P-MPD-CCL-02	
Política de Ciberseguridad y Seguridad de la Información	Aplica a: CICAL SpA.

POLÍTICA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 2026

P-MPD-CCL-02	CICAL UNA EMPRESA REMA TIP TOP CHILE
Política de Ciberseguridad y Seguridad de la Información	Aplica a: CICAL SpA.

Contenido

1. Introducción **3**

2. Objetivo **3**

3. Alcance y ámbito de aplicación **4**

4. Documentos de Referencia **5**

5. Definiciones **5**

6. Roles y responsabilidades **6**

7. Política de Seguridad de la Información **7**

7.1 *Deberes de los colaboradores* **7**

7.2 *Aplicación respecto de terceros* **8**

7.3 *Directrices* **8**

7.3.1 *Respecto a la seguridad de la información* **8**

7.3.2 *Respecto de la Ciberseguridad* **9**

7.3.3 *Compromisos según esta Política* **10**

7.3.4 *Consecuencias del incumplimiento* **11**

7.3.5 *Protección de activos* **11**

8. Dudas y consultas **12**

9. Tabla de Cambios **12**

P-MPD-CCL-02	
Política de Ciberseguridad y Seguridad de la Información	Aplica a: CICAL SpA.

1. Introducción

En la era digital, la seguridad de la información se ha convertido en un aspecto fundamental para la protección de la información y los recursos tecnológicos de las organizaciones.

Las crecientes amenazas cibernéticas, el mal uso de los dispositivos, poco conocimiento sobre riesgos como el malware, el phishing, los ataques de ransomware y otros tipos de intrusiones, representan un riesgo significativo no solo para la infraestructura tecnológica, sino también para la reputación y el rendimiento operativo de las empresas. Por esta razón, es crucial adoptar un enfoque integral que permita anticipar, identificar y responder de manera efectiva a posibles incidentes de seguridad.

La transformación digital ha ampliado la superficie de ataque, exponiendo a las organizaciones a un entorno de amenazas cada vez más sofisticado y en constante evolución. En este escenario, la ciberseguridad no se limita únicamente a la protección técnica, sino que implica una cultura de conciencia y responsabilidad compartida entre todos los miembros de la organización.

2. Objetivo

La Política de Seguridad de la Información de CICAL Chile SpA. ha sido desarrollada con el objetivo de establecer un marco de acción que guíe a todos los colaboradores en la implementación de medidas preventivas y reactivas frente a los riesgos cibernéticos y fugas de información sensible de la compañía o de terceros.

Esta política proporciona directrices claras para el manejo seguro de la información y los sistemas tecnológicos, definiendo roles y responsabilidades, así como procedimientos y buenas prácticas de seguridad.

La adopción de estas medidas contribuye a minimizar la exposición a incidentes de seguridad y a salvaguardar la confianza de los clientes, socios, colaboradores y otros actores relevantes. Al adherirse a esta política, CICAL Chile SpA. reafirma su compromiso con la protección de su entorno digital y el cumplimiento de las normativas de seguridad aplicables.

3. Alcance y ámbito de aplicación

Lo definido en esta política aplica a todos los colaboradores de la empresa, cualquiera sea el cargo que desempeñen.

Alcanza a los colaboradores externos y a los proveedores que entreguen servicios a CICAL Chile SpA.

Es aplicable a cualquier persona o institución que tenga acceso permanente o temporal a la información e infraestructura tecnológica que dispone CICAL Chile SpA. para sus servicios, procesos en el ciberespacio o en sus activos fijos.

Junto con ello, involucra toda la información y activos tecnológicos de tratamiento de información de la empresa y las plataformas externas en las que CICAL Chile SpA. procese o almacene su información.

