Aprueba versión actualizada de la Política de Seguridad y Ciberseguridad de la Información.

**RESOLUCIÓN EXENTA N° 365/ 2026**

Concepción, 16 de abril de 2026.

**VISTOS:**

La Ley Nº17.995, de 8 de mayo de 1981, publicada en el Diario Oficial de la misma fecha, que crea la Corporación de Asistencia Judicial de la Región Biobío, Decreto con Fuerza de Ley Nº994, de fecha 16 de julio de 1981, publicados en el Diario Oficial de 21 de septiembre del mismo año, que aprueba los Estatutos de la Corporación, las atribuciones del Director/a General, establecidas en el artículo 19 de los Estatutos de la Corporación, 12 y 27 del Reglamento Interno de esta Corporación de Asistencia Judicial; La Ley 19.913, que crea la Unidad de Análisis Financiero, para prevenir el lavado de activos y el financiamiento del terrorismo, incluyendo delitos base como cohecho, malversación y fraude al fisco; La Ley 20.393 que establece responsabilidad penal para personas jurídicas por delitos de corrupción y lavado de activos; Artículos 11 y 12 de la Ley N°19.880 sobre principios de imparcialidad, probidad y deber de abstención de autoridades y funcionarios; y, Art. 16 sobre principios de transparencia y publicidad; La Ley N°18.575 Orgánica Constitucional de Bases de la Administración del Estado en sus Art. 52 a 64, que establece el principio de probidad administrativa, incompatibilidades y prohibiciones y declaración de intereses y patrimonio; el Art. 8° de la Constitución Política de la República; y, la resolución 36 de 2024 de la Contraloría General de la República.

**CONSIDERANDO:**

1. Que, la Corporación de Asistencia Judicial de la Región del Biobío es una institución pública creada por la Ley N°17.995, y que se encuentra sujeta, en el cumplimiento de sus funciones, a las disposiciones constitucionales y legales que rigen la actuación de los órganos de la Administración del Estado.

2. Que, el artículo 8°, inciso primero, de la Constitución Política de la República, establece que el ejercicio de las funciones públicas obliga a sus titulares a dar estricto cumplimiento al principio de probidad en todas sus actuaciones, el cual, en conformidad con el artículo 52, inciso segundo, de la ley N°18.575, consiste en observar una conducta funcionaria intachable y un desempeño honesto y leal de la función o cargo, con preeminencia del interés general sobre el particular. El artículo 53 de la misma ley dispone que el interés general se expresa, entre otros,

MJTS

en lo razonable e imparcial de las decisiones de las autoridades; en la rectitud de ejecución de las normas, planes, programas y acciones, y en la integridad ética y profesional de la administración de los recursos públicos que se gestionan.

3. Que, el Documento Técnico N°70 Versión 0.4-2026 sobre la Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público, documento que tiene como principal objetivo facilitar a las organizaciones gubernamentales, la implementación y cumplimiento del proceso de gestión de riesgos, así como su mantención y mejora continua.

4. Que, la Política de Seguridad y Ciberseguridad de la Información, fue puesta a disposición de los Directores (as) Regionales, Directores (as) de Área y las Asociaciones de Funcionarios (as), conforme al principio de revisión participativa.

5. Que, habiendo finalizado el plazo para la presentación de observaciones a los documentos por parte de los Directores (as) Regionales, Directores (as) Área y las Asociaciones de funcionarios (as), y en cumplimiento del principio de revisión participativa, corresponde aprobar formalmente los documentos.

6. Que, dentro del plazo establecido, no se recibieron observaciones ni comentarios a los documentos sometidos a revisión participativa.

**RESUELVO:**

I. **APRÚEBASE** la versión actualizada de la Política de Seguridad y Ciberseguridad de la Información, que contiene las modificaciones introducidas y cuyo texto es del siguiente tenor:

# Política de Seguridad y Ciberseguridad de la información

## CORPORACIÓN DE ASISTENCIA JUDICIAL REGIÓN BIOBÍO

## Objetivo

Esta política tiene como propósito establecer un marco normativo integral para la gestión segura de la información dentro de la institución. Su objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de los datos, en especial aquellos considerados críticos y sensibles, mediante la implementación de medidas de protección avanzadas, la formación continua de los funcionarios (as) y la adopción de estrategias de respuesta ante riesgos cibernéticos, contribuyendo a la protección de los activos de información y al cumplimiento de los objetivos institucionales, incorporando un enfoque basado en riesgos.

