DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LA DIRECCIÓN CHILECOMPRA

RESOLUCIÓN EXENTA N ° 507-B

SANTIAGO,14 de noviembre de 2024

VISTOS: Lo dispuesto en la Ley N° 18.575 Orgánica Constitucional de Bases General de la Administración del Estado, cuyo texto Refundido, Coordinado y Sistematizado fue fijado por el D.F.L. N°1/19.653, de 2001, del Ministerio Secretaría General de la Presidencia; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; en la Ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios; en el Decreto N° 250, de 2004, del Ministerio de Hacienda, que aprueba su Reglamento; en el Decreto N° 792, de 2023, del Ministerio de Hacienda, que designa a la Directora de la Dirección de Compras y Contratación Pública; en la Resolución N°35-B, de 2024, que aprueba Nuevo Estatuto Interno para la Dirección de Compras y Contratación Pública; y en la Resoluciones Nºs 7, de 2019, y 14, de 2022, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón y establece montos en unidades tributarias mensuales.

CONSIDERANDO:

1. Que, la Dirección de Compras y Contratación Pública, Organismo Público descentralizado, creado por la Ley N°19.886 de Bases sobre los Contratos Administrativos de Suministro y Prestación de Servicios (en adelante Ley de Compras Públicas), y sujeto a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, tiene dentro de sus funciones la administración del Sistema de Información de las Compras y Contrataciones de la Administración, www.mercadopublico.cl, creado por la citada Ley N°19.886,

funcionando con un marco regulatorio único, basado en la transparencia, la eficiencia, la universalidad, la accesibilidad y la no discriminación, a través del cual los organismos públicos regidos por dicha norma deben cotizar, licitar, contratar, adjudicar, solicitar el despacho y, en general, desarrollar todos sus procesos de adquisición de bienes y contratación de servicios y por otra parte, los proveedores del Estado deben presentar sus ofertas y cotizaciones, participar, de ser el caso, del Catálogo de Convenio Marco y, en general, desarrollar todas las actividades tendientes a ofertar productos y servicios a los organismos de la Administración.

2. Que, el artículo 5 del Decreto N°7 del año 2023 del Ministerio Secretaria General de la Presidencia, que "Establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme la Ley Nº 21.180", establece que "Cada órgano de la Administración del Estado deberá elaborar una Política de Seguridad de la Información y Ciberseguridad, en adelante "Política", aprobada a través de acto administrativo por el respectivo Jefe(a) Superior de Servicio, que tendrá como objetivo establecer las directrices generales en materia de seguridad de la información y ciberseguridad dentro del órgano, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan. Asimismo, deberá contener la visión estratégica del respectivo órgano de la Administración del Estado respecto de la seguridad de la información y ciberseguridad".

3. Que, en virtud de lo expuesto en los considerandos precedentes, esta Dirección debe contar con una política de seguridad de la información y ciberseguridad a fin de prevenir amenazas que pudiesen afectar la infraestructura informática del Sistema de Información www.mercadopublico.cl, y resguardar la confidencialidad, integridad y disponibilidad de la información que este posee, asi como del resto de los Sistemas Informáticos que utiliza esta Dirección para el cumplimiento de las funciones que la Ley le encomienda.

RESUELVO:

1. APRUÉBASE, la siguiente Política de Seguridad de la Información y Ciberseguridad para la Dirección ChileCompra:

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LA DIRECCIÓN CHILECOMPRA"

1. Objetivo

Esta política tiene como objetivo establecer las directrices generales en materia de seguridad de la información y ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos y activos manejados en ChileCompra, así como asegurar la continuidad de los procesos críticos de la institución ante cualquier evento relacionado con la seguridad de la información y ciberseguridad.

Para lograr este objetivo, se implementará la estrategia de seguridad de la información y ciberseguridad institucional, basada en tres pilares: controles de seguridad para mitigar riesgos y proteger activos; concientización para educar a los funcionarios; y un plan de continuidad del negocio que asegure la operatividad en situaciones de crisis.