4. Documentos de Referencia

- Código de Ética y Conducta de la Organización
- Ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos que indica
- Reglamento Interno de Orden, Higiene y Seguridad

5. Definiciones

a) **Empresa CICAL Chile SpA**.: Se refiere a la sociedad matriz, no incluyendo filiales.

b) **Colaborador**: Es toda persona que tenga un vínculo contractual laboral con CICAL Chile SpA., sea éste de carácter indefinido, a plazo fijo o a honorarios.

c) **Política**: Corresponde a una orientación general o directriz expresada formalmente por CICAL Chile SpA.

d) **Seguridad de la Información:** Se encarga de proteger la confidencialidad, integridad y disponibilidad de la información, tanto en formato digital como físico. La seguridad de la información se ocupa de los activos de información de una organización, como datos confidenciales, propiedad intelectual y secretos comerciales.

e) **Ciberseguridad:** Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de estos y del daño causado antes, durante y después de su ocurrencia.

f) **Amenaza**: Es la causa de un incidente no deseado, el cual podría ocasionar un daño a un sistema o una empresa.

g) **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

h) **Información confidencial:** Para CICAL Chile SpA., será considerada como información de carácter confidencial, la siguiente:

- Información de clientes, proveedores y accionistas.
- Clientes potenciales y datos relacionados con las ventas.
- Patentes, procesos de negocio y/o nuevas tecnologías.
- Contraseñas, asignaciones e información personal de los colaboradores.
- Contratos de empresa y registros legales.

i) **Riesgo**: Combinación de la probabilidad de un suceso y de su ocurrencia.

j) **Terceros**: Aquellas personas o entidades que están reconocidas como independientes de las partes implicadas para el asunto en cuestión.

6. Roles y responsabilidades

- **Gerencia General**:
  a) Aprobar y supervisar la implementación de esta política.
  b) Asignar recursos necesarios para su cumplimiento.

- **Departamento de Personas**:
  a) Implementar y gestionar esta política.
  b) Desarrollar procedimientos que aseguren la prevención de riesgos.
  c) Realizar capacitaciones periódicas en temas de ética, compliance y prevención de delitos.
  d) Velar por el cumplimiento de la normativa y ética en los procesos que involucren infraestructura tecnológica y su información.

- **Oficial de Cumplimiento**:
  a) Asesorar al área de Personas en la correcta aplicación de esta política.
  b) Resolver dudas y consultas relacionadas con la presente política.
  c) Monitorear y evaluar la efectividad de las medidas implementadas.
  d) Informar a la Alta Dirección sobre posibles riesgos y situaciones críticas.

- **Colaboradores**:
  a) Cumplir con las disposiciones de esta política.
  b) Reportar cualquier situación que pueda implicar un riesgo o vulneración de la normativa interna o externa.

7. Política de Seguridad de la Información

CICAL Chile SpA. en cumplimiento de su objetivo en materia de Seguridad de la Información ha establecido los siguientes deberes:

7.1 Deberes de los colaboradores

Todo colaborador que forme parte de la empresa tiene el deber de contribuir proactivamente a la seguridad de la información, respetando y cumpliendo las políticas, procedimientos y normas, así como también comprendiendo el contenido y alcance de ellas.

7.2 Aplicación respecto de terceros

Las políticas de seguridad de la información y ciberseguridad se darán a conocer y se exigirán a terceros con quienes CICAL Chile SpA. se relacione, sean estos clientes o proveedores, incorporándose las cláusulas pertinentes en los contratos respectivos.

7.3 Directrices

7.3.1 Respecto a la seguridad de la información

La información de la empresa y de sus colaboradores, debe ser tratada de forma ética y de manera prudente, en consonancia con la legislación vigente y normativa interna de la empresa, evitando su mal uso y exposición indebida.

Además, cualquier información obtenida, se debe utilizar de manera transparente y según la finalidad para la cual se obtuvo.

El acceso a las informaciones y recursos sólo se debe realizar si está autorizado por el dueño del proceso. Por ello, es que la identificación de cualquier colaborador debe ser única, personal e intransferible, siendo responsable por todas las acciones realizadas.