Este documento abarca todos los ámbitos de la organización, incluyendo los sistemas de información, infraestructura tecnológica, activos digitales, personal interno y externo, así como empresas contratistas y proveedores de servicios, en la medida que gestionen o accedan a activos de información institucional.

La aplicación de esta política busca prevenir la pérdida, alteración o acceso no autorizado a la información, asegurando su protección y disponibilidad para quienes estén debidamente autorizados. Para ello, se establecen las siguientes directrices fundamentales:

- Se fomentará una cultura organizacional orientada hacia la seguridad de la información, promoviendo buenas prácticas en el manejo de datos.
- Se definirán responsabilidades individuales y colectivas en la gestión y protección de la información institucional.
- Se implementarán controles técnicos y procedimientos operativos que refuercen la seguridad de los activos de información.
- Se proporcionarán herramientas y recursos para que el personal pueda tomar decisiones informadas en materia de ciberseguridad.
- Se establecerán mecanismos de monitoreo y respuesta para la detección y mitigación de amenazas digitales.
- Se desarrollarán planes de contingencia que permitan la recuperación eficiente de los datos en caso de incidentes de seguridad.

## Alcance

Esta política es de aplicación obligatoria para todos los funcionarios (as) de la institución, sin importar su cargo o tipo de contrato. Asimismo, se extiende a los proveedores y prestadores de servicios que manejen información institucional. Además, se aplica a:

- Todos los sistemas de información, redes de comunicación, dispositivos tecnológicos y plataformas digitales utilizadas en la institución.
- Todos los activos de información institucional, sin importar su formato o soporte.
- Toda información impresa, electrónica, audiovisual y cualquier otro medio de transmisión de datos.
- Todas las operaciones realizadas en entornos digitales, incluyendo almacenamiento, transacciones electrónicas y accesos remotos, considerando especialmente aquellos sistemas y activos de información definidos como críticos para la institución.

## Vigencia y Periodicidad de Evaluación y Revisión de la Política

La presente política entrará en vigencia a contar de la fecha de su aprobación y tendrá una duración de dos años. La presente Política de Seguridad y Ciberseguridad de la Información entrará en vigencia a contar de la fecha de su aprobación y tendrá una duración de dos años.

Será revisada por el Comité de Riesgos y actualizada por el Coordinador de Riesgos al término de dicho período, o de manera anticipada si se producen cambios relevantes en el entorno tecnológico, normativo o institucional que así lo requieran.

La presente versión corresponde al período 2026–2027, reemplazando versiones anteriores, e incorpora mejoras en concordancia con el Documento Técnico N°70 versión 0.4 del Consejo de Auditoría Interna General de Gobierno (CAIGG) y demás lineamientos aplicables en materia de seguridad de la información.

## Responsabilidades

Director/a General:

- Asignar recursos adecuados para la seguridad de la información.
- Fomentar una cultura organizacional de seguridad de la información y gestión de riesgos en toda la institución.
- Aprobar las políticas, estándares y procedimientos de seguridad de la información de acuerdo con las regulaciones y políticas vigentes.

Director (a) de Gestión Estratégica:

- Desarrollar, implementar y mantener políticas y procedimientos de seguridad de la información de acuerdo con las regulaciones y estándares pertinentes.

Encargado (a) de Transformación Digital:

- Coordinar la gestión y respuesta a incidentes de seguridad de la información, asegurando su registro y tratamiento oportuno.
- Proporcionar formación y concienciación sobre seguridad de la información conforme a los requisitos establecidos.
- Realizar campañas permanentes de seguridad con la finalidad de mantener una cultura permanente en esta materia.
- Implementar y administrar controles de seguridad de TI, como firewalls, sistemas de detección de intrusiones, etc., en conformidad con las regulaciones y políticas establecidas.
- Supervisar la actividad de red para detectar y responder a posibles amenazas de acuerdo con los protocolos establecidos.
- Mantener actualizados y seguros los sistemas y herramientas de seguridad según las normativas vigentes.
- Almacenar y gestionar datos de manera segura, asegurando la confidencialidad, integridad y disponibilidad de acuerdo con las regulaciones y políticas aplicables, considerando los riesgos asociados a la seguridad de la información.
- Implementar y mantener medidas de seguridad física y lógica para proteger los datos de acuerdo con las normativas vigentes.

