

DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA
APRUEBA DIRECTIVA DE CONTRATACIÓN PÚBLICA N° 47/2026
“RECOMENDACIONES PARA INCORPORAR MEDIDAS DE SEGURIDAD DE LA
INFORMACIÓN Y CIBERSEGURIDAD EN LOS PROCESOS DE COMPRAS
PÚBLICAS”

RESOLUCIÓN EXENTA

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; 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°661, de 2024, del Ministerio de Hacienda, que aprueba su Reglamento; en la Resolución Exenta RA 870/109/2024 de 2024, que nombra en el cargo de Alta Dirección Pública a Jefe de División que indica, de este origen; en el artículo 80 del DFL N°29 de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.834, sobre Estatuto Administrativo; en la Resolución Exenta N°537-B de 2024, de esta Dirección, que deja sin efecto Resolución Exenta N°35-B, de 2024, y aprueba Nuevo Estatuto Interno para la Dirección de Compras y Contratación Pública, y sus modificaciones; y en la Resolución N°36 de 2024, de la Contraloría General de la República, que establece normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, la Dirección de Compras y Contratación Pública, en adelante e indistintamente la “Dirección”, “ChileCompra” o la “DCCP”, es un servicio público descentralizado, sometido a la supervigilancia del Presidente de la República, a través del Ministerio de Hacienda, que tiene como misión liderar un sistema de compras públicas eficiente, con altos estándares de probidad y transparencia, promoviendo la participación y sustentabilidad, para el buen uso de los recursos en beneficio de las personas.
2. Que, la Dirección tiene la función legal de asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras en la plataforma www.mercadopublico.cl, dispuesto en el artículo 30, letra a), de la ley N°19.886.
3. Que, en el mismo sentido, se contempla en el artículo 10 del Reglamento de Compras Públicas sancionado por el Decreto N° 661 del Ministerio de Hacienda, que esta Dirección en conformidad al literal a) señalado en el considerando precedente, podrá dictar directivas en el ejercicio de sus atribuciones, las cuales, tendrán como objetivo servir de referencia y guía para las Entidades en la planificación y gestión de sus procesos de compras y contrataciones, respetando el marco normativo aplicable.
4. Que, en este sentido, el objetivo de la presente Directiva es entregar orientaciones y recomendaciones para incorporar medidas de seguridad de la información y ciberseguridad en los procesos de compras y contrataciones públicas, promoviendo la protección de los datos personales, los activos de información y los sistemas tecnológicos involucrados en la prestación de servicios al Estado.

RESUELVO

1. **APRUEBESE** la **DIRECTIVA DE CONTRATACIÓN PÚBLICA N°47/2026 “RECOMENDACIONES PARA INCORPORAR MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN LOS PROCESOS DE COMPRAS PÚBLICAS”**, cuyo texto se transcribe a continuación:

**DIRECTIVA DE CONTRATACIÓN PÚBLICA N°47 RECOMENDACIONES PARA
INCORPORAR MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD EN LOS PROCESOS DE COMPRAS PÚBLICAS**

I. Resumen ejecutivo: La creciente incorporación de tecnologías digitales en los procesos de gestión pública, así como la contratación de servicios proporcionados por terceros, plantean nuevos desafíos para la seguridad de la información y la ciberseguridad de los organismos del Estado.

En este contexto, resulta relevante considerar medidas que permitan prevenir, mitigar y gestionar los riesgos asociados al acceso, almacenamiento, procesamiento y transmisión de información institucional por parte de proveedores.

La presente Directiva, elaborada por la Dirección de Compras y Contratación Pública (ChileCompra) en colaboración con la Agencia Nacional de Ciberseguridad (ANCI), entrega orientaciones y recomendaciones para incorporar medidas de seguridad de la información y ciberseguridad en los procesos de compras y contrataciones públicas, promoviendo la protección de los datos personales, los activos de información y los sistemas tecnológicos involucrados en la prestación de servicios al Estado.

Estas recomendaciones se enmarcan en la normativa de compras públicas y consideran las disposiciones de la Ley N° 21.663, Ley Marco de Ciberseguridad, particularmente respecto de la gestión de riesgos, la prevención de incidentes y la protección de la información, los sistemas tecnológicos y los servicios involucrados en las contrataciones públicas.

