Código - Versión	**PL-10-CMCH Versión 09**
Vigente desde	**Octubre 2025**
Próxima Revisión	**Sujeto a cambios de acuerdo a las necesidades de la Dirección de la Empresa**
POLÍTICA INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	
PL-10-CMCH	

APROBACIÓN
Nº Sesión y fecha en que se aprueba el Directorio
Comité de Auditoría, Riesgos y Seguridad (CARS) N° 128 de fecha 28-octubre del 2025. Sesión Ordinaria del Directorio N° 196 de fecha 29-octubre del 2025.

Tabla de Contenido

1. OBJETIVO

Definir los principios y reglas generales para una adecuada protección y resguardo de los activos de información y tecnología, frente a amenazas internas o externas, deliberadas o accidentales, así como de las vulnerabilidades técnicas que pudiesen generar brechas de seguridad. También, la seguridad de la información y ciberseguridad nos permite asegurar y garantizar la continuidad operacional, determinar los recursos, resguardar la imagen y reputación de Casa de Moneda de Chile S.A. (en adelante "CMCH").

Adicionalmente, establece un esquema de seguridad de la información y ciberseguridad en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

2. ALCANCE

Esta política es aplicable a toda la organización, a los trabajadores y trabajadoras de CMCH, ya sea de planta o temporales, a honorarios, a personal externo, y proveedores, que presten servicios permanentes o temporales.

3. DEFINICIONES

- **Activo Informático**: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- **Activo de Información**: Son aquellos elementos que hacen posible o sustenten los procesos de negocios, pudiendo ser sistemas de información, personas, aplicaciones o herramientas tipo software, base de datos, equipos computacionales, equipos móviles, documentos electrónicos, o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información relevante, para los procesos de negocios de CMCH.
- **Seguridad de la información**: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esta triada de la información se define:
    - **Confidencialidad**: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
    - **Integridad**: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

- **Disponibilidad**: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

- **Ciberseguridad**: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos (por ejemplo: computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes), con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
  Se conoce también como seguridad de tecnología de la información o seguridad de la información electrónica.
- **Red y sistema informático**: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
- **CSIRT** (*Computer Security Incident Response Team*, en español "Equipo de Respuesta ante Incidentes de Seguridad Informática"): centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.
- **Incidente de ciberseguridad**: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- **Sistema de gestión de seguridad de la información (SGSI)**: Comprende los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.
- **Amenaza:** Cualquier cosa que es capaz de actuar en contra de un activo de manera que puede resultar en un daño.
- **Vulnerabilidad**: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.
- **Riesgo**: posibilidad de ocurrencia de un incidente de ciberseguridad o de seguridad de la información; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.

- **Trabajadores y Trabajadoras**: Todas las personas que trabajan en CMCH, independiente de su régimen contractual,

4. ROLES ORGANIZACIONES, RESPONSABILIDADES Y AUTORIDADES

El Gerente General es el responsable de:

- Implementar y gestionar la Política Integral de Seguridad de la Información y Ciberseguridad, como también sus modificaciones posteriores.
- Facilitar la provisión de recursos presupuestarios y humanos para el desarrollo, implementación y mantención de la Política Integral de Seguridad de la Información y Ciberseguridad.

Comité de Auditoría, Riesgos y Seguridad (CARS):

Este Comité tiene por objeto apoyar en el proceso de gestión de riesgos a los Administradores de Riesgos de Casa de Moneda de Chile, los cuales son:

- Directorio.
- Gerente General.
- Gerentes y/o Subgerentes de área.
- Oficial de Cumplimiento, o un representante designado por este.

Este Comité, dentro de otros ítems, aborda aspectos relevantes y revisión completa del “Sistema de Gestión de Seguridad de la Información y Ciberseguridad”; siendo estas instancias lideradas por el Oficial de Seguridad de la Información, acorde a requerimiento normativo (ISO 27001).

Dentro de las responsabilidades de este Comité relacionadas a la seguridad de la información y ciberseguridad están:

- Mantener y mejorar continuamente las estrategias de la empresa sobre temas de seguridad de la información y ciberseguridad, revisando periódicamente el funcionamiento del sistema de gestión y su efectividad, siendo el ciclo anual de revisión completo acorde a la norma ISO SGSI 27001:2022.
- Revisar el Plan Director de Seguridad de Información, así como el presupuesto para soportar el “Sistema de Gestión de Seguridad de la Información y Ciberseguridad”.

