Sistemas de Gestión

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, RIESGOS Y CONTINUIDAD DE NEGOCIOS

I. INTRODUCCIÓN

El Banco Central de Chile pone a disposición de todas sus partes interesadas los aspectos generales de su (i) Sistema de Gestión de Seguridad de la Información, (ii) Sistema de Gestión Integral de Riesgos, (iii) Sistema de Gestión de Continuidad de Negocios. Estos aspectos son parte del marco normativo dispuesto por el Banco para su funcionamiento interno.

II. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El marco de seguridad de la información establecido en el Banco Central de Chile, incluye la definición de un conjunto de políticas, normas y procedimientos. Todos estos documentos junto con otros elementos definidos al interior de la institución como Comités, herramientas informáticas (a nivel de perímetro y estaciones de trabajo) y roles con funciones asociados a tareas tanto de seguridad de la información como seguridad informática, permiten en su conjunto disponer de los mecanismos necesarios para mantener un ambiente de control de acuerdo a lo esperado al interior del Banco.

Política de Seguridad Integral

Esta Política apoya el logro de los objetivos institucionales y la continuidad operacional, proporcionando la adecuada protección a las personas, a la información y a los activos físicos del Banco Central de Chile con objeto de prevenir y reducir los riesgos de daño.

La Política establece el siguiente objetivo:

Esta política busca proteger a las personas, preservar la confidencialidad, integridad y disponibilidad de la información y de los valores de sus activos y asegurar la continuidad operacional en la entrega de los servicios que provee la institución.

La Política establece los siguientes principios:

- La seguridad es tarea de todos los miembros de la organización por lo que cada uno debe velar y contribuir a preservar dicho ambiente colaborando con las guías y controles establecidos.

- Las personas constituyen el capital humano que permite a la organización cumplir su misión y objetivos, por tanto quienes trabajan en la Institución contarán con un lugar de trabajo que cumpla con las condiciones básicas de seguridad y prevención de riesgos necesaria para él.

- La información es un bien valioso y los sistemas de información son activos críticos para la organización. Por esta razón es que deben estar adecuadamente protegidos de acuerdo a su sensibilidad contra malos usos, daños, modificaciones, robo y/o pérdidas.

- Los activos físicos, títulos de crédito y demás valores del Banco son parte del patrimonio institucional que debemos cautelar y, por tanto, deben ser protegidos y resguardados gestionando eficientemente los mejores medios físicos y tecnológicos disponibles para estos efectos y que constituyen la mejor práctica para instituciones como el Banco Central de Chile.

- Es deber del personal y de las personas que prestan servicios en el Banco, tomar todas las medidas de precaución necesarias para resguardar la seguridad de las personas, de la información, los bienes físicos, títulos de crédito y demás valores que utilizan en el desempeño de sus funciones.

- Es obligación del personal y demás personas que prestan servicios en el Banco, a cualquier título, tomar conocimiento de esta política y dar cumplimiento a ella. Las personas que infrinjan las disposiciones de seguridad serán sancionadas según la gravedad de los hechos, en los términos fijados en el Reglamento del Personal.
- El Banco capacitará al personal en estas materias y la administración proporcionará los recursos necesarios para mejorar el desempeño en la seguridad y salud de las personas que trabajan en la Institución, como también en la seguridad de la información y en la de sus activos.

- El Banco tiene el compromiso de cumplir con las leyes y reglamentaciones vigentes, que sean aplicables a sus funciones.

- Los estándares que adoptará el Banco, en lo que le sea aplicable a la institucionalidad que lo rige, serán las normas ISO vigentes para Seguridad de la Información y las normas OHSAS vigentes para Seguridad y Salud Ocupacional.

- Los dominios de referencia que considerarán los manuales y procedimientos de Seguridad del Banco, son: organización de la seguridad, seguridad relacionada a los recursos humanos, gestión de activos, control de accesos, criptografía, seguridad física y del ambiente, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de los sistemas, relaciones con los proveedores, gestión de incidentes de seguridad, gestión de la continuidad de las actividades del Banco, y cumplimiento.

III. SISTEMA DE GESTIÓN INTEGRAL DE RIESGOS

Para dar cumplimiento a la misión, la visión y los objetivos estratégicos del Banco Central de Chile es necesario contar con un Sistema de Gestión Integral de Riesgos con el propósito de mantener acotados y minimizados los riesgos.

