

POLÍTICA CORPORATIVA DE CIBERSEGURIDAD Y RESILIENCIA OPERACIONAL

SOCIEDAD ADMINISTRADORA DE CASINOS Y SERVICIOS ALISERVICE S.A. Y FILIALES

Alineada con la Ley N° 21.663 Marco de Ciberseguridad y la institucionalidad de la Agencia Nacional de Ciberseguridad (ANCI)

SECCIÓN I: MENSAJE DE NUESTRO DIRECTOR EJECUTIVO

MENSAJE DE LUIS ALBERTO YAPUR — DIRECTOR EJECUTIVO GRUPO ALISERVICE

Estimada comunidad de Aliservice, colaboradores, clientes y aliados estratégicos:

Me dirijo a cada uno de ustedes con profunda gratitud y satisfacción por el camino recorrido. En Aliservice nos hemos consolidado como la empresa líder de alimentación institucional de capitales 100% chilenos, un logro sustentado en el profesionalismo, la entrega diaria y la mística operacional de miles de trabajadoras y trabajadores a lo largo de todo nuestro país.

Nuestra responsabilidad operacional es gigantesca y vital para la sociedad: proveemos diariamente cientos de miles de raciones escolares a través de JUNAEB, garantizamos la alimentación hospitalaria en clínicas y redes de salud pública, y servimos a más de 200 clientes estratégicos del sector privado. Para que una ración llegue a tiempo, con la calidad e inocuidad requerida, detrás existe una compleja e interconectada red tecnológica y logística que abarca desde la adquisición de insumos hasta la entrega final en cada uno de nuestros restaurantes corporativos.

Hoy en día, la ciberseguridad y la continuidad de nuestras tecnologías de la información no son meros asuntos técnicos o del área informática; constituyen un pilar fundamental para garantizar la seguridad alimentaria de Chile. Un ciberataque o una falla en nuestros sistemas de compras, minutas o logística no solo afectaría a nuestra empresa, sino que podría interrumpir la alimentación de miles de niños en escuelas, de trabajadores y de pacientes en hospitales.

Con la promulgación de la Ley N° 21.663, Ley Marco de Ciberseguridad, Chile ha establecido un estándar de excelencia para proteger la infraestructura crítica del país. En Aliservice asumimos con entusiasmo esta normativa, comprometiéndonos a fortalecer nuestro Sistema de Gestión de Seguridad de la Información, promoviendo una cultura permanente de 'ciberhigiene' en todos los niveles de la organización.

Presento esta Política Corporativa de Ciberseguridad con la plena confianza en que, actuando con prevención, coordinación y el espíritu fraternal que nos caracteriza, resguardaremos la resiliencia operacional del Grupo Aliservice y la tranquilidad de las familias que confían en nosotros día a día.

Luis Alberto Yapur

Director Ejecutivo | Grupo Empresarial Aliservice

SECCIÓN II: MARCO LEGAL Y ADOPCIÓN PROACTIVA Y ADAPTABLE

La presente Política Corporativa se fundamenta orgánicamente en la Ley N° 21.663, Ley Marco de Ciberseguridad (publicada en el Diario Oficial el 8 de abril de 2024), la cual establece la institucionalidad nacional de ciberseguridad, crea la Agencia Nacional de Ciberseguridad (ANCI), el CSIRT Nacional y el Consejo Multisectorial, fijando deberes de ciberseguridad para los Servicios Esenciales (SE) y Operadores de Importancia Vital (OIV).

1. Adopción Proactiva y Posicionamiento Operacional (Accountability)

Considerando que Aliservice provee servicios críticos de alimentación e insumos a la Red Pública de Salud (hospitales, clínicas) y programas de asistencia social estatal (JUNAEB), la Compañía reconoce su rol indispensable en la cadena de abastecimiento del país. En virtud del principio de responsabilidad proactiva, Sociedad Administradora de Casinos y Servicios Aliservice S.A. y sus filiales adoptan de forma anticipada la presente Política, implementando controles de ciberseguridad antes del vencimiento de los plazos reglamentarios previstos por la ANCI.