- Presentar los riesgos relevantes en seguridad de la información y ciberseguridad, revisar y aprobar la gestión de estos riesgos (identificación, evaluación, tratamiento, aceptación, monitoreo y comunicación de riesgos).
- Velar por la existencia, aplicación y perfeccionamiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad de CMCH (Política, Normas y Procedimientos de control, continuidad operacional, seguridad física, entre otros).
- Tomar conocimiento, analizar, aprobar y verificar la gestión del proceso de auditorías internas y externas de Seguridad de la Información y Ciberseguridad, por medio del cumplimiento del plan anual de auditoría y sus resultados.
- Velar por la actualización permanente de la Política Integral de Seguridad de la Información y Ciberseguridad, asegurando su vigencia, cumplimiento y alineación con las normativas y la legislación aplicable. Asimismo, supervisa el mantenimiento y la difusión de las medidas de protección de la información que integran el marco normativo, aplicables tanto a los activos tecnológicos como a cualquier tipo de información, independientemente de su forma o medio de conservación.
- Supervisar el cumplimiento y efectividad de los planes de continuidad del negocio relacionados con la seguridad de la información y la ciberseguridad, asegurando que contemplen adecuadamente la respuesta, recuperación y aprendizaje frente a incidentes significativos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información.

Oficial de Seguridad de la información (O.S.I.) responsable de:

- Planificación de gestión:
  - Elaborar y presentar al CARS una propuesta de planificación para la gestión del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI), asegurando su alineación con la estrategia de CMCH, y con las exigencias derivadas de su carácter de empresa pública garante de la fe pública. Dicha planificación deberá incorporar criterios de excelencia en materia de ciberseguridad, en coherencia con los estándares nacionales e internacionales que rigen a las entidades del Estado.
  - Coordinar la identificación, análisis y evaluación de los riesgos relacionados con la seguridad de la información y la ciberseguridad, incluyendo aquellos emergentes asociados a nuevas

líneas de negocio con componente digital o mediático. En este marco, el OSI deberá considerar el estatus de CMCH como Servicio Esencial y potencial Operador de Importancia Vital (OIV) conforme a la Ley Marco de Ciberseguridad N° 21.663, asegurando que los planes de tratamiento contemplen controles reforzados y mecanismos de resiliencia tecnológica y operativa.

- Definir y liderar la implantación del plan anual de difusión y sensibilización de la seguridad de la información y Ciberseguridad, con especial énfasis en los riesgos reputacionales, regulatorios y de exposición mediática derivados de la digitalización e innovación en productos de alto valor, como los vinculados al oro u otros activos estratégicos.
- Proponer oportunidades de mejora continua para la gestión del SGSI e implementación de controles, orientadas a mantener niveles de madurez acordes a las mejores prácticas de los marcos y normativas de seguridad de la información y ciberseguridad.
- Gestionar la planificación y ejecución de auditorías internas y externas al SGSI, garantizando la trazabilidad y cumplimiento de las obligaciones asociadas al marco regulatorio nacional en materia de ciberseguridad.

• Implementación:

- Velar por el desarrollo, la implementación y la operación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, asegurando su cobertura en toda la cadena de valor y procesos productivos, incluyendo aquellos digitalizados o con exposición pública.
- Asegurar el cumplimiento de los estándares normativos, leyes, reglamentos y procedimientos definidos por el CARS y por los organismos reguladores competentes en materia de seguridad y ciberseguridad, en concordancia con las disposiciones de la Ley Marco de Ciberseguridad (Ley n° 21.663), la Ley de Delitos Informáticos (Ley n° 21.459) y la Ley de Protección de Datos Personales (Vigente Ley n°19.628 y Ley n°21.719 que entra en vigencia en diciembre de 2026).
- Coordinar, controlar y monitorear la elaboración de planes de respuesta a incidentes que afecten los activos tecnológicos, información y reputación institucional de CMCH, asegurando mecanismos de contención y recuperación oportunos.

