REGLAMENTO DEL COMITÉ ESPECIALIZADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL BBVA PERÚ Y SUBSIDIARIAS

El comité especializado de seguridad de la información y ciberseguridad (en adelante CESIC) tiene por principal objetivo asistir al directorio y las gerencias del Banco en la protección de sus activos de información, activos tecnológicos, en la detección de eventos de seguridad, en la adopción de las medidas de respuesta y recuperación frente a eventuales incidentes de ciberseguridad y sobre el control de las medidas de seguridad aplicadas por terceros proveedores de servicios tecnológicos.

El CECIC está organizado con visión y enfoque integral.

Para el cumplimiento de sus objetivos, el CESIC se acopla de manera complementaria al Comité Integral de Riesgos (en adelante CIR), en el cual se declaran y gestionan los riesgos vinculados a datos, ciberseguridad y tecnología, bajo el modelo Global de Riesgos que han escalado desde las áreas de negocio e informe al Directorio. En caso sea necesario en el comité especializado de seguridad de la información y ciberseguridad se tratarán temas a detalles que puedan impactar en el Heatmap de Riesgos de la Organización y que necesiten medidas de mitigación. La aprobación de documentos que requieran una validación de Directorio, podrán ser aprobados en el CIR (NFR).

Artículo 1°. Composición del comité especializado de seguridad de la información y ciberseguridad.

El CESIC estará conformado por el comité de dirección y un director designado por el directorio para ver temas de Seguridad de la Información & Ciberseguridad

Artículo 2°. Forma de participación en el comité especializado de seguridad de la información y ciberseguridad.

Las decisiones del CESIC, se adoptarán por mayoría absoluta de sus miembros integrantes, participantes de la reunión.

Artículo 3°. Designación de miembros.

La designación de los miembros que conformarán el CESIC corresponde al CIR El cargo es personal, indelegable y no remunerado.

Artículo 4°. Desempeño de la función.

Los miembros del CESIC ejercerán sus funciones con independencia de criterio.

Están obligados a participar de las reuniones convocadas, salvo la existencia de causa justificada, e intervenir en las deliberaciones, discusiones y debates que se susciten sobre los asuntos sometidos a consideración.

El CESIC actuará ajustándose a los cauces establecidos por el directorio del Banco o el CIR y revisará lineamientos de control y gestión para las empresas comprendidas,

El CESIC informará al CIR sobre los principales temas de impacto y decisiones de relevancia tratados en sus reuniones, con el fin que pueda hacerse el seguimiento de los mismos.

El Head of Corporate Security será el encargado de presentar, cuando corresponda, los informes y acuerdos correspondientes en los directorios de las empresas comprendidas, en el ámbito de gestión del presente comité. Esta función podrá ser objeto de delegación.

Artículo 5°. Derecho de información.

Los miembros del CESIC tienen derecho a ser informados por las gerencias y los comités especializados de todo lo relacionado a las amenazas de seguridad y ciberseguridad que afronta el Banco y las empresas comprendidas.

El presidente del comité, es responsable de presentar y sustentar ante el comité especializado de seguridad de la información y ciberseguridad, todas las propuestas que sean elevadas a dicho comité.

El derecho de información sólo debe ser ejercido en el seno del comité y de manera de no afectar la gestión social del Banco o de las empresas comprendidas, generar conflictos de interés y cautelando la información que tenga la calidad de reservada, privilegiada o confidencial.

En ese sentido, los miembros del CESIC dispondrán de la información suficiente para poder formar criterio respecto de las cuestiones que le correspondan resolver.

El CESIC podrá contar con el auxilio de expertos del BBVA y terceros en la materia y en aquellos temas sometidos a su consideración que, por su especial complejidad o trascendencia, a su juicio, así lo requiriera.

Artículo 6°. Presidencia y vicepresidencia.

El CESIC elegirá entre sus miembros a un presidente, quien conducirá las sesiones.

Artículo 7°. Secretaria del comité especializado de seguridad de la información y ciberseguridad.

El CESIC nombrará a un secretario que será el encargado de la redacción de las actas y de la custodia de las mismas. No se requiere ser miembro del comité para ejercer dicha función. El secretario estará sujeto a las reglas de confidencialidad y reserva establecidas en el presente reglamento.

Artículo 8°. Deber de confidencialidad.