2. Principio de Adaptabilidad y Actualización Regulatoria Continuada

De conformidad con los artículos 7°, 11 y 25 de la Ley N° 21.663, la ANCI dictará progresivamente protocolos, estándares técnicos, instrucciones generales y resoluciones de calificación de Operadores de Importancia Vital. La Fiscalía Corporativa y de Compliance, junto a la Gerencia de TI actualizarán dinámicamente este instrumento para alinearlos con las normas generales que publique la ANCI y las autoridades sectoriales competentes.

SECCIÓN III: ÁMBITO DE APLICACIÓN Y DEFINICIONES LEGALES

1. Ámbito de Aplicación Subjetivo

Las normas de esta Política son de cumplimiento obligatorio para:

- **Colaboradores Directos:** Todos los ejecutivos, administradores de restaurantes, jefes de compra, programadores de minutas, nutricionistas, administrativos y personal operacional.
- **Proveedores de Tecnologías y Servicios Gestionados:** Proveedores de infraestructura digital, software contable/logístico, servicios TI gestionados y contratistas con acceso a redes de la Compañía.
- **Clientes y Contrapartes:** Clientes del sector público y privado, garantizando la continuidad operacional de los servicios prestados.

2. Definiciones Legales Clave (Art. 2° de la Ley N° 21.663)

- **Activo Informático:** Toda información almacenada en una red o sistema informático que tenga valor estratégico u operacional para Aliservice.
- **Ciberataque:** Intento no autorizado de destruir, exponer, alterar, deshabilitar, exfiltrar u obtener acceso a un activo informático de la Compañía.
- **Ciberseguridad:** Preservación de la confidencialidad, integridad, disponibilidad y resiliencia de las redes y sistemas informáticos.
- **Confidencialidad:** Propiedad que asegura que la información solo sea accedida por personas o procesos autorizados.

- **Disponibilidad:** Propiedad que garantiza que la información esté disponible y utilizable cuando la operación de alimentación lo requiera.
- **Integridad:** Propiedad que asegura que la información o sistemas no hayan sido modificados o destruidos sin autorización.
- **Incidente de Ciberseguridad:** Todo evento que perjudique o comprometa la confidencialidad, integridad, disponibilidad, resiliencia o autenticación de las redes y sistemas.
- **Resiliencia:** Capacidad de las redes y sistemas informáticos para seguir operando (aún en estado degradado) tras un ciberataque y recuperar rápidamente su función normal.
- **Servicios Esenciales (SE):** Servicios prestados por instituciones públicas y privadas en sectores estratégicos (salud, seguridad social, provisión de bienes críticos) cuya interrupción puede causar grave daño a la población o la economía (Art. 4°).
- **Operadores de Importancia Vital (OIV):** Prestadores de servicios esenciales calificados por la ANCI cuya afectación tenga un impacto significativo en el orden público, abastecimiento o funciones del Estado (Art. 5°).

SECCIÓN IV: PRINCIPIOS RECTORES (ART. 3° LEY N° 21.663)

Toda acción de ciberseguridad en Aliservice se orientará por los siguientes principios legales:

- **1. Control de Daños:** Frente a un incidente, se actuará diligente y coordinadamente para contener la escalada del ataque y evitar la propagación a otros sistemas.
- **2. Cooperación con la Autoridad:** Deber de colaborar activamente con la ANCI, el CSIRT Nacional y autoridades sectoriales para la gestión de incidentes.
- **3. Racionalidad y Proporcionalidad:** Las medidas técnicas de seguridad serán racionales y proporcionales al nivel de riesgo y al potencial impacto en el abastecimiento alimentario.
- **4. Seguridad y Privacidad desde el Diseño y por Defecto:** Todo software, plataforma logística o sistema de casinos debe diseñarse e implementarse priorizando la seguridad y la privacidad de los datos.
- **5. Seguridad Informática:** Se garantiza el derecho a adoptar técnicas de cifrado y protección avanzada de activos informáticos.
- **6. Respuesta Responsable:** Las medidas de respuesta jamás incluirán ni apoyarán operaciones ofensivas informáticas.