- Prevenir riesgos de fuga o manipulación indebida de información estratégica, o deteniendo o restringiendo su entrega cuando se detecten incumplimientos o riesgos significativos, y supervisando las medidas de mitigación asociadas.

- <u>Reportabilidad:</u>
  - Presentar periódicamente al CARS los resultados del SGSI, conforme a un calendario de revisión previamente definido, integrando indicadores de desempeño y madurez que reflejen el nivel de cumplimiento con las exigencias propias de un Servicio Esencial y garante de la fe pública.
  - Gestionar la implementación y documentación del proceso de revisión por la dirección al SGSI. incorporando análisis sobre los impactos de nuevas líneas de negocio digitales y la exposición mediática derivada de productos estratégicos.
  - Gestionar los reportes generados en cada etapa del proceso de auditoría al SGSI conforme a la norma ISO/IEC 27001, incluyendo el plan de auditoría, el informe final y los registros de hallazgos. Asimismo, coordinar el desarrollo, seguimiento y cierre de los planes de tratamiento derivados de no conformidades, observaciones y oportunidades de mejora, asegurando su trazabilidad y resolución oportuna. Dichos reportes deberán integrar análisis sobre el impacto potencial en la fe pública, los servicios esenciales y las líneas de negocio digital o mediáticamente expuestas, conforme a los lineamientos del CARS y las exigencias de la Ley Marco de Ciberseguridad N° 21.663.
  - Reportar incidentes significativos de seguridad de la información y ciberseguridad, y brechas que afecten activos críticos, servicios esenciales o la confianza pública, tanto al Gerente General como al CARS que puedan afectar a CMCH.
  - Informar al CSIRT sobre los incidentes significativos de manera oportuna en tiempo y forma, en conformidad a lo que indica la Ley Marco de Ciberseguridad N° 21.663, considerando su naturaleza, impacto y medidas adoptadas:
    - Plazos de notificación:
      - Alerta temprana: dentro de 3 horas desde que se detecta un incidente con potencial impacto significativo.
      - Actualización inicial: en un máximo de 72 horas, o 24 horas si el incidente afecta servicios esenciales u operadores de importancia vital.

- Informe final: en un plazo máximo de 15 días corridos desde la alerta, o el reemplazo por un informe en curso si aún no está cerrado.
- Presentación de plan de acción en no más de 7 días.
- Omisión de datos personales sensibles según la legislación vigente.
- Disponibilidad para entregar actualizaciones adicionales si el CSIRT lo solicita.
- Evaluación criteriosa del efecto significativo.
- Notificación a los afectados cuando corresponda, en los términos legales.

El Oficial de Seguridad de la Información (OSI) es el responsable principal de reportar incidentes de ciberseguridad al CSIRT de Gobierno; en su ausencia, la responsabilidad recaerá en el Jefe del Departamento de Tecnología y, en segundo término, en el Encargado de Infraestructura Tecnológica.

Propietarios de Activos de Información, responsables de:

- Coordinar con el Oficial de Seguridad de la Información la identificación, clasificación y etiquetado de los activos de información y tecnológicos, así como proporcionar la información necesaria para evaluar los riesgos asociados y apoyar en la definición de medidas de mitigación.
- Las actividades conducentes a identificación, clasificación y etiquetado de la información según su categoría (baja, media o alta criticidad), de acuerdo con lo determinado en el “Procedimiento Clasificación de Activos de Información (QP-187-SINF)”.
- Mantener la seguridad de los activos de información bajo su responsabilidad, asegurando niveles de protección proporcionales a su clasificación, criticidad y riesgos identificados en los análisis de riesgos del SGSI y controles establecidos en sus tratamientos.
- Apoyar en la implementación de los controles de seguridad de la información identificados a partir del análisis de riesgos del SGSI, con el fin de proteger los activos bajo su responsabilidad de acuerdo con su nivel de criticidad y clasificación.
- Entregar información de valor para lograr los objetivos del SGSI, los cuales se declaran por acta en el CARS.