La Directiva propone considerar los riesgos de ciberseguridad durante las distintas etapas del proceso de contratación, desde la planificación y elaboración de las bases hasta la ejecución y término del contrato. Asimismo, proporciona criterios para seleccionar cláusulas contractuales según la naturaleza de los bienes o servicios contratados, el tipo de información involucrada y su nivel de criticidad.

Como herramienta de apoyo, se presenta un conjunto de 17 modelos de cláusulas contractuales que abordan materias como confidencialidad, control de accesos, notificación de incidentes, gestión de vulnerabilidades, auditorías, protección de datos, coordinación con proveedores y restitución de información.

Las cláusulas propuestas tienen carácter referencial y su incorporación no es obligatoria por el solo hecho de estar contenidas en esta Directiva. Corresponderá a cada organismo público evaluar su pertinencia, considerando las características y riesgos de la contratación, sin perjuicio del cumplimiento de las obligaciones establecidas en la normativa vigente.

De esta manera, la Directiva busca contribuir a una gestión preventiva de los riesgos de ciberseguridad en las compras públicas, fortaleciendo la protección de la información institucional y la continuidad de los servicios prestados a la ciudadanía.

II. Introducción: La seguridad de la información y la ciberseguridad constituyen materias relevantes para el funcionamiento de los organismos del Estado y la continuidad de los servicios públicos, especialmente en un contexto de creciente digitalización y contratación de bienes y servicios proporcionados por terceros.

La Ley N° 21.663, Ley Marco de Ciberseguridad, establece la institucionalidad nacional en esta materia, contemplando la Agencia Nacional de Ciberseguridad (ANCI), encargada de ejercer las funciones y atribuciones que dicha ley le confiere, así como deberes para las instituciones comprendidas en su ámbito de aplicación. En este contexto, los responsables de seguridad de la información y ciberseguridad de los organismos públicos cumplen un rol relevante en la identificación y gestión de riesgos.

Por su parte, la Dirección de Compras y Contratación Pública, en el ejercicio de sus funciones de asesoría a los organismos públicos conforme al artículo 30, letra a), de la Ley N° 19.886, pone a disposición la presente Directiva, destinada a orientar la incorporación de medidas de seguridad de la información y ciberseguridad en los procesos de compras y contrataciones públicas.

III. Objetivo: El presente documento tiene por finalidad establecer lineamientos y recomendaciones para la incorporación de cláusulas de seguridad de la información y ciberseguridad en los procesos de contratación que realice un Organismo de Administración del Estado (OAE).

Su propósito es garantizar que los proveedores implementen medidas preventivas, de control y de respuesta que resguarden la confidencialidad, integridad disponibilidad y autenticidad de la información institucional, incluyendo datos sensibles y personales, activos tecnológicos y sistemas críticos.

El documento constituye una guía referencial que orienta sobre las cláusulas que pueden aplicarse en cada contrato. La selección de las cláusulas pertinentes deberá realizarse caso a caso, considerando el tipo de servicio o producto contratado y el nivel de criticidad para la seguridad institucional.

La evaluación e incorporación de estas cláusulas debe ser un proceso acompañado por el Departamento de Seguridad de la Información y Ciberseguridad o el equivalente del organismo.

IV. Alcance: Este documento aplica exclusivamente a los procesos de compra y contratación efectuados por el OAE, que contemplen:

- Acceso a sistemas, aplicaciones o infraestructura tecnológica.
- Tratamiento de datos personales o sensibles.
- Prestación de servicios tecnológicos, de soporte o que involucren activos de información institucional.
- Almacenamiento, procesamiento o transmisión de información.
- Ejecución de proyectos que puedan generar riesgos en materia de seguridad de la información y ciberseguridad.
- Contratación de servicios de tecnologías de la información en general.

Se hace presente que las cláusulas contenidas en este documento tienen un carácter exclusivamente referencial y constituyen recomendaciones para los organismos públicos. En ningún caso ChileCompra establece su aplicación como obligatoria, siendo responsabilidad de cada organismo evaluar su pertinencia e incorporación en los respectivos procesos de contratación, considerando la naturaleza de la compra y el nivel de riesgo asociado a la información o servicios involucrados.