SECCIÓN V: SISTEMA DE GESTIÓN DE SEGURIDAD Y PLANES DE CONTINUIDAD

1. Sistema de Gestión de Seguridad de la Información (SGSI - Art. 8° a)

Aliservice mantendrá un SGSI continuo (basado en estándares ISO/IEC 27001 o marcos equivalentes reconocidos por la ANCI), diseñado para:

- **Mapeo de Activos:** Identificar y clasificar activos informáticos críticos (servidores de facturación, bases de datos de minutas, sistemas de control de asistencia).
- **Evaluación Continua de Riesgos:** Evaluar la probabilidad de ocurrencia e impacto de riesgos cibernéticos sobre la cadena logística de raciones.
- **Registro de Auditoría:** Mantener un registro ejecutable de todas las acciones que componen el SGSI (Art. 8° b).

2. Planes de Continuidad Operacional y Ciberseguridad (BCP / DRP - Art. 8° c)

Aliservice elaborará, mantendrá y pondrá a prueba planes formales de continuidad operativa ante ciberataques (ej. secuestro de datos por ransomware o denegación de servicio), garantizando que la producción diaria de alimentos en casinos de hospitales y escuelas no sufra interrupciones.

- **Certificación Obligatoria:** Los planes de continuidad serán certificados periódicamente por centros de certificación acreditados ante la ANCI con una frecuencia mínima de dos años (Art. 8° c y 28).

3. Monitoreo, Ciberhigiene y Capacitación (Art. 8° d, h)

- **Revisiones y Simulacros:** Realización continua de simulacros, auditorías de seguridad, pruebas de penetración y escaneo de vulnerabilidades.
- **Capacitación y Ciberhigiene:** Programa permanente de educación continua para los +6.000 trabajadores, incluyendo campañas de 'ciberhigiene' (prevención de phishing, gestión segura de contraseñas y uso adecuado de dispositivos).

SECCIÓN VI: ESQUEMA OBLIGATORIO DE REPORTE DE INCIDENTES (ART. 9°)

Ante la ocurrencia de un ciberataque o incidente de ciberseguridad que pueda tener un ****efecto significativo**** (interrupción de servicio esencial, afectación de sistemas con datos personales o continuidad operacional), Aliservice cumplirá estrictamente el siguiente esquema de reporte ante el ****CSIRT Nacional****:

- **1. Alerta Temprana (Plazo MÁXIMO 3 HORAS):** Envío de una notificación preliminar o alerta temprana dentro del plazo máximo de TRES (3) HORAS desde que se tome conocimiento de la ocurrencia del ciberataque o incidente significativo.
- **2. Actualización de Información (24h OIV / 72h General):** Envío de actualización con evaluación inicial de gravedad, impacto e Indicadores de Compromiso (IoC). Si Aliservice es calificado como Operador de Importancia Vital (OIV) y ve afectado su servicio, la actualización se entregará en un plazo MÁXIMO DE 24 HORAS; en caso contrario, dentro de 72 HORAS.
- **3. Informe Final (Plazo MÁXIMO 15 DÍAS CORRIDOS):** Presentación de un informe final detallado que describa la causa raíz, tipo de amenaza, impacto exacto y medidas de mitigación aplicadas.
- **4. Plan de Acción de Respuesta (Plazo MÁXIMO 7 DÍAS):** En caso de ocurrir un incidente, la Compañía adoptará y notificará su plan de acción al CSIRT Nacional dentro de un plazo máximo de SIETE (7) DÍAS CORRIDOS desde el conocimiento del hecho.

Regulación de Contratación con Proveedores TI

En cumplimiento del inciso final del Art. 9°, los contratos que Aliservice celebre con proveedores de servicios de tecnologías de la información exigirán a estos compartir inmediatamente información sobre vulnerabilidades e incidentes. Prohíbese expresamente cualquier cláusula contractual que restrinja o dificulte el reporte de amenazas a la autoridad.

SECCIÓN VII: DELEGADO DE CIBERSEGURIDAD Y RESERVA LEGAL DE INFORMACIÓN

1. Delegado de Ciberseguridad (CISO / Contraparte ANCI - Art. 8° i)

La Alta Dirección de Aliservice designará formalmente a un “Delegado de Ciberseguridad”, quien actuará como contraparte oficial ante la ANCI y el CSIRT Nacional, reportando directamente al Director Ejecutivo, al Directorio y a la Gerencia de Compliance.