Trabajadores y Trabajadoras:

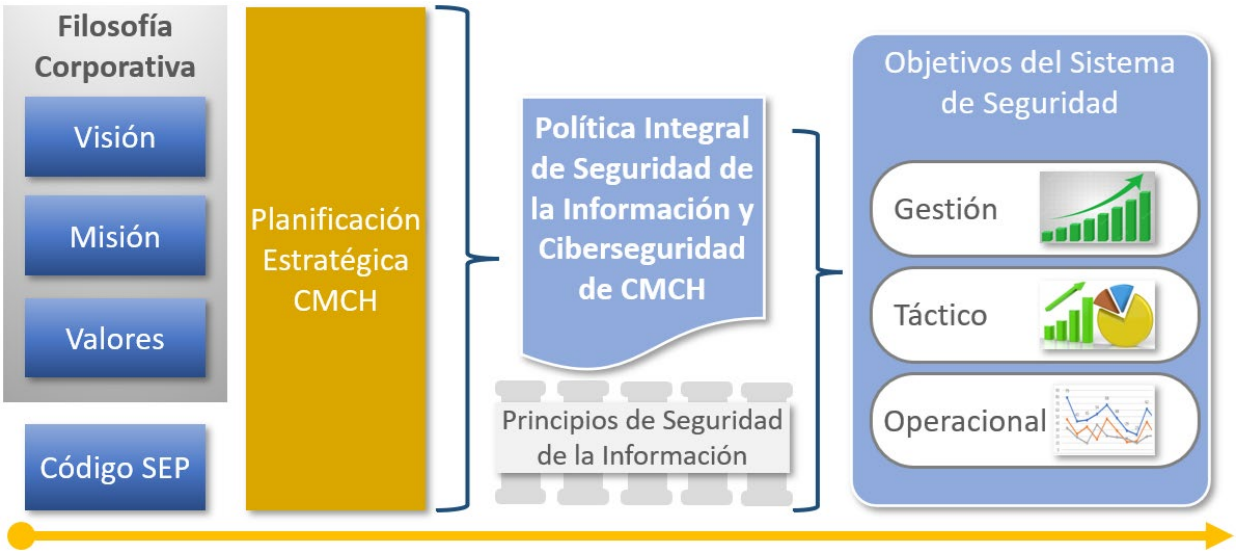
Todas las personas que trabajan en CMCH, son responsables de proteger la información y cumplir con las políticas y procedimientos de seguridad de la información y ciberseguridad. Deben utilizar los recursos tecnológicos de forma responsable, asistir a las capacitaciones, reportar incidentes, proteger sus credenciales y respetar las medidas de control del SGSI

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

CMCH demuestra su compromiso con la seguridad de la información y la ciberseguridad mediante la definición formal de la presente política seguridad de la información y ciberseguridad, y la implementación de estándares internacionales como la norma NCh-ISO/IEC 27001; esto permite proteger la confidencialidad, integridad y disponibilidad de los activos de información, cumpliendo con la normativa legal vigente:

- Ley N° 21.633, Marco de ciberseguridad.
- Ley N°19.628, Sobre protección de la vida privada.
- Ley N° 21.459, Normas sobre delitos informáticos

Por ello, la presente Política, se determina de forma coherente a partir de la planificación estratégica y objetivos de CMCH, lo mandatado por el “Código SEP”, y la visión y misión corporativa, para definir los principios de la seguridad de la información que sustentan la política de seguridad de la información y ciberseguridad. A partir de la presente política integral, se define el marco de trabajo para la determinación de los objetivos de seguridad de la información. De acuerdo con lo expuesto su ciclo se visualiza:



5.1. Principios y acciones de la Seguridad de la Información y Ciberseguridad.

Para el cumplimiento de los objetivos del sistema de gestión de seguridad de la información y ciberseguridad (en su conjunto organizado de políticas, procedimientos y controles), se han establecido los siguientes principios, los cuales son presentados a la Administración Superior de CMCH por medio del CARS:

1. La Seguridad de la Información y Ciberseguridad de los activos de información, es responsabilidad de todos los trabajadores y trabajadoras, independientemente de su cargo, así como también de las partes externas interesadas. Para efectos de esta Política, se entiende por partes externas interesadas a proveedores, contratistas, subcontratistas, socios comerciales, prestadores de servicios tecnológicos, operadores logísticos, consultores, clientes digitales y autoridades regulatorias que accedan o gestionen activos de información o servicios críticos de CMCH. Su responsabilidad se exigirá mediante contratos y acuerdos de seguridad. Los detalles operativos se registran en el documento controlado **“**Matriz de Contexto de la Organización, RG-808-GSI”.