Los miembros del CESIC guardarán reserva y confidencialidad de las deliberaciones ocurridas en su seno, así como de toda aquella información a la que hayan tenido acceso en el ejercicio de sus funciones. La información a la que accedan, se utilizará exclusivamente para la adopción de las decisiones o el establecimiento de las políticas y procedimientos de su competencia. La obligación de confidencialidad subsistirá aún después de que se haya cesado en el cargo.

Artículo 9°. Ética y normas de conducta.

Los miembros del CESIC deberán guardar en su actuación un comportamiento ético acorde con las exigencias normativas aplicables a quienes desempeñen cometidos de administración en entidades financieras, de buena fe, y conforme a los principios que constituyen los valores corporativos a los que se hubiere adherido el Banco y las empresas comprendidas

Artículo 10°. Conflictos de intereses.

El miembro CESIC que presente un potencial conflicto de interés en algún asunto sometido a su consideración deberá abstenerse de intervenir en la deliberación del tema, dejando constancia de ello en el acta correspondiente de la sesión.

A manera de ejemplo enunciativo y no taxativo, se presentan algunos casos de potenciales conflictos de interés y reglas de conducta que deberán observar los miembros del comité especializado de seguridad de la información y ciberseguridad frente a aquellos:

10.1 No podrán intervenir en las deliberaciones en asuntos en los que pudiere tener un interés personal de negocio, sea directo o indirecto;

10.2 No podrán intervenir en las deliberaciones de los asuntos que afecten a las personas con él vinculadas en los términos legalmente establecidos, recomendando la realización de transacciones sea con el Banco y/ o sus subsidiarias, que sean distintas de las relaciones habituales propias a cada una de ellas;

10.3 No podrán valerse de su posición para aprovechar en beneficio propio, directa o indirectamente, o de personas vinculadas a él, una oportunidad de negocio de la que haya tenido conocimiento como consecuencia de su actividad como miembro del comité.

En todo caso, los miembros del CESIC deberán someterse en su actuación a las disposiciones que le resulten aplicables contenidas en los códigos de conducta vigentes para el Banco y las empresas comprendidas, así como a las disposiciones legales que fueran aplicables; evitando en todo momento el uso indebido de información privilegiada o reservada obtenida en el ejercicio del cargo.

Artículo 11°. Cese de los integrantes del comité especializado de seguridad de la información y ciberseguridad.

Los miembros del CESIC permanecerán en funciones mientras ocupen los cargos para los cuales fueron originalmente designados. Asimismo, deberán poner su cargo a disposición, y aceptar la decisión que el CIR pudiera adoptar sobre su continuidad, quedando obligados en este último caso a formalizar la correspondiente renuncia, en los siguientes supuestos:

11.1 Cuando se vean incursos en alguno de los supuestos de incompatibilidad o prohibición que esté previsto en la normativa aplicable, en el estatuto del Banco y las empresas comprendidas, o en el presente reglamento;

11.2 Cuando se produjeran cambios significativos en su situación profesional o en el carácter en virtud del cual hubieran sido designados como tales;

11.3 En caso de incumplimiento grave en el desempeño de sus obligaciones y funciones;

Artículo 12°. Funciones del comité especializado de seguridad de la información y ciberseguridad

El CESIC, tiene como principales funciones las siguientes:

12.1 Aprobar el plan estratégico del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C) del Banco y las empresas comprendidas; considerando el tamaño y la complejidad de los servicios que cada una de ellas presta;

12.2 Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y ciberseguridad.

12.3 En concordancia con lo establecido por el Art. 14.3 del Reglamento del CIR, el CESIC apoyará a las áreas de control y riesgos en la difusión e implementación de la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención alineado a la protección de la información.

12.4 Solicitar a las gerencias de gestión de Fraude, Seguridad de la Información y Ciberseguridad el informe de los principales temas tratados y las resoluciones adoptadas para efectos de su control y monitoreo de los temas de seguridad.

12.5 Los riesgos que se identifiquen como parte de la gestión del Fraude, Seguridad de la Información y Ciberseguridad deberán ser informados en el CIR del Banco.

12.6 Deberá apoyar a la toma de decisiones sobre la gestión de fraude, seguridad de la información, ciberseguridad y seguridad física, según sea el caso y sobre los proyectos o iniciativas para mejorar la seguridad integral de la empresa.