Las claves entregadas por la empresa son secretas y no deben ser compartidas por otros colaboradores ni respeto de terceros.

Se prohíbe la descarga mediante cualquier formato de la información en cualquier dispositivo que no sean de los propios de la empresa y que no haya sido previamente autorizado por escrito por la Jefatura directa con copia a Gerencia General.

7.3.2 Respecto de la Ciberseguridad

La creciente adopción de tecnologías plantea desafíos significativos en materia de seguridad. Es fundamental prevenir riesgos como la fuga de información, los ciberataques y los fraudes informáticos, que no solo podrían comprometer servicios críticos, sino también impactar a los grupos de interés relacionados con la empresa.

Debido a lo anterior, es que CICAL Chile SpA. y su compromiso con la gestión de la seguridad de la información, ha impulsado iniciativas que aseguren un enfoque más robusto y proactivo.

CICAL Chile SpA., se compromete y responsabiliza a:

a) Implementar la política y marco normativo de Ciberseguridad y Seguridad de la información, asegurándose que sus dependientes cumplan los mismos.

b) Identificar y evaluar los riesgos relacionados con ciberseguridad y seguridad corporativa, implementar acciones para remediar vulnerabilidades y garantizar la

detección, comunicación, resolución o mitigación de eventos que afecten la seguridad de los activos.

c) Gestionar y mantener actualizado el inventario de los activos tecnológicos vinculados a los procesos de CICAL Chile SpA.

d) Proteger los activos de la compañía asegurando el cumplimiento de la normativa vigente y los compromisos asumidos con terceros

7.3.3 Compromisos según esta Política

a) Cumplir con el marco normativo establecido, que incluye normas, procedimientos, estándares de seguridad, instructivos y recomendaciones derivadas de esta Política, aplicable a todos los integrantes de CICAL Chile SpA.

b) Participar activamente en el plan de capacitación y concientización sobre seguridad de la información.

c) Establecer y ejecutar procesos eficientes para la gestión de la seguridad, alineados con la gestión de riesgos corporativa y basados en estándares y mejores prácticas reconocidas por la industria.

d) Colaborar con organizaciones y entidades externas para desarrollar controles efectivos contra riesgos.

e) Realizar investigaciones internas necesarias para esclarecer incidentes de seguridad o posibles incumplimientos al Código de Ética y Conducta, garantizando objetividad,

confidencialidad, exhaustividad, relevancia, precisión y oportunidad. Los hallazgos deberán ser reportados a las instancias correspondientes.

f) Toda vez que sea plausible y necesario, se deben realizar las actividades de revisión de los pasos realizados para resolver un incidente de Ciberseguridad.

7.3.4 Consecuencias del incumplimiento

El incumplimiento de esta Política, así como de las normas, procedimientos y estándares relacionados con Ciberseguridad y Seguridad Corporativa, implica riesgos para los activos de CICAL Chile SpA. y puede conllevar sanciones disciplinarias o medidas judiciales en los ámbitos administrativo, laboral, civil o penal.

7.3.5 Protección de activos

La negligencia en la protección de los activos ya sea por acción u omisión, que resulte en robo o divulgación de información, será considerada equivalente a un fraude económico. Dichas situaciones serán elevadas al área respectiva para evaluar responsabilidades y su impacto fiduciario.

8. Dudas y consultas

Cualquier duda, consulta o solicitud de aclaración relacionada con esta política debe ser dirigida al **Oficial de Cumplimiento** a través del correo oficialdecumplimiento@rema-tiptop.cl o mediante comunicación directa en horario laboral.

9. Tabla de Cambios

Versión	Fecha	Descripción del Cambio	Responsable del Cambio	Aprobación
1.0	10 de abril de 2026	Creación del documento	Oficial de Cumplimiento	Gerencia General

Este documento es parte integrante del **Modelo de Prevención de Delitos** y debe ser revisado periódicamente para garantizar su vigencia y adecuación a las normativas legales y necesidades organizacionales.