2. Alcance

Esta política aplica a todos los funcionarios de ChileCompra, a los sistemas de información utilizados, y a todos los activos de información relacionados con la operación que ofrece ChileCompra a través de la plataforma Mercado Público y otras relacionadas. También involucra a los proveedores y a cualquier tercero que gestione información o sistemas por orden, encargo o autorización de ChileCompra.

3. Principios rectores

- **Confidencialidad:** Proteger los datos sensibles y evitar su divulgación no autorizada.

- **Integridad:** Asegurar que los datos no sean alterados sin autorización.

- **Disponibilidad:** Garantizar el acceso continuo a los sistemas de información esenciales.

- **Continuidad Operacional:** Implementar y mantener un plan de continuidad de negocio (BCP) y plan de recuperación ante desastres (DRP) que garantice la operatividad de los servicios críticos, incluso ante incidentes de seguridad de la información o ciberseguridad.

4. Responsabilidades

Director(a) de ChileCompra:

- Aprobar y supervisar la implementación de la Política de Seguridad de la Información y Ciberseguridad.
- Asegurar que la institución cuente con los recursos necesarios para cumplir con los lineamientos de seguridad establecidos en la política.
- Promover una cultura de seguridad de la información y ciberseguridad en todos los niveles de la organización, garantizando el apoyo institucional a las iniciativas de concientización y capacitación.
- Monitorear el cumplimiento de la política a través de reportes periódicos presentados por el Jefe(a) de Seguridad de la Información y Ciberseguridad.

Jefe(a) de Seguridad de la Información y Ciberseguridad:

- Liderar la implementación, mantenimiento y mejora continua de las iniciativas que fortalecen el Plan de Seguridad de Información Institucional.
- Coordinar el desarrollo del Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP).
- Asesorar al Director(a) y a otras áreas en temas relacionados con la seguridad de la información y ciberseguridad.
- Diseñar y ejecutar programas de concientización y capacitación en seguridad de la información para todo el personal.
- Evaluar y mitigar los riesgos de seguridad de la información y garantizar la correcta aplicación de controles de seguridad en la organización.

Funcionarias y funcionarios de ChileCompra

- Cumplir con las directrices y procedimientos establecidos en la Política de Seguridad de la Información y Ciberseguridad.
- Participar activamente en las iniciativas de concientización y capacitación sobre buenas prácticas en el manejo de la información y la ciberseguridad.
- Reportar de inmediato cualquier incidente o riesgo potencial relacionado con la seguridad de la información a sus superiores o al equipo de seguridad.
- Aplicar las medidas de seguridad necesarias en sus actividades diarias para proteger los activos de información y garantizar la integridad de los datos manejados en ChileCompra.

5. Gestión de riesgos

ChileCompra implementará un enfoque basado en la gestión de riesgos, identificando, evaluando y mitigando los riesgos que puedan comprometer la seguridad de la información y la ciberseguridad en los distintos procesos de la institución. Esto incluye la adopción de buenas prácticas de ciberseguridad, como la gestión de vulnerabilidades y el monitoreo continuo de las amenazas emergentes, principalmente las que puedan afectar a los componentes que dan soporte a la plataforma de Mercado Público.

6. Protección y seguridad de los activos informáticos

La seguridad de los activos informáticos en ChileCompra es fundamental para garantizar la protección de la información crítica y el correcto funcionamiento de los procesos institucionales. Todos los activos informáticos, incluyendo hardware, software, redes y datos, serán gestionados y protegidos mediante controles estrictos que aseguren su integridad, disponibilidad y confidencialidad. Los funcionarios deberán seguir los protocolos establecidos para el uso seguro de los sistemas y la protección de los equipos. Además, se implementarán medidas preventivas como el monitoreo continuo y la actualización de sistemas, con el fin de minimizar riesgos y proteger estos activos frente a posibles amenazas o vulnerabilidades.