12.7 Deberá analizar la situación del Banco y de las empresas comprendidas, así como de la industria propia a cada una de ellas , frente a los principales eventos de fraude, seguridad, ciberseguridad materializados y el seguimiento del desarrollo de la estrategia en la lucha contra el fraude y mitigación de eventos de mal uso de información y estrategia de respuesta a eventos de ciberseguridad.

12.8 Deberá velar por el cumplimiento de las regulaciones vigentes en materia de seguridad vinculadas a la regulación aplicable. Considerando mayor foco de monitoreo a la Resolución S.B.S. Nº 504-2021 - Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

Artículo 13°. Operatividad del comité especializado de seguridad de la información y ciberseguridad.

El CESIC debe contar con un calendario de sesiones ordinarias. El calendario de sesiones debe aprobarse en la sesión que corresponda el último mes del año en ejercicio. El número y la programación de las sesiones deben permitir cumplir adecuadamente con su plan de trabajo.

Artículo 14°. Sesiones del comité especializado de seguridad de la información y ciberseguridad

El CESIC se reunirá en forma ordinaria cada tres meses; sin perjuicio de la celebración de cualquier sesión extraordinaria que sea necesaria para el cumplimiento de sus funciones. Las sesiones extraordinarias se llevarán a cabo a pedido de cualquier miembro

Artículo 15°. Orden del día de las sesiones.

A la convocatoria se acompañará la agenda de la sesión, pudiendo decidirse igualmente, aun hecha la convocatoria, que algún asunto no estipulado en aquella sea tratado en la sesión, siempre que estén presentes todos sus miembros, incluyendo su secretario.

Artículo 16°. Quórum de constitución y adopción de acuerdos.

El CESIC quedará válidamente constituido cuando participen en la reunión el número entero superior a la mitad de sus miembros.

Los acuerdos se adoptarán por mayoría absoluta de votos de los miembros participantes.

Artículo 17°. Sesiones no presenciales.

Podrán realizarse sesiones no presenciales del CESIC a través de videoconferencia u otros medios escritos o electrónicos, siempre que ningún miembro se oponga a este procedimiento y tendrán validez las actas y acuerdos que se comuniquen por medios electrónicos dirigidos a los miembros del comité

Artículo 18°. Desarrollo de las sesiones.

Las sesiones del CESIC se celebrarán en el lugar, fecha y hora programada siguiendo el orden del día establecido al efecto por el presidente, quien dirigirá sus deliberaciones y discusiones.

En caso de impedimento del presidente presidirá las sesiones el vicepresidente. Los miembros del comité podrán acceder a cuanta información consideren necesaria o conveniente en relación con los asuntos que se traten en la sesión. En ese sentido, la información de los asuntos a tratar deberá estar a disposición de todos sus miembros con la debida antelación; salvo que se trate de algún un tema que requiera inmediata resolución en cuyo caso será de aplicación lo señalado en el artículo 15° del presente reglamento.

A las sesiones podrán incorporarse ejecutivos del Banco, de las empresas comprendidas u otras personas cuya presencia se considere conveniente para el más adecuado tratamiento de los asuntos sometidos a consideración.

Artículo 19°. Actas.

Los acuerdos adoptados por el comité especializado de seguridad de la información y ciberseguridad constarán en actas, las cuales deberán contener un resumen de los temas tratados en la reunión. La documentación que se presente en las reuniones, formará parte del archivo de actas de la sesión.

Corresponderá al secretario configurar la redacción definitiva del acta sobre la base de las consideraciones y acuerdos que se hubieren tratado en la sesión. Las mismas se comunicarán a los involucrados por un medio físico o virtual y se considerarán como aprobadas en el momento de la recepción.

Las actas estarán a disposición de los miembros del comité, en una carpeta electrónica de acceso restringido creada para tales efectos.

Artículo 20° Programas de inducción.

A cada nuevo miembro del CESIC se le proporcionará copia del presente reglamento y se le explicará la mecánica operativa de las reuniones.

Artículo 21° Interpretación.

Corresponde al CIR interpretar y resolver las dudas que suscite la aplicación de este reglamento de

conformidad con los criterios generales de interpretación de las normas jurídicas.

Se interpretará de conformidad con las normas legales y estatutarias que sean de aplicación y tomando en consideración los principios y recomendaciones.