Política Gestión Integral de Riesgos

Establece dentro de su alcance como procesos clave la gestión preventiva de riesgos, la gestión de continuidad del negocio y la gestión de seguros. Se establece una estructura organizacional, para la definición de roles y responsabilidades, haciendo énfasis en riesgos estratégicos, financieros, operacionales, legales y reputacionales. A su vez, señala la existencia de comités, los cuales facilitan la discusión relacionada con planes de tratamiento, niveles de aceptación y tolerancia de riesgos en los ámbitos de personas, sistemas, procesos, seguridad, continuidad, financiero y crisis operativa. Por último hace mención a la cultura de riesgos y a los principios que sustentan el riesgo aceptable.

La Política establece los siguientes objetivos:

- Promover una cultura de gestión del riesgo que incremente el entendimiento, conciencia y acción de las personas, e incluya también la promoción de la eficiencia y un efectivo control;

- Establecer una infraestructura básica auto sostenible y sustentable en el tiempo, que permita gestionar en forma integral los riesgos en el Banco Central de Chile (incluye la Política, la Metodología de Riesgos, la Documentación, el Sistema de Desempeño e Incentivos, la Revisión, etc.).

- Facilitar la identificación de nuevas oportunidades para las operaciones de la organización.

- Evitar y/o disminuir los posibles eventos de pérdida.

La Política establece los siguientes principios:

- Gestión Preventiva de Riesgos,
- Gestión de la Continuidad del Negocio y
- Gestión de Seguros.

IV. SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS

La continuidad operacional del Banco Central de Chile (BCCh), es administrada mediante un sistema de gestión que permite identificar los posibles impactos ante interrupciones que amenazan la continuidad de sus operaciones. Además de proporcionar un marco que permite aumentar la resiliencia y la capacidad de respuesta.

Política de Continuidad de Negocios

El Banco Central de Chile cuenta con una Política de Continuidad de Negocios que se sustenta en el entendimiento de los riesgos de interrupción y la necesidad de mantener las operaciones asociadas a las funciones encomendadas al BCCh por su Ley Orgánica Constitucional. Además considera las expectativas y necesidades de los grupos de interés externos e internos y aplica a todo el personal de la institución, quienes a su vez deben estar consciente de lo expresado en su contenido.

La Política establece los siguientes objetivos:

- Velar por la protección y seguridad de las personas dentro de las dependencias del Banco, según lo establecido en la Política de Seguridad Integral del Banco Central de Chile.
- Comunicar a todos los grupos de interés externos e internos los principios de la Continuidad de Negocios del Banco.
- Cumplir con los requerimientos legales y regulatorios aplicables al Banco.
- Proveer una estructura a través de la cual se establezca y mantenga un Sistema de Gestión de Continuidad de Negocios, el cual permita el desarrollo de planes para asegurar la continuidad a un nivel mínimo aceptable, en casos de interrupción de los sistemas.
- Mantener los planes de continuidad aptos y vigentes a través de entrenamiento, pruebas y actualizaciones periódicas.

La Política establece los siguientes principios:

- Otorgar protección y seguridad a las personas dentro de las dependencias de la Institución, según los principios establecidos en su Política de Seguridad Integral.

- Cada Gerencia a cargo de procesos críticos, cautelará y asegurará la continuidad de los productos y servicios que el Banco entrega, previniendo riesgos de interrupción o en caso de ocurrencia de ellos, evitando comprometer la misión y funciones críticas del Banco.

- Cada Gerencia debe poner énfasis en desarrollar objetivos de recuperación para aquellos servicios y procesos críticos que, en instancias de interrupciones, puedan poner en peligro la continuidad de negocios del Banco.

- Cada Gerencia debe realizar las pruebas y evaluaciones necesarias para asegurar que las acciones y planes desarrollados funcionen de manera óptima frente a situaciones de contingencia.

- Desarrollar la capacidad de comunicarse con eficacia durante un incidente que pudiese tener efectos en la continuidad operacional del Banco.

- Garantizar los canales de diálogo con los distintos grupos de interés externos e internos para conocer sus expectativas y necesidades y transmitir los compromisos del Banco.

- Proteger la imagen y reputación del Banco.

- Desarrollar competencias y proveer entrenamiento adecuado en materias de Continuidad de Negocios a su personal.

- Cumplir con los requisitos contemplados en las normas y reglamentaciones vigentes.

- Aplicar la mejora continua en el Sistema de Gestión de la Continuidad de Negocios.