Asimismo, todo desarrollo de software que se realice o adquiera deberá seguir los principios de desarrollo seguro, asegurando que las aplicaciones cuenten con controles de seguridad adecuados desde las primeras fases del ciclo de vida del desarrollo. Esto incluye revisiones de código, pruebas de penetración y la implementación de medidas que minimicen vulnerabilidades y garanticen la protección de los datos y servicios operados por ChileCompra.

7. Control de accesos a sistemas internos y externos

ChileCompra garantizará un control riguroso tanto en los accesos a sus sistemas internos como a aquellos sistemas externos que estén disponibles para la institución. Todos los accesos serán gestionados bajo el principio de privilegio mínimo, limitando los permisos solo a los usuarios que lo requieran para el cumplimiento de sus funciones. Se implementarán controles de autenticación segura, incluyendo autenticación multifactor, para todos los sistemas, tanto internos como externos, con el fin de proteger la información y los recursos de la institución. Además, se realizarán auditorías periódicas

para revisar y monitorear los accesos, asegurando la detección y respuesta ante cualquier actividad inusual o no autorizada en los sistemas críticos.

8. Almacenamiento de datos en el repositorio institucional

Todos los datos generados como parte de la gestión en ChileCompra deberán ser almacenados de manera segura en el repositorio institucional definido por la institución. Este repositorio garantizará la protección, integridad y disponibilidad de la información, cumpliendo con los estándares de seguridad de la información y privacidad vigentes. El acceso al repositorio estará restringido a personal autorizado, y se implementarán controles para asegurar que solo se almacenen datos relevantes y necesarios para las operaciones. Además, se llevarán a cabo copias de seguridad regulares para asegurar la continuidad y recuperación de la información en caso de incidentes, protegiendo la confidencialidad y la integridad de los datos críticos para ChileCompra.

9. Concientización y capacitación

ChileCompra promoverá para todos sus funcionarios iniciativas de concientización que permitan generar una cultura sólida de seguridad de la información y ciberseguridad. Estas actividades estarán orientadas a garantizar que los funcionarios comprendan la importancia crítica de aplicar buenas prácticas en el manejo de la información, minimizando los riesgos de seguridad. Además, se ofrecerá capacitación periódica para abordar los riesgos relacionados a la seguridad de la información y ciberseguridad.

10. Continuidad del negocio

ChileCompra garantizará la continuidad de sus operaciones mediante un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), los cuales serán probados regularmente.

11. Protección de sistema crítico

Consideramos a la plataforma mercadopublico.cl un sistema crítico para el funcionamiento del Estado. ChileCompra adoptará medidas para protegerla, incluyendo la implementación de controles de acceso, monitoreo continuo, auditorías de seguridad y actualizaciones de software que mitiguen el riesgo de un ataque de ciberseguridad y en caso de presentarse uno, que cuente con un alto grado resiliencia para seguir entregando el servicio a sus usuarios.

12. Seguridad de la información y ciberseguridad en los procesos de compra

ChileCompra garantizará que todos los procesos de compra para servicios internos, tanto tecnológicos como no tecnológicos, incluyan medidas adecuadas para resguardar la seguridad de la información y la ciberseguridad. En cada adquisición de servicios, se evaluarán y establecerán controles específicos para proteger los datos y activos de información involucrados. Los proveedores deberán cumplir con los requisitos de seguridad establecidos por la institución. Además, los contratos incluirán cláusulas específicas sobre seguridad de la información, asegurando que los proveedores adopten buenas prácticas y cumplan con las normativas vigentes en ciberseguridad.

13. Uso responsable de las herramientas de inteligencia artificial

ChileCompra promoverá el uso responsable y seguro de las herramientas de inteligencia artificial (IA) en sus procesos, garantizando que estas tecnologías se utilicen de manera ética y en cumplimiento con los estándares de seguridad de la información y privacidad. El uso de IA deberá estar alineado con los principios institucionales de confidencialidad, integridad y transparencia, y será auditado para prevenir cualquier riesgo potencial para la información crítica o los derechos de los usuarios. Además, se asegurará que los datos utilizados para alimentar los sistemas de IA sean gestionados de forma segura, protegiendo la privacidad de las personas involucradas y de los procesos críticos de la institución. Cualquier implementación de IA será revisada y aprobada por el Departamento de Seguridad de la Información y Ciberseguridad para garantizar su correcta operación y minimizar posibles riesgos de ciberseguridad.

