Modificación de la Disposición Vinculada N° 01
del Capítulo II De los Participantes del Reglamento Interno de CAVALI

Por medio de la presente, ponemos a conocimiento del público en general, que se ha acordado modificar la Disposición Vinculada N° 01 del Capítulo II De los Participantes del Reglamento Interno de CAVALI, con la finalidad de incorporar los temas referidos a los procedimientos PLAFT que deben contar los Participantes de CAVALI.

En este sentido, a fin de dar cumplimiento a lo dispuesto por el artículo N° 27 del Reglamento de Instituciones de Compensación y Liquidación de V alores, aprobado por Resolución CONASEV N° 031-99-EF/94.10, y el artículo N° 5 del Capítulo I De las Disposiciones Preliminares y Definiciones del Reglamento Interno de CAVALI, aprobado por Resolución CONASEV N° 057-2002-EF/94.10; se informa que el texto de las referidas modificaciones, tal como se muestra en el Anexo a la presente comunicación, se estará difundiendo a Participantes, así como a través de la página web de CAVALI (www.cavali.com.pe), por un plazo de cinco (5) días útiles, el cual se inicia el 03.12.21 y finaliza el 09.12.21, por lo que su entrada en vigencia será el 10.12.2021.

Lima, 02 de diciembre de 2021

ANEXO

Modificación de la Disposición Vinculada N° 01
del Capítulo II De los Participantes del Reglamento Interno de CAVALI

TEXTO VIGENTE	TEXTO PROPUESTO
CAPITULO II **Disposición Vinculada N° 01** (…) ANEXO 2 REQUERIMIENTOS OPERATIVOS **(i) Gestión del Riesgo Operacional** a) Tener implementados políticas, procedimientos y controles adecuados para la administración de los riesgos operativos, incluyendo aquellos relacionados a la seguridad de la información y continuidad del negocio. b) Contar con un equipo humano, recursos e infraestructura definida y adecuada para asegurar el cumplimiento de sus obligaciones y responsabilidades frente a CAVALI, así como frente a los demás Participantes, Emisores, Titulares o tenedores y demás personas naturales o jurídicas que correspondan, según corresponda. c) Contar con sistemas (sean automatizados o no) con un alto grado de fiabilidad operativa y controles de seguridad que salvaguarden la confidencialidad, integridad y	**CAPITULO II** **Disposición Vinculada N° 01** (…) ANEXO 2 REQUERIMIENTOS OPERATIVOS **(i) Gestión del Riesgo Operacional** a) Tener implementados políticas, procedimientos y controles adecuados para la administración de los riesgos operativos, incluyendo aquellos relacionados a la seguridad de la información y continuidad del negocio. b) Contar con un equipo humano, recursos e infraestructura definida y adecuada para asegurar el cumplimiento de sus obligaciones y responsabilidades frente a CAVALI, así como frente a los demás Participantes, Emisores, Titulares o tenedores y demás personas naturales o jurídicas que correspondan, según corresponda. c) Contar con sistemas (sean automatizados o no) con un alto grado de fiabilidad operativa y controles de seguridad que salvaguarden la confidencialidad, integridad y disponibilidad de la información intercambiada con CAVALI

disponibilidad de la información intercambiada con CAVALI y otros actores del mercado. d) Contar con planes de contingencia para la recuperación de su capacidad operativa con la mayor inmediatez posible, de modo que aseguren que no se afecte el normal desenvolvimiento del mercado. Dichos planes deben ser revisados, actualizados y sometidos a prueba, al menos, una vez al año. e) Contar con manuales de procedimientos y funciones que contemplen los servicios vinculados al Registro Contable que administra CAVALI, de acuerdo a lo señalado en el artículo 2, literal b),tercer párrafo, del Capítulo II del Reglamento Interno, y en la Disposición Vinculada Nº 02 de dicho capítulo. **(ii) Gestión de la Ciberseguridad:** a) Establecer y mantener una estrategia y marco de ciberseguridad adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS, entre otros.	y otros actores del mercado. d) Contar con planes de contingencia para la recuperación de su capacidad operativa con la mayor inmediatez posible, de modo que aseguren que no se afecte el normal desenvolvimiento del mercado. Dichos planes deben ser revisados, actualizados y sometidos a prueba, al menos, una vez al año. e) Contar con manuales de procedimientos y funciones que contemplen los servicios vinculados al Registro Contable que administra CAVALI, de acuerdo a lo señalado en el artículo 2, literal b),tercer párrafo, del Capítulo II del Reglamento Interno, y en la Disposición Vinculada Nº 02 de dicho capítulo. **(ii) Gestión de la Ciberseguridad:** a) Establecer y mantener una estrategia y marco de ciberseguridad adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS, entre otros.

