RESUMEN EJECUTIVO DE

LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DE LA CORPORACIÓN DE AYUDA AL NIÑO QUEMADO (COANIQUEM)

Octubre 2025

COANIQUEM
todo por el niño quemado

La Política de Seguridad de la Información de la Corporación de Ayuda al Niño Quemado (COANIQUEM) es el marco institucional esencial para la protección de sus activos de información. Su propósito fundamental es garantizar la Confidencialidad, Integridad, y Disponibilidad de los datos que maneja la organización, ya sean internos o compartidos con terceros.

1. INTRODUCCIÓN Y COMPROMISO

COANIQUEM reconoce que la información es un activo estratégico crucial para su misión y correcto funcionamiento. Por ello, la institución establece medidas rigurosas para asegurar su protección en cualquier medio donde se registre, utilice, almacene, procese o transmita. El cumplimiento de estas medidas es obligatorio, y su inobservancia puede acarrear responsabilidades administrativas, civiles y penales, conforme al marco jurídico vigente.

2. OBJETIVOS Y ALCANCE

2.1 OBJETIVO PRINCIPAL

Asegurar la confidencialidad, integridad y disponibilidad de la información de COANIQUEM.

2.2 OBJETIVOS ESPECIFICOS

a) Gobernanza: Definir los roles y responsabilidades para una gestión efectiva del riesgo de seguridad de la información.
b) Cumplimiento legal: Asegurar que las acciones cumplan con las normativas de seguridad de la información.
c) Capacitación: Promover la formación continua de los colaboradores en la gestión de la seguridad de la información.
d) Protección: Implementar controles físicas y tecnológicas adecuadas para evitar accesos no autorizados.
e) Mejora continua: Establecer un ciclo de revisión y perfeccionamiento constante de la gestión de la seguridad de la información.

2.3 ALCANCE

Esta política se aplica a todos los procesos de COANIQUEM, incluidas la dirección, gestión, operación, investigación, supervisión y apoyo, y abarca a todo el personal de la Corporación, incluyendo colaboradores, socios, contratistas, proveedores y asesores que manejen activos informáticos de la organización.

3. DOCUMENTOS DE REFERENCIA

Se toman como base diversas leyes y normativas, entre las que destacan:

a) Ley N° 21.663: Ley Marco de Ciberseguridad.
b) Ley N° 21.459: Normas sobre delitos informáticos.

c) Ley N° 19.628: Protección de la vida privada y datos personales.
d) Ley N° 17.336, octubre de 1970, sobre Propiedad Intelectual, Ministerio de Educación y su Reglamento
e) Decreto Supremo N° 83, del 03/06/2004 del Ministerio Secretaría General de la Presidencia.
f) Ley N° 19.799 del año 2002, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma y su Reglamento.
g) Norma NCh-ISO 27000:2018, Sistemas de Gestión de la Seguridad de la Información – Visión general y vocabulario.
h) Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información – Requisitos.

4. DEFINICIONES

Se establecen definiciones clave para entender los términos utilizados en la política. Algunos de los conceptos más importantes son:

a) Activo informático: Cualquier información almacenada en un sistema informático que tenga valor para COANIQUEM.
b) Ciberataque: Intento de destruir, exponer, alterar o utilizar de manera no autorizada un activo informático.
c) Confidencialidad: Propiedad que garantiza que la información solo está disponible para individuos o procesos autorizados.
d) Disponibilidad: Asegurar que la información esté accesible cuando sea requerida.
e) Incidente de ciberseguridad: Evento que afecta la confidencialidad, integridad o disponibilidad de la información.

