LINEAMIENTOS GENERALES PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Av. Apoquindo 4001, Piso 12, Las Condes, Santiago, Chile.
Tel.: (56 2) 2393 9001
www.dcv.cl

INDICE

1. OBJETIVO

Como un soporte a su visión, misión, objetivos, productos y servicios prestados, el Depósito Central de Valores y sus filiales, en adelante DCV, se compromete y asigna una alta prioridad a sus activos de información, es por ello que se establece, documenta, implementa y se mantiene un sistema de gestión de la seguridad de la información, en adelante SGSI, con tal de proteger de la mejor forma toda la información que maneja.

Para la gestión de la seguridad de la información se establece una serie de políticas, procedimientos, estándares y lineamientos que, en su conjunto, aportan a mantener la confidencialidad, integridad y disponibilidad de la información, entregan protección ante potenciales amenazas y permiten responder y contener de manera controlada los incidentes de seguridad de la información.

2. OBJETIVOS ESPECÍFICOS

- Estructurar un marco formal con el fin de mantener la confidencialidad, integridad y disponibilidad de la información.
- Establecer una planificación con objetivos claros y medibles, para dar visibilidad a la alta administración.
- Establecer un modelo de evaluación y tratamiento de los riesgos relacionados a la seguridad de la información e implementar los controles necesarios para minimizar el impacto.
- Dar cumplimiento a regulaciones gubernamentales y contractuales que norman los servicios otorgados por el DCV desde el punto de vista de seguridad de la información.
- Promover una cultura que aumente el entendimiento, la conciencia y las responsabilidades de las personas respecto de la seguridad de la información.
- Asignar recursos para la cobertura de los riesgos detectados en seguridad de la información en cuanto al costo beneficio y a la exposición del activo de información.
- Establecer un marco de referencia que permita definir y evaluar la gestión de la información y la mejora continua del sistema.
- Establecer y mantener planes y procedimientos para detectar y responder a la ocurrencia de incidentes de seguridad, que afecte la confidencialidad, disponibilidad o integridad de la información.

3. ALCANCE

Aplica sobre los activos de información que se desarrollan y controlan bajo el sistema de gestión de seguridad de la información, y que son mantenidos por los colaboradores del DCV, personal externo y proveedores.

4. RESPONSABILIDADES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN

Del contenido de este documento, se desprende una responsabilidad básica de: implementar, mantener, y mejorar la gestión de la seguridad de la información del DCV, responsabilidad directa de las áreas que se mencionan a continuación:

Cargo	Descripción
Alta gerencia del DCV	Participación directa con el SGSI a través del comité de seguridad, comité de planificación, comité de gestión, comité de riesgo y ciberseguridad, entre otros, conformados por gerentes del DCV.
Grupo de seguridad de TI	Reuniones quincenales con generación de acuerdos, seguimientos y compromisos relacionados a temas de seguridad, gestión de excepciones, requerimientos, vulnerabilidades y brechas.
Jefe de seguridad de la información y riesgo tecnológico	Dedicación exclusiva a su función con el sistema de gestión, bajo la coordinación de la gerencia de riesgo y cumplimiento.
Oficial de ciberseguridad	Dedicación exclusiva a la gestión de ciberseguridad sobre la plataforma del DCV, bajo la coordinación de la gerencia de operaciones TI y ciberseguridad.

Para obtener más información sobre las responsabilidades ver el documento: Roles y responsabilidades SGI.

Adicionalmente, para asegurar el cumplimiento de las políticas, se establecen roles y responsabilidades específicas por cada proceso, las que requieren del compromiso de todo el personal del DCV, y de quienes se relacionan con la compañía, al objeto de crear y mantener un ambiente que permita asegurar la seguridad de la información.

5. DOCUMENTOS RELACIONADOS

- Catálogo de control maestro documental. (Documento de trabajo de control interno que identifica la evidencia documentada que deben ser mantenidos por el SGCN y el SGSI bajo las normas ISO 22301 e ISO 27001).
- Contexto de la organización.
- Alcance del SGI
- Roles y responsabilidades SGI

6. POLÍTICA GENERAL DE SEGURIDAD

El DCV cuenta con su política de seguridad de la información, la cual establece las directrices que deben cumplir los colaboradores del DCV, para proteger su información bajo los más altos estándares de seguridad.

7. PRINCIPIOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Para la gestión de seguridad de la información del DCV se contemplan los siguientes principios:

7.1 Visión del negocio

La seguridad de la información se reconoce como un atributo necesario de los servicios ofrecidos por el DCV a sus clientes, tanto en el ámbito nacional como internacional.

7.2 Responsabilidad

La organización reconoce que la sensibilización, capacitación y entrenamiento adecuados a su personal en las materias de seguridad de la información son tareas prioritarias.

7.3 Necesidad del saber

El acceso a la información debe ser de manera controlado. Tanto a los colaboradores como a procesos, se otorgan solamente los accesos necesarios para poder operar.

7.4 Ciclo de vida

Se debe resguardar y proteger la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida, esto es, desde la creación, transmisión, almacenamiento hasta su destrucción final.

7.5 Segregación funcional

Se considera necesario que las actividades críticas sean divididas en funciones que se realizan por personal o procesos independientes y/o requieran supervisión y aprobación previa.

7.6 Legislación

La organización declara cumplir con la normativa y legislación vigente en relación con aspectos de reserva y privacidad de la información de sus accionistas, clientes, colaboradores y otras partes interesadas.

7.7 Separación

Se distingue y controla la información del negocio y la información personal de los colaboradores.

7.8 Clasificación

Se requiere de un esquema de clasificación de la información y se asegura que el acceso a ésta se realiza de forma controlada y autorizada.

7.9 Riesgos

El SGSI adhiere al modelo de riesgo de la compañía, que incluye dentro de la evaluación de riesgo los ámbitos de seguridad de la información.

8. REFERENCIAS NORMATIVAS TOMADAS EN CONSIDERACIÓN PARA EL SGSI

Para la elaboración de la documentación que compone el sistema de gestión de seguridad de la información que se describe en este documento se han tomado como referencia las siguientes normas:

Referencia	Edición	Titulo
ISO/IEC 27001:2013	2013	Information technology – Security techniques – Information security management systems – Requirements (Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos).
ISO/IEC 27002:2013	2013	Information technology – Security techniques – Code of practice for information security management (Tecnología de la Información – Código de Prácticas para la Gestión de la Seguridad de la Información)
ISO/IEC 27004:2016	2016	Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation
ISO/IEC 27005:2011	2011	Information technology – Security techniques – Information security risk management (Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo de Seguridad de la Información).
ISO/IEC 31000:2009	2009	Information technology – Security techniques - Risk management - Principles and guidelines (Tecnología de la Información – Técnicas de Seguridad – Gestión de riesgos - principios y directrices).

9. OPERACIÓN DEL SGSI

El SGSI del DCV ha de definir e implementar planes de tratamiento de riesgos, así como los respectivos controles, según el grado que aplique con el objetivo de proteger los activos de información y minimizar la vulnerabilidad de estos, para lo cual se deberá establecer en políticas específicas y detalladas que definen la forma de controlar y medir la eficacia de los respectivos controles.

10. PROCESO DE GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El SGSI permite una pronta detección de eventos e incidentes de seguridad. En relación con los incidentes de seguridad de la información, el objetivo es restablecer la operación normal de los servicios tan pronto como sea posible, minimizando el impacto en las operaciones del negocio. En cuanto a los requerimientos, el objetivo es satisfacer las expectativas del cliente dentro del alcance de los servicios contratados por éste.

Para tener un mayor detalle de este proceso, se sugiere consultar el procedimiento de gestión de incidentes y requerimientos.

11. MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

El SGSI permite una evaluación de desempeño de la gestión sobre la seguridad de la información y la efectividad de la gestión implementada. Es por ello, por lo que es requerido monitorear los controles implementados y los procesos de la seguridad de la información, lo que es realizado a través de mediciones de indicadores, y también con la ejecución de las auditorías internas y externas, estas son planificadas a intervalos periódicos de revisión anuales.

12. MANTENIMIENTO Y MEJORA DEL SGSI

Producto de las revisiones y evaluación del SGSI se ha definido que cuando se identifique una desviación del sistema, se generará una no conformidad que incorpora una adecuada gestión implementando oportunidades de mejora, acciones correctivas y acciones que permitan que no vuelva a ocurrir.

La alta gerencia se encuentra comprometida con la mejora continua y asegurar la efectividad en el tiempo de su sistema de gestión de la seguridad de la información.