(Nota: este requerimiento será exigible a partir del 01 de enero de 2022). b) Definir los roles y responsabilidades para la gestión de la ciberseguridad, proporcionar los recursos adecuados, la autoridad apropiada y el acceso al órgano correspondiente dentro de la empresa (por ejemplo: directorio, gerencia, etc). c) Tener identificados los riesgos cibernéticos a los que está expuesto el negocio del postulante, y tener implementados los controles para gestionar tales riesgos y proteger de los mismos al negocio. Asimismo, realizar una evaluación periódica de dichos riesgos. d) Implementar procesos de monitoreo sistemático para detectar oportunamente los incidentes cibernéticos y evaluar periódicamente la efectividad de los controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios. e) Tener la capacidad de responder oportunamente ante los incidentes cibernéticos de la siguiente manera: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas	(Nota: este requerimiento será exigible a partir del 01 de enero de 2022). b) Definir los roles y responsabilidades para la gestión de la ciberseguridad, proporcionar los recursos adecuados, la autoridad apropiada y el acceso al órgano correspondiente dentro de la empresa (por ejemplo: directorio, gerencia, etc). c) Tener identificados los riesgos cibernéticos a los que está expuesto el negocio del postulante, y tener implementados los controles para gestionar tales riesgos y proteger de los mismos al negocio. Asimismo, realizar una evaluación periódica de dichos riesgos. d) Implementar procesos de monitoreo sistemático para detectar oportunamente los incidentes cibernéticos y evaluar periódicamente la efectividad de los controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios. e) Tener la capacidad de responder oportunamente ante los incidentes cibernéticos de la siguiente manera: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas (CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinar las actividades de

(CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinar las actividades de respuesta conjunta según sea necesario. f) Reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético, permitiendo: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa. g) Compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por la entidad, , vinculada a los servicios a los que el postulante accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda. h) Implementar de forma periódica la revisión de la estrategia y el marco de ciberseguridad cuando los eventos lo justifiquen, incluidos los componentes de gobernanza, evaluación	respuesta conjunta según sea necesario. f) Reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético, permitiendo: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa. g) Compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por la entidad, , vinculada a los servicios a los que el postulante accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda. h) Implementar de forma periódica la revisión de la estrategia y el marco de ciberseguridad cuando los eventos lo justifiquen, incluidos los componentes de gobernanza, evaluación de riesgos y control, monitoreo, respuesta, recuperación e intercambio de información, para abordar los cambios en los riesgos cibernéticos, asignar recursos, identificar y remediar las brechas e incorporar lecciones aprendidas.

de riesgos y control, monitoreo, respuesta, recuperación e intercambio de información, para abordar los cambios en los riesgos cibernéticos, asignar recursos, identificar y remediar las brechas e incorporar lecciones aprendidas. **(iii) Gestión del Riesgo Antisoborno:** Contar con políticas y procedimientos diseñados a prevenir los delitos relacionados al soborno y todo acto de corrupción en la ejecución de los servicios relacionados a CAVALI. En caso de no contar con dichas políticas y procedimientos, deberá tomar conocimiento del Modelo de Prevención de la Corrupción de CAVALI contenido en sus Normas Internas de Conducta, disponible en la página web de CAVALI, manifestándolo a través de la presentación de una declaración jurada.	**(iii) Gestión del Riesgo Antisoborno:** Contar con políticas y procedimientos diseñados a prevenir los delitos relacionados al soborno y todo acto de corrupción en la ejecución de los servicios relacionados a CAVALI. En caso de no contar con dichas políticas y procedimientos, deberá tomar conocimiento del Modelo de Prevención de la Corrupción de CAVALI contenido en sus Normas Internas de Conducta, disponible en la página web de CAVALI, manifestándolo a través de la presentación de una declaración jurada. **(iv) Gestión del Riesgo Lavado de Activos y Financiamiento del Terrorismo:** Contar con políticas y procedimientos diseñados a prevenir los delitos relacionados lavado de activos y financiamiento del terrorismo (PLAFT) en la ejecución de los servicios relacionados a CAVALI, en caso que, de acuerdo a la legislación aplicable, sea sujeto obligado a cumplir con estas normas. En caso de no aplicarle las normas de PLAFT y de no contar con dichas políticas y procedimientos de debida diligencia de conocimiento del cliente, deberá declarar que ha tomado conocimiento del Modelo de Prevención de la Corrupción de CAVALI contenido en sus Normas Internas de Conducta, disponible en la página web de CAVALI.