- 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.