentes que pudieran interrumpir o afectar la provisión de los productos, servicios o actividades.

- La entidad se preocupa de generar información suficiente, adecuada y oportuna de los riesgos vinculados con esta materia, los cuales son reportados a las instancias que toman decisiones en caso de ser necesario.

- La entidad mantiene un plan de comunicaciones que opera ante contingencias, para informar a todas las partes interesadas, ya sean internas o externas.

- La entidad se asegura de mantener personal con experiencia y debidamente capacitado para afrontar todos los escenarios de contingencia definidos.

- La entidad tiene programas de capacitación y entrenamiento que permiten que todos los niveles del personal asuman y comprendan sus responsabilidades en la mantención del modelo de continuidad del negocio.

- La entidad realiza auditorías independientes al proceso de administración de la continuidad del negocio, con la profundidad y alcance necesario y suficiente.

II. SITIOS DE PROCESAMIENTO DATOS E INFRAESTRUCTURA TECNOLÓGICA.

Uno de los aspectos relevantes que contribuyen a fortalecer la resiliencia operacional de las entidades, es la mantención de sitios de procesamiento de datos e infraestructura tecnológica robusta resultante de una adecuada gestión, la que se manifiesta en hechos tales como:

- Los centros de procesamiento de datos, ya sea principal o de contingencia, se encuentran permanentemente homologados en la infraestructura tecnológica y versiones de *software*, y operando preferentemente en modalidad activo-activo.

- El diseño, la construcción y la operación de los sitios de procesamiento de datos se encuentran certificados por una entidad especializada e independiente.

- La infraestructura de los sitios de procesamiento de datos tienen la capacidad, en cuanto a energía, refrigeración y mantenimiento, para alcanzar una disponibilidad de operación de al menos 99,98% o *downtime* de 1,6 horas anuales.

- La configuración de los sitios permite disponer de una infraestructura de telecomunicaciones y de equipamiento computacional con la redundancia necesaria para evitar puntos únicos de falla; con medios de comunicación distintos en sus trayectorias; y gestionado por especialistas, de manera de proporcionar soporte técnico que funcione de acuerdo con las necesidades del negocio y operando preferentemente en modalidad 24x7.

- Los sitios principal y de contingencia han sido dispuestos de tal forma que no queden expuestos a los mismos riesgos, considerando, entre otros, factores como la ubicación y distancia entre las instalaciones.

- La entidad cuenta con infraestructura y procedimientos de respaldo que permiten recuperar los datos, *software* básico y aplicativos, ante una contingencia o corrupción de la información de acuerdo con los RPO y RTO establecidos.

III. CONTINGENCIAS DE CARÁCTER SISTÉMICO.

La continuidad del negocio no sólo debe gestionarse a nivel de cada entidad financiera, sino que debe considerarse que su funcionamiento se da en un entorno donde existen diferentes actores que pueden verse afectados simultáneamente. En este contexto, es necesario que las entidades cuenten con planes específicos para mitigar el efecto que una contingencia de carácter sistémico pueda producir en el sistema financiero.

En línea con lo anterior, en las evaluaciones se examinarán al menos los siguientes aspectos:

- La entidad dispone de un plan comunicacional para informar en forma efectiva la materialización de algún escenario de contingencia a todas las partes interesadas.

- La entidad tiene equipos humanos altamente capacitados y/o entrenados para las labores de coordinación, tanto en el plano interno como con las autoridades competentes y otras instituciones públicas y privadas.

- La entidad cuenta con procedimientos para ubicar y contactar al personal dentro de las zonas afectadas, considerando además la provisión de transporte para facilitar la logística y el traslado del personal.

- La entidad ha establecido medios de comunicación alternativos a los de uso regular, que permitan enviar y recibir mensajería instantánea mediante el uso de telefonía satelital u otros servicios de transmisión inalámbrica que puedan servir como contingencia.

- La entidad cuenta con planes de contingencia operativos para proveer de liquidez (dinero efectivo) al mercado, de manera de mitigar el efecto que pueda producirse por indisponibilidad de los medios de pago de bajo monto, como las tarjetas de crédito y de débito, y la eventual imposibilidad de utilizar cajeros automáticos.

- La entidad considera alianzas de cooperación con otras instituciones financieras, de acuerdo con la legalidad vigente, a fin de que la entidad afectada pueda mantener sus operaciones críticas. Por ejemplo, acuerdos para compartir infraestructura y mesas de ayuda.

- La entidad dispone de políticas para la adecuada gestión del riesgo de concentración de los servicios externalizados críticos.

- En los contratos con proveedores de servicios, la entidad cuenta con adecuados planes de contingencia en caso de que tengan cláusulas que limiten el acceso físico del personal a los centros de datos y/o faculten al proveedor de servicios para tomar decisiones unilaterales en escenarios de contingencias mayores.

_____

ANEXO

DEFINICIONES

Análisis de impacto o BIA: Comprende el análisis de actividades o procesos y el efecto que una disrupción del negocio pudiera tener sobre ellos.

Análisis de riesgo o RIA: Comprende la identificación, evaluación y valoración de los riesgos de los procesos, centrados en aquellos riesgos que podrían afectar a la continuidad del negocio.

Continuidad del negocio: Se refiere a la capacidad de la organización para continuar la entrega de productos o servicios en los niveles aceptables de operación, previamente definidos, tras un incidente.

Gestión de la continuidad del negocio: Se entiende como un proceso de administración, que incluye las políticas, normas y procedimientos necesarios para garantizar que los productos o servicios entregados por las instituciones bancarias se puedan mantener o recuperar de manera oportuna en el caso de una interrupción.

Incidente(s): Interrupción o reducción en la calidad del servicio o cualquier acontecimiento que podría afectar negativamente el servicio.

Plan de contingencia operativo: Se refiere a los procedimientos orientados a recuperar las operaciones ante la ocurrencia de fallas producto de la materialización de alguno de los escenarios de contingencia definidos por el banco. Son complementarios, en lo que corresponde, al Plan de recuperación ante desastres.

Plan de recuperación ante desastres (DRP): Procedimientos diseñados para dar respuesta ante una pérdida parcial o total de los recursos computacionales e instalaciones físicas que las soportan.

Proveedor(es) de servicios: entidad relacionada o no a la institución contratante, que preste servicios o provea bienes y/o instalaciones a ésta.

Proceso de gestión de incidentes: conjunto de actividades orientadas a restaurar la operación normal del servicio a la brevedad y a mantener al mínimo el impacto adverso en la operación normal.

Punto Objetivo de recuperación (RPO): Máxima pérdida de datos aceptada por la entidad.

Sitio o centro principal (producción): Infraestructura física donde se centralizan los recursos informáticos para proveer la tecnología necesaria para la operativa diaria.

Sitio o centro de contingencia: Centro de procesamiento que debe contar con los recursos necesarios, para asegurar la recuperación tecnológica de los sistemas en el tiempo estimado por la entidad.

Tiempo de recuperación objetivo o RTO: Periodo de tiempo después de un incidente en que la provisión tecnológica de los productos, servicios o actividad debe reanudarse; o los recursos deben ser recuperados

---