



Cláusulas de Seguridad de la Información y Ciberseguridad en procesos de compra de ChileCompra

¿Por qué incorporar cláusulas de seguridad?



Incorporar cláusulas de ciberseguridad en los contratos de compra de servicios y productos, mitiga riesgos sobre la confidencialidad, integridad y disponibilidad de la información y los sistemas.

De cláusulas declarativas a cláusulas controlables

Antes



El adjudicatario deberá implementar y mantener un programa de seguridad que cumpla con los requisitos de seguridad y privacidad y que incorpore las mejores prácticas de la industria. El programa de seguridad del adjudicatario deberá incluir las medidas apropiadas de seguridad administrativas, técnicas y físicas, asegurar la confidencialidad, disponibilidad, integridad y seguridad de la Información de ChileCompra y sus sistemas e incluirá por lo menos las siguientes medidas de seguridad:

1. Controles adecuados para la autenticación de usuarios, incluyendo métodos seguros para asignar, seleccionar y almacenar el acceso de credenciales, limitar el acceso sólo a los usuarios activos y bloquear el acceso después de un número intentos de accesos fallidos acorde a las

Página 44 de 70



buenas prácticas de seguridad definidos de la industria detallados en los requisitos de seguridad y privacidad.

2. Controles de acceso seguro, incluyendo aquellos que limiten el acceso a la Información de ChileCompra para los individuos que tengan una razón fidedigna y demostrable de negocios para acceder a dicha información, respaldados mediante políticas, protocolos y controles apropiados que faciliten la autorización, establecimiento, modificación y eliminación de los accesos.

Foco en buenas prácticas y responsabilidades globales del proveedor, pero no controlables y fiscalizables.

Ahora



6) Cláusula Auditorías y evaluaciones: ChileCompra podrá realizar auditorías y evaluaciones in-situ o remotas **previo aviso de 2 días hábiles.**

El proveedor deberá proporcionar lo solicitado de acuerdo a lo que se establece en cada uno de los puntos de este apartado.

El aviso para las auditorías será enviado desde una casilla de correo electrónico oficial, la cual será proporcionada por ChileCompra en la reunión de inicio sobre Seguridad de la Información y Ciberseguridad. Este aviso se enviará a la dirección de correo electrónico de la contraparte de seguridad designada por el adjudicatario y al administrador del contrato de ChileCompra. En este aviso se informará por parte de ChileCompra, como mínimo, los siguientes detalles:

- Fecha y hora programada para la auditoría o evaluación.
- Modalidad de la auditoría (in-situ o remota).
- Objetivo de la auditoría.
- Documentos, información o acceso requerido al proveedor.
- Contacto de la persona responsable de la auditoría por parte de ChileCompra.

Enfoque en buenas prácticas y en las responsabilidades integrales del proveedor, con mecanismos que permiten su control y fiscalización.

Cláusulas de seguridad y ciberseguridad actuales

N°	Cláusula
1	Responsabilidad y confidencialidad
2	Notificación de incidentes
3	Eliminación segura de datos
4	Acceso a sistemas de ChileCompra
5	Medidas de seguridad en el uso de equipos propios
6	Auditorías y evaluaciones
7	Cooperación en incidentes de seguridad de la información y ciberseguridad
8	Contraparte responsable de seguridad
9	Hallazgo y notificación de vulnerabilidades
10	Notificación de cambios de infraestructura
11	Notificación de cambios en el personal con acceso a la información
12	Declaración y validación de software utilizado en el proyecto
13	Reuniones de inicio y coordinación periódica sobre Seguridad de la Información y Ciberseguridad
14	Comunicación oficial entre adjudicatario y ChileCompra
15	Política de Seguridad de la Información y Ciberseguridad del adjudicatario

Ejemplo 1

4) Cláusula Acceso a sistemas de ChileCompra

El proveedor deberá informar previamente a ChileCompra los detalles del personal que accederá a los sistemas, incluyendo datos del dispositivo que utilizará.

Las cuentas de acceso serán nominativas e intransferibles. Para accesos mediante VPN, el proveedor deberá usar únicamente dispositivos autorizados y que cumplan con las medidas de seguridad que se señala la cláusula “Medidas de seguridad en el uso de equipos propios” de este contrato. Los dispositivos serán sujetos a auditorías y evaluaciones periódicas, las cuales serán informadas con un aviso previo de 2 días hábiles.

Para controlar el cumplimiento de lo anterior, el proveedor deberá completar el “Anexo: Solicitud de Acceso a Sistemas de ChileCompra” con los profesionales que requiera acceso, detallando la información requerida y enviarlo, al momento de la firma del contrato, a la o las casillas que serán proporcionada por ChileCompra en la reunión de inicio sobre Seguridad de la Información y Ciberseguridad. al administrador del contrato. Una vez que este anexo sea recibido por el administrador del contrato, se gestionaran los respectivos accesos. Este mismo anexo se deberá enviar si se desea solicitar accesos para un nuevo profesional que se sume al proyecto.

5) Cláusula Medidas de seguridad en el uso de equipos propios

Los equipos propios por parte del adjudicatario deberán cumplir con los siguientes estándares de seguridad establecidos por ChileCompra:

- Tener un sistema operativo Windows o MacOS con soporte activo por parte del fabricante, incluyendo la recepción de actualizaciones de seguridad periódicas. En casos excepcionales, podrá permitirse el uso de dispositivos con sistemas operativos distintos, siempre que estos cuenten con soporte activo del fabricante y cumplan con los requisitos de seguridad establecidos por ChileCompra.
- Contar con un sistema de seguridad activo para proteger contra amenazas conocidas y desconocidas.
- Implementar cifrado completo del disco duro utilizando BitLocker (Windows), FileVault (MacOS) u otro que sea validado por el Departamento de Seguridad de la Información y Ciberseguridad de ChileCompra.
- Aplicar parches de seguridad del sistema operativo en un plazo máximo de 7 días tras su liberación.
- Tener el firewall local habilitado y configurado para restringir accesos no autorizados.
- Utilizar navegadores web actualizados a la última versión disponible.