2. Reserva Legal y Secreto Absoluto de Antecedentes (Art. 33 de la Ley N° 21.663)

De conformidad al Título VI de la Ley N° 21.663, se declara que los antecedentes, matrices de riesgo, planes de continuidad operativa (BCP/DRP), planes de mitigación y registros del SGSI de Aliservice tienen legalmente el carácter de SECRETOS Y DE CIRCULACIÓN RESTRINGIDA, por entenderse que su divulgación afecta la seguridad e interés nacional.

- **Deber de Reserva Indefinido:** Todo colaborador, ejecutivo o proveedor que tenga acceso a dichos planes o matrices está obligado a guardar estricta reserva, obligación que perdurará indefinidamente tras el cese de sus funciones.
- **Sanciones Penales y Disciplinarias:** La infracción al deber de reserva será sancionada disciplinariamente como falta gravísima al RIOHS y penalmente conforme a los artículos 246, 247 y 247 bis del Código Penal (Art. 36).

SECCIÓN VIII: NOTIFICACIÓN RESPONSABLE DE VULNERABILIDADES

En concordancia con el Art. 55 de la Ley N° 21.663 (que modifica la Ley N° 21.459 de Delitos Informáticos), Aliservice reconoce la figura de la “notificación responsable de vulnerabilidades”. No será objeto de sanción penal ni persecución quien detecte una vulnerabilidad en los sistemas de la Compañía, siempre que:

- **Requisitos Legales:** Se encuentre previamente inscrito en el registro de la ANCI e informe previamente el acceso.
- **Conducta Ética:** Reporte la vulnerabilidad inmediatamente a Aliservice y a la ANCI sin haber actuado con ánimo fraudulento, sin apoderarse de información ni haber provocado denegación de servicio o alteración de datos.
- **Confidencialidad:** Mantenga estricta reserva y no divulgue públicamente la vulnerabilidad detectada.

SECCIÓN IX: RÉGIMEN DISCIPLINARIO Y SANCIONES LEGALES

1. Sanciones Disciplinarias Internas

El incumplimiento de los protocolos de ciberseguridad, la omisión intencional de reporte de incidentes, la negligencia grave en la ciberhigiene o la filtración no autorizada de matrices de riesgo constituirá una infracción grave a las obligaciones laborales, sancionable de acuerdo con el RIOHS, pudiendo dar lugar al término del contrato de trabajo sin derecho a indemnización (Art. 160 N° 7 del Código del Trabajo).

2. Régimen de Sanciones Administrativas ANCI (Art. 38 a 40)

Las infracciones legales cometidas por instituciones obligadas ante la ANCI conllevan multas a beneficio fiscal de altísima severidad:

- **Infracciones Leves (Art. 38 N° 1 / 39 N° 1):** Incumplir instrucciones generales, falta de registro de acciones o entrega tardía de información no crítica. Multa: hasta 5.000 UTM (hasta 10.000 UTM para OIV).
- **Infracciones Graves (Art. 38 N° 2 / 39 N° 2):** No haber implementado el SGSI, no contar con planes de continuidad (BCP), no reportar incidentes o entregar información falsa. Multa: hasta 10.000 UTM (hasta 20.000 UTM para OIV).
- **Infracciones Gravísimas (Art. 38 N° 3 / 39 N° 3):** No adoptar medidas para reducir el impacto de ciberataques significativos, entregar información falsa durante incidentes críticos o reincidir en faltas graves. Multa: hasta 20.000 UTM (hasta 40.000 UTM para OIV).

SECCIÓN X: VIGENCIA, DIFUSIÓN Y AUDITORÍA

- **Vigencia:** La presente Política entra en vigencia a contar de su aprobación por el Directorio del Grupo Aliservice.
- **Difusión:** Se difundirá en la intranet corporativa y se incorporará en las inducciones del personal y contratos de proveedores TI.
- **Auditoría:** Se someterá a auditorías de seguridad periódicas y a revisiones del BCP cada dos años, acreditadas ante centros autorizados por la ANCI.