14. Monitoreo y auditoría de la seguridad de la información y ciberseguridad

ChileCompra implementará un sistema de monitoreo continuo y auditorías periódicas para evaluar el cumplimiento de las políticas y controles de seguridad de la información y ciberseguridad. Las auditorías internas se llevarán a cabo regularmente para identificar posibles vulnerabilidades y asegurar que los controles de seguridad sean efectivos. Asimismo, se podrán realizar auditorías externas por parte de terceros para evaluar de manera independiente la robustez de las medidas de seguridad implementadas.

15. Políticas específicas para la implementación de controles de seguridad

Cada medida o control de seguridad que se implemente en ChileCompra estará respaldada por una política específica que detallará los lineamientos y el alcance de su

aplicación. Estas políticas definirán claramente cómo deberán operar los funcionarios en relación con cada control, estableciendo responsabilidades, procedimientos y acciones a seguir para cumplir con los estándares de seguridad establecidos. De esta manera, se asegurará que todos los funcionarios comprendan y sigan las directrices necesarias para mantener la seguridad de la información y ciberseguridad, promoviendo un entorno seguro y controlado en todas las operaciones de la institución.

16. Comité de Seguridad de la Información y Ciberseguridad

ChileCompra establecerá un Comité de Seguridad de la Información que sesionará una vez al mes para revisar el estado de la seguridad institucional. En estas sesiones, se presentarán métricas clave que midan la efectividad de los controles de seguridad implementados, las iniciativas de concientización y el estado de los planes de continuidad del negocio. Además, se abordarán los hitos relevantes en la ejecución de la estrategia de seguridad, evaluando los avances y proponiendo mejoras para fortalecer la protección de los activos informáticos y la resiliencia de los servicios críticos.

17. Legislación y Normativa Vigente

ChileCompra se compromete a cumplir con las leyes y regulaciones aplicables en relación con la Seguridad de la Información y Ciberseguridad. Entre estas se encuentran:

- La Ley N°21.459 que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
- El Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Pública que aprueba la Política Nacional de Ciberseguridad 2023-2028.
- Decreto N° 7, de 2023, del Ministerio Secretaría General de la Presidencia que establece la Norma Técnica de Seguridad de la Información y Ciberseguridad conforme a la Ley N°21.180.
- Decreto N°273 de 2022 que establece la obligación de reportar incidentes de ciberseguridad.
- Decreto N°83 de 2017 que promulga el Convenio de Budapest sobre la Ciberdelincuencia.

18. Revisión y actualización de la Política

Esta política será revisada y actualizada anualmente o cuando se produzcan cambios significativos en la estructura organizativa, tecnológica o regulatoria de ChileCompra. Cualquier cambio deberá ser aprobado por la Jefatura Superior de la institución.

19. Cumplimiento

El cumplimiento de esta política es obligatorio para todo el personal de ChileCompra. Las infracciones a la misma serán tratadas conforme a las normativas internas de la institución y a las leyes vigentes.

2. PUBLÍQUESE la presente resolución en la intranet institucional.

Anótese, regístrese y comuníquese,

CRISTIÁN PÉREZ CONTRERAS
DIRECTOR (S)
DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

VPC/MNM/CCV/PJR/

Distribución:
- Dirección
- Fiscalía
- División Tecnología
- Departamento Seguridad de la Información y Ciberseguridad
- Area Estrategia y Gestión Institucional

Firmado electrónicamente por:
Cristian Perez Contreras
DIRECTOR (s)
Fecha: 14-11-2024 - 14:51:15