V. Marco Normativo: La presente Directiva considera las disposiciones de la Ley N° 21.663, Ley Marco de Ciberseguridad, y su aplicación en el contexto de las compras y contrataciones públicas reguladas por la Ley N° 19.886 y su Reglamento, con el propósito de orientar a los organismos públicos en la incorporación de medidas que contribuyan a proteger la información, los sistemas tecnológicos y la continuidad de los servicios contratados.

La Ley N° 19.886, modificada por la Ley N° 21.634 que moderniza el sistema de compras públicas, establece el marco jurídico aplicable a los procesos de adquisición de bienes y contratación de servicios realizados por los organismos públicos comprendidos en su ámbito de aplicación.

En particular, el artículo 30, letra a), de la Ley N° 19.886 establece entre las funciones de la Dirección de Compras y Contratación Pública asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras y contrataciones.

Por su parte, el artículo 10 del Reglamento de la Ley N° 19.886, aprobado mediante el Decreto N° 661 de 2024 del Ministerio de Hacienda, contempla la facultad de ChileCompra para dictar directivas destinadas a servir de referencia y guía a las entidades en la planificación y gestión de sus procesos de contratación, respetando el marco normativo aplicable.

En este contexto, la incorporación de consideraciones de seguridad de la información y ciberseguridad en las contrataciones públicas constituye una materia relevante para la adecuada definición de requerimientos técnicos, condiciones contractuales y mecanismos de supervisión de los bienes y servicios adquiridos.

Las recomendaciones contenidas en esta Directiva buscan apoyar a los organismos públicos en la identificación de riesgos y en la selección de medidas contractuales pertinentes, procurando que estas sean proporcionales al objeto de la contratación, estén debidamente justificadas y respeten los principios y disposiciones aplicables a las compras públicas. Para ello, se proponen criterios de evaluación relacionados con el tipo de información involucrada, los accesos requeridos por el proveedor, la criticidad del servicio y el impacto potencial de un incidente de ciberseguridad, los cuales se desarrollan en el apartado de criterios para seleccionar cláusulas de ciberseguridad.

La Ley N° 21.663 establece la institucionalidad y el marco general de ciberseguridad en Chile, definiendo principios, atribuciones y obligaciones destinadas a prevenir, contener, resolver y responder a incidentes de ciberseguridad.

Esta ley contempla obligaciones para las instituciones comprendidas en su ámbito de aplicación, incluyendo a los prestadores de servicios esenciales y a aquellas instituciones calificadas como Operadores de Importancia Vital (OIV).

Entre sus disposiciones se encuentran deberes relacionados con la adopción de medidas de seguridad, la gestión de riesgos, la prevención y respuesta ante incidentes de ciberseguridad y la continuidad operacional de los servicios.

Asimismo, la Ley Marco de Ciberseguridad reconoce la importancia de la colaboración con proveedores tecnológicos. En este sentido, el artículo 9 contempla que, para cumplir los deberes de reporte, los jefes de servicio de los organismos del Estado deberán exigir a sus proveedores de servicios de tecnologías de la información compartir antecedentes sobre vulnerabilidades e incidentes que puedan afectar sus redes y sistemas informáticos, en los términos y para los fines establecidos en dicha disposición.

En el ámbito de las contrataciones públicas, estas disposiciones refuerzan la importancia de considerar mecanismos de coordinación, intercambio de información, notificación de incidentes y gestión de riesgos asociados a los servicios proporcionados por terceros.

La presente Directiva busca facilitar la incorporación de estas consideraciones en los procesos de contratación pública, mediante recomendaciones y modelos de cláusulas contractuales que podrán ser utilizados y adaptados por los organismos según sus necesidades y riesgos particulares.

Las recomendaciones contenidas en este documento no sustituyen ni modifican las obligaciones legales y reglamentarias aplicables a cada organismo o proveedor, ni las instrucciones que puedan dictar las autoridades competentes en el ejercicio de sus atribuciones.