2. La Administración Superior de CMCH se compromete con la atención efectiva y responsable de los incidentes de seguridad de la información y ciberseguridad, por medio de procesos formales de tratamiento de mitigación (identificación, análisis, respuesta y resolución),

garantizando el cumplimiento legal, informando al CSIRT sobre los incidentes significativos de manera oportuna, en tiempo y forma como exige la ley.

3. Todo trabajador y trabajadora, personal externo o proveedor, debe acceder exclusivamente a la información que le sea necesaria para el cumplimiento de sus funciones laborales y dar estricto cumplimiento a las reglamentaciones, políticas y normas internas. Para garantizar este principio, el OSI liderará un plan de acción que incluye: revisión periódica de accesos según roles, monitoreo y registro de accesos, programas de concientización y capacitación, y auditorías internas con seguimiento de desviaciones y medidas correctivas.

4. Todo trabajador y trabajadora de CMCH, debe cumplir con la normativa y legislación vigente relacionada a la seguridad de la información y ciberseguridad. El incumplimiento de estas normas y legislación, por parte de personas que trabajan en CMCH, puede tener consecuencias legales, administrativas, contractuales, operacionales y personales, las que se agravan debido al carácter crítico y estratégico de CMCH.

Acciones de apoyo a los principios:

1. Identificar, clasificar, evaluar su criticidad, etiquetar y proteger adecuadamente, los activos de información, con el fin de asegurar su confidencialidad, integridad y disponibilidad.

2. Identificar y evaluar los riesgos de seguridad de la información de forma periódica con el fin de implementar los controles, y tratar los riesgos que permitan proteger los activos de información.

3. Promover y determinar estrategias y planes que aseguren la gestión de los procesos para continuidad operacional del negocio.

4. Implementar las medidas de seguridad de información y ciberseguridad comprometidas, ya sean tecnológicas, administrativas y/o legales, declarados en los tratamientos de las matrices de riesgos y en la “Declaración de Aplicabilidad” con atención a los recursos presupuestados.

5. Promover la cultura organizacional de seguridad de la información y ciberseguridad e impresión, para que sean conscientes, competentes e informados los trabajadores y trabajadoras, a través de la sensibilización, entrenamiento y capacitación.

6. Mejorar de manera continua nuestros procesos de gestión y operación de seguridad de la información y ciberseguridad, con mediciones, evaluaciones y auditorias tecnológicas y administrativas permanentes, que aseguren la gestión y el adecuado control de estas.

5.2. Declaración de la Política de la Seguridad de la Información y Ciberseguridad de Casa Moneda de Chile S.A.

"Casa de Moneda de Chile SA, para sus procesos de negocio, activos tecnológicos y sistemas de información que soportan las unidades organizacionales en diseño, elaboración, impresión de billetes y acuñación de monedas, fabricación y personalización de tarjetas, reconoce que el activo más valioso es la información para la continuidad del negocio; por lo que se compromete la protección de la confidencialidad, integridad y disponibilidad de los activos tecnológicos y de información, asignando recursos económicos, humanos y tecnológicos, promoviendo cultura participativa hacia el empoderamiento en seguridad de la información, ciberseguridad e impresión de documentos, en cada trabajador, trabajadora, y partes interesadas.

Por ello, Casa de Moneda de Chile SA, para evitar interrupciones de procesos críticos de negocio como consecuencia de incidentes, gestiona, planifica, implementa, verifica y mejora continuamente sus procesos, así como de forma proactiva implementa la gestión de riesgos asociados. Ello, con la finalidad de alcanzar los objetivos propuestos satisfaciendo los requerimientos de las partes interesadas, en apego a la normativa y legislación aplicable.

5.3. Objetivo y compromiso de Ciberseguridad

La ciberseguridad en CMCH tiene como objetivo proteger los activos de información frente a posibles ciberataques que afecten su infraestructura tecnológica. Esta infraestructura incluye:

- Infraestructura de red y comunicaciones que sustentan los servicios y procesos productivos, incluyendo firewalls, switches, routers, software de red, servicios en la nube y el entorno digital (ciberespacio).
- Plataformas, aplicaciones, software, sistemas operativos y bases de datos.
- Equipos físicos como servidores, computadores, notebooks, impresoras, escáneres, dispositivos móviles, terminales industriales y periféricos.