Ejemplo 3

8) Cláusula Contraparte responsable de seguridad

El adjudicatario deberá **designar un Jefe(a) de Seguridad de la Información y Ciberseguridad, o un cargo equivalente, como contraparte para coordinar con el Jefe(a) de Seguridad de la Información y Ciberseguridad de ChileCompra todos los temas relacionados con la seguridad establecidos en este contrato.**

Para garantizar esta coordinación, posterior a la adjudicación del contrato, el adjudicatario deberá completar el **"Anexo: Contraparte responsable de Seguridad de la Información y Ciberseguridad del adjudicatario".**

Las **cláusulas de seguridad** se incorporan en virtud de lo dispuesto en el numeral 6° del artículo 41 del Reglamento de la ley 19.886, que contempla como **contenido adicional**: "6. *Cualquier otra materia que no contradiga disposiciones de la Ley de Compras y este reglamento.*"



Asociación de cláusulas a medidas contractuales

Las cláusulas de seguridad deben asociarse a medidas definidas en las bases de compra para tener efecto real. Estas pueden ser **multas, amonestaciones, cobro de garantía o término anticipado del contrato** ante incumplimientos graves. Su inclusión asegura obligaciones exigibles y mecanismos proporcionales a la criticidad del proceso.



Lo anterior, da cumplimiento al numeral 12 del artículo 41 del Reglamento, que señala como contenido obligatorio: **12. La determinación de las medidas a aplicar en los casos de incumplimiento del Proveedor y de las causales expresas** en que dichas medidas deberán fundarse, así como el procedimiento para su aplicación.



Aplicación de las cláusulas (modelo lego)

- Las cláusulas están diseñadas como bloques independientes, que pueden tomarse, combinarse o descartarse según la naturaleza del proceso de compra.
- No todos los contratos requieren el mismo nivel de exigencia en seguridad: por ejemplo, una compra de papelería no necesita tantas cláusulas como un servicio de hosting o de desarrollo de software.
- La lógica es la misma que armar con piezas de Lego: se construye a medida, asegurando una base de seguridad, pero con la posibilidad de ir añadiendo complejidad cuando el riesgo lo amerite.



ID Licitación: 869591-2-LP25

LP Publicada y disponible para ofertar

Análisis de Documentos mediante modelos de IA

El objetivo es generar un procedimiento automatizado que permita la detección, con un alto nivel de certeza, de anomalías relacionadas con 20 reglas o hipótesis de incumplimientos a la normativa de compras y contratación pública en un conjunto de aproximadamente 200 mil procesos anuales a partir del análisis de documentos de texto mediante grandes modelos de lenguaje (LLM).

Monto	Fecha de publicación	Fecha de cierre
Igual o superior a 1.000 UTM e inferior a 2.000 UTM	14/08/2025	15/09/2025 (En 5 días)

DIRECCION DE COMPRAS Y CONTRATACION PUBLICA	Cantidad de compras efectuadas*	Cantidad de reclamos por pago no oportuno*
DIRECCION DE COMPRAS Y CONTRATACION PUBLICA	26	14

* En base a todas las compras realizadas en los últimos 12 meses

ID Licitación: 869591-3-LP25

LP Publicada y disponible para ofertar

Contratación del Servicio de Centro de Operaciones de Seguridad SOC 27X7

la contratación del servicio de Centro de Operaciones de Seguridad (SOC) 24x7 para la Dirección de Compras y Contratación Pública (DCCP), abarcando tanto infraestructura on-premise como en la nube.

Monto disponible	Fecha de publicación	Fecha de cierre
\$138.000.000	26/08/2025	23/09/2025 (En 13 días)

DIRECCION DE COMPRAS Y CONTRATACION PUBLICA	Cantidad de compras efectuadas*	Cantidad de reclamos por pago no oportuno*
DIRECCION DE COMPRAS Y CONTRATACION PUBLICA	26	14

10.9.1.2. No conformidades por incumplimiento de obligaciones del adjudicatario

La Dirección de Compras y Contratación Pública (DCCP) registrará una "No Conformidad" ante la ocurrencia de los siguientes incumplimientos, siempre que sean imputables al proveedor. Cada vez que el proveedor acumule tres (3) "No Conformidades" durante la vigencia del contrato, se le aplicará una multa de 1% del total del contrato, de conformidad con lo establecido en la Cláusula 10.9.1.2.

Las "No Conformidades" serán notificadas al proveedor a través de correo electrónico institucional del administrador de contrato, con un plazo de 24 horas para que el proveedor presente sus descargos o un plan de subsanación. La DCCP evaluará los descargos y, de considerarlos insuficientes o no subsanado el incumplimiento, mantendrá el registro de la "No Conformidad".

Incumplimiento
11.9. Cláusula 3. Propiedad y uso de la información
11.9. Cláusula 4. Acceso a sistemas de ChileCompra
11.9. Cláusula 5. Auditorías y evaluaciones
11.9. Cláusula 6. Contraparte responsable de seguridad
11.9. Cláusula 7: Notificación de cambios de infraestructura

Integrar las cláusulas en el flujo de compras



Desafíos en trabajar con cláusulas