5. ROLES Y RESPONSABILIDADES

La implementación de la esta política se estructura a través de roles clave:

- Comité Ejecutivo de Seguridad de la Información: Responsable de la elaboración, revisión y modificación de la política, y de tomar decisiones sobre incidentes que afecten la seguridad de la información.
- Comité Técnico de Seguridad de la Información: Órgano asesor del Comité Ejecutivo, encargado de desarrollar y aplicar estrategias relacionadas con la seguridad de la información.
- Gerente de Sistemas y Procesos: Responsable de la actualización y gestión de la política, así como de la capacitación técnica en temas de seguridad informática.
- Delegado de ciberseguridad: Punto de contacto con la Agencia Nacional de Ciberseguridad, encargado de informar sobre incidentes relevantes.

6. DESCRIPCIÓN DEL DOCUMENTO

La política establece directrices claras para la protección de la información y define los estándares y controles que deben ser adoptados por la organización. A continuación, se destacan algunos de los puntos clave:

- La información es un activo estratégico, y su protección es responsabilidad de todos los colaboradores.
- Los colaboradores deben alertar ante cualquier evento o incidente que pueda comprometer la seguridad de la información.
- COANIQUEM asignará los recursos necesarios para implementar y desarrollar estrategias efectivas de seguridad.
- El acceso a la información puede ser restringido para usuarios externos, y se podrán tomar medidas administrativas o contractuales ante incumplimientos de la política.

7. CLASIFICACIÓN DE LA INFORMACIÓN

La política establece que la información debe clasificarse según su nivel de confidencialidad:

- Información pública: De acceso general, como indicadores de atención o técnicas de tratamiento.
- Información de uso interno: Limitada al personal de COANIQUEM.
- Información confidencial: Restringida a aquellos colaboradores que la necesiten para cumplir con sus funciones.

8. SEGURIDAD FÍSICA Y ACCESO

COANIQUEM implementará controles rigurosos sobre el acceso a la información, tanto en formato físico como digital. Algunas de las medidas incluyen:

- Utilización de credenciales de identificación por parte de los colaboradores.
- Restricción de acceso a áreas sensibles, como oficinas donde se maneje información confidencial.
- Control de acceso a servidores, centros de datos y equipos de comunicación.
- Ubicación estratégica de puestos de trabajo para evitar el acceso no autorizado a documentos físicos o digitales.

9. SISTEMAS Y CIBERSEGURIDAD

La política también aborda la protección de los sistemas de información. Entre las medidas propuestas se destacan:

- Implementación de cortafuegos y sistemas de detección de intrusiones (IDS).
- Realización de pruebas de vulnerabilidad para detectar y corregir debilidades en los sistemas.
- Supervisión constante de las redes para identificar actividades sospechosas.
- Documentación de todos los incidentes de seguridad para mejorar la respuesta ante futuros eventos.

10. NOTIFICACIONES Y DENUNCIAS

Todo el personal, proveedores y colaboradores deben notificar cualquier evento que pueda representar una amenaza para la seguridad de la información. Estas notificaciones deben realizarse de forma inmediata al superior directo y al canal de denuncias de COANIQUEM. La

política también hace referencia al Manual de Prevención de Delitos, que contiene más información sobre el uso del canal de denuncias.

11. DIFUSIÓN Y REVISIÓN

La política fue difundida entre todos los colaboradores y estará disponible un resumen en la web institucional de COANIQUEM. Se llevarán a cabo otras acciones de comunicación interna para asegurar que todos los empleados comprendan sus responsabilidades en materia de seguridad de la información. Además, la política será reevaluada cada año o cuando se produzcan cambios significativos en la organización, con el objetivo de asegurar su vigencia y efectividad continua.

12. CONCLUSIÓN

En resumen, la Política de Seguridad de la Información de COANIQUEM establece un marco integral y robusto para proteger la información crítica de la organización, tanto en términos de seguridad física como digital. Define claramente las responsabilidades de todos los colaboradores, establece medidas preventivas y correctivas, y asegura el cumplimiento de las leyes y normativas aplicables. Su correcta implementación garantizará que COANIQUEM pueda cumplir con su misión de forma segura, minimizando los riesgos asociados a la gestión de la información.