Funcionarios (as) de la Institución:

- Proteger la información en soportes físicos, como documentos impresos y dispositivos de almacenamiento, en cumplimiento con las regulaciones y políticas de seguridad establecidas.
- Controlar el acceso físico a áreas de almacenamiento de datos de acuerdo con los protocolos de seguridad establecidos.
- Seguir las políticas y procedimientos de seguridad de la información establecidos por la institución.
- Participar en actividades de formación y concienciación sobre seguridad de la información.
- Reportar cualquier incidente o violación de seguridad de la información a las autoridades correspondientes.

## Disposiciones Generales

- Protección de la información: Se establecerán medidas de seguridad adaptadas al nivel de criticidad de cada tipo de información.

- Clasificación: La información institucional se categorizará como "Pública", "Reservada" o "Secreta", según su sensibilidad y uso.
- Acceso: Se regulará el acceso a la información con base en los roles y responsabilidades asignadas a cada funcionario (a), conforme al principio de mínimo privilegio.
- Incidentes de seguridad: Se establecerán procedimientos específicos para gestionar, registrar y responder a incidentes de seguridad de manera eficaz.
- Confidencialidad: Todos los funcionarios (as) y terceros que accedan a información institucional deberán firmar acuerdos de confidencialidad.
- Uso de cuentas institucionales: Se prohíbe el envío, reenvío o almacenamiento de información institucional, especialmente aquella clasificada como reservada o secreta, a cuentas de correo personales de los funcionarios (as) o terceros no autorizados. Toda comunicación que involucre información institucional deberá realizarse exclusivamente a través de canales y cuentas oficiales provistas por la institución.

## Protección de Datos Personales y Seguridad

- La información de usuarios externos será resguardada con los mismos estándares de seguridad aplicados a los datos institucionales y no podrá ser compartida sin la debida autorización.
- Toda transferencia de información a terceros requerirá la firma de acuerdos de confidencialidad formales.

## Evaluación de Cumplimiento y Sanciones

1. **Supervisión del Cumplimiento**: Cada unidad será responsable de garantizar la aplicación de esta política y estará sujeta a auditorías internas para evaluar su efectividad, en coherencia con el Sistema de Gestión de Riesgos institucional.
2. **Acciones Correctivas**: En caso de incumplimientos, se implementarán medidas correctivas como capacitaciones adicionales, ajustes en procedimientos internos y refuerzo de controles de seguridad.
3. **Sanciones**: Cualquier incumplimiento será sancionado conforme al reglamento interno de la institución, considerando la gravedad del incidente y la responsabilidad de los involucrados.

## Difusión y Capacitación

- Se llevará a cabo un plan de difusión y formación en seguridad de la información, supervisado por la Dirección de Gestión Estratégica.

- Se utilizarán diversos medios de comunicación para garantizar que todos los funcionarios tengan acceso a la información y comprendan su aplicación.

## Compromiso Institucional

- La seguridad de la información será un pilar fundamental en la planificación y gestión de la institución.
- Se establecerán mecanismos que garanticen la continuidad de las operaciones ante incidentes que comprometan la seguridad de los datos institucionales, considerando escenarios de riesgo.

**II.** **DÉJASE SIN EFECTO** la actual Política de Seguridad y Ciberseguridad de la Información, aprobada por Resolución Exenta N°140/2025, de fecha 09 abril 2025.

**III.** **PUBLÍQUESE,** la presente resolución en la página web institucional www.cajbiobio.cl, para el debido conocimiento de los funcionarios (as) de la Corporación de Asistencia Judicial Región Biobío.

**IV.** **ANÓTESE, NOTIFÍQUESE Y ARCHÍVESE.**

FIRMA ELECTRÓNICA AVANZADA GOBIERNO DE CHILE

Firmado por:
Mauricio Alejandro Decap Fernández
Director General
Fecha: 16-04-2026 17:41 CLT
Corporación de Asistencia Judicial de la Región del Biobío

**MDF/MTS/RNI/AGE**
**DISTRIBUCIÓN:**
- Intranet/Documentos DGE/Gestión de Riesgos.
- Archivo.

MJTS