Este listado se puede ampliar según la evolución tecnológica y las necesidades de protección de la organización.

Por ello la Administración Superior de CMCH, gestiona activamente la estructura de gobierno corporativo, supervisa de forma planificada el estado general del programa de seguridad de la información y ciberseguridad, asignando los recursos y lineamientos necesarios para el cumplimiento de sus objetivos. El Directorio y la Gerencia desempeñan funciones diferenciadas en la gobernanza del Sistema de Gestión de Seguridad de la Información y Ciberseguridad:

- El Directorio cumple un rol de supervisión estratégica, velando por la alineación del Plan Director **de Seguridad de la Información y Ciberseguridad** — documento que define la planificación, prioridades y metas estratégicas del programa — con los objetivos institucionales del SGSI, el cumplimiento normativo y los niveles de riesgo que la organización está dispuesta a aceptar (“*apetito de riesgo”*). Asimismo, aprueba normas, políticas y estándares relevantes y promueve la mejora continua del modelo de gobernanza.
- La Gerencia, por su parte, implementa y gestiona operativamente la estrategia de seguridad de la información y ciberseguridad, asegurando su ejecución efectiva, la disponibilidad de recursos y correcta aplicación de controles técnicos y administrativos, en línea con las directrices del Directorio; gestiona los recursos necesarios para la operación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información y ciberseguridad.

6. REVISION Y ACTUALIZACION DE LA POLITICA

La política es revisada de forma anual y los criterios a considerar para su revisión son:

- Alineación de la Política con las directrices del Directorio en temas de ciberseguridad y seguridad de la información.
- Modificaciones importantes en legislación, reglamentos, instrucciones, decretos, normativas ISO y/o Código SEP en temas de ciberseguridad y seguridad de la información que tengan impacto significativo en CMCH.
- Cambios significativos en la organización que impacten en el Sistema de Gestión de Seguridad de la Información implementado.

En los casos que existan modificaciones de esta política, deberán ser aprobados por el Directorio.

7. APROBACION

Esta Política es aprobada por el Directorio de CMCH. El Gerente General liderará su implementación y dispondrá de los recursos necesarios, aprobados por el Directorio, en las partidas presupuestarias correspondientes.

8. DIFUSIÓN Y CONOCIMIENTO DE LA POLITICA

La versión vigente de esta política está disponible para los trabajadores y trabajadoras y otras partes interesadas en el Sistema de Gestión Documental (SGD) de CMCH. Adicionalmente, se desarrolla un plan de sensibilización, divulgación, concientización y capacitación en “seguridad de la información y ciberseguridad”, así como en técnicas de ciber-higiene a los trabajadores y trabajadoras de CMCH.

9. CONTROL DE VERSIONES

Nº MOD.	APROBÓ				OBSERVACIONES
	FECHA	NOMBRE	CARGO	FIRMA	
01	01/2016	Juan Ramírez	Gerente Seguridad Integral		
02	10/2016	Juan Ramírez	Gerente Seguridad Integral		
03	05/2018	Juan Ramírez	Gerente Seguridad Integral		
04	02/2020	Juan Ramírez	Gerente Seguridad Integral		
05	05/2021	Juan Ramírez	Gerente Seguridad Integral		
06	07/2023	Juan Ramírez	Gerente Seguridad Integral		Se actualizan roles. Se incorpora la estructura en la cual se sustenta la Política, así como se incorpora su declaración.
07	12/2023	Juan Ramírez	Gerente Seguridad Integral		Se incorpora políticas de alto nivel relacionadas a la Seguridad Tecnológica y Ciberseguridad.
08	08/2024	Juan Ramírez	Gerente Seguridad Integral		Ratificación de la política frente al CARS y Directorio.
09	Jul./2025	Carlos Tolosa	Gerente General		- Se discrimina entre “Principios” y “Acciones de apoyo a los principios. - Mejora de redacción general el documento. - Se actualiza y describe en apego a la Ley 21.663. - Se especifica el CARS, describiendo responsabilidades y composición para el “Sistema de Gestión de Seguridad de la Información”. - Se discriminan funciones generales entre Directorio y la Gerencia.