VI. Riesgos de ciberseguridad asociados a las contrataciones públicas: La contratación de bienes y servicios puede incorporar riesgos de seguridad de la información y ciberseguridad para los organismos públicos, especialmente cuando los proveedores requieren acceder a sistemas institucionales, tratar información, administrar infraestructura tecnológica o prestar servicios que resulten relevantes para la continuidad de las operaciones.

Estos riesgos pueden presentarse durante cualquiera de las etapas de una contratación y no necesariamente se encuentran limitados a servicios estrictamente tecnológicos. Por ejemplo, un servicio de atención de usuarios puede involucrar el tratamiento de datos personales, una consultoría puede requerir acceso a información confidencial y un servicio de mantenimiento puede necesitar acceso a sistemas institucionales. Por ello, la ciberseguridad debe considerarse una materia transversal a las contrataciones públicas, evaluando su pertinencia según las características y riesgos de cada contratación.

Entre los principales riesgos que se recomienda considerar se encuentran:

1. Acceso no autorizado a sistemas e información institucional: La utilización de cuentas, credenciales o mecanismos de acceso por parte de proveedores puede generar riesgos de acceso indebido a información y sistemas institucionales, especialmente cuando no existen controles adecuados de autenticación, autorización y gestión de permisos.

2. Exposición, pérdida o divulgación de información: Los proveedores pueden acceder, almacenar o procesar información institucional, incluyendo datos personales o sensibles. La ausencia de medidas de protección adecuadas puede ocasionar accesos no autorizados, pérdida de información o divulgación de antecedentes confidenciales.

3. Interrupción de servicios y continuidad operacional: Los incidentes que afecten la infraestructura, plataformas o servicios administrados por terceros pueden impactar la disponibilidad de sistemas institucionales y la continuidad de los servicios públicos.

4. Vulnerabilidades en productos y servicios tecnológicos: Los sistemas, aplicaciones, componentes de software y servicios proporcionados por proveedores pueden contener vulnerabilidades de seguridad que faciliten accesos no autorizados, alteraciones de información o interrupciones operacionales.

5. Gestión insuficiente de incidentes de ciberseguridad: La ausencia de mecanismos contractuales de notificación, coordinación y entrega de antecedentes puede dificultar la detección, análisis, contención y recuperación ante incidentes que involucren servicios contratados.

6. Dependencia tecnológica y pérdida de control sobre la información: La utilización de plataformas o servicios administrados por terceros puede generar dependencia del

proveedor, especialmente cuando no existen mecanismos que garanticen la disponibilidad, portabilidad y restitución de la información al término del contrato.

7. Falta de supervisión y verificación de medidas de seguridad: La ausencia de mecanismos de seguimiento, auditoría o entrega de evidencias puede dificultar que los organismos públicos verifiquen el cumplimiento de las medidas de seguridad comprometidas por los proveedores.

La identificación de estos riesgos permite a los organismos públicos evaluar la necesidad de incorporar medidas de seguridad durante la contratación, considerando la naturaleza del servicio, los activos involucrados y las posibles consecuencias de un incidente.

Se recomienda que este análisis sea realizado por el área requirente, con el apoyo de los responsables de seguridad de la información y ciberseguridad o quienes cumplan funciones equivalentes dentro de la institución.

VII. Criterios para seleccionar cláusulas de ciberseguridad: La selección de cláusulas de seguridad de la información y ciberseguridad debe considerar las características particulares de cada contratación y los riesgos que puedan derivarse de la prestación del bien o servicio requerido. Por ejemplo, estas consideraciones pueden resultar pertinentes en contrataciones de desarrollo y mantenimiento de software, servicios en la nube, soporte tecnológico, consultorías que involucren información confidencial o servicios que contemplen el tratamiento de datos personales.

No todas las contrataciones presentan el mismo nivel de exposición ni requieren idénticas medidas de protección. Por ello, se recomienda que los organismos públicos realicen una evaluación previa que permita determinar cuáles de las cláusulas propuestas en esta Directiva resultan pertinentes.

Para apoyar este análisis, se sugiere considerar los siguientes criterios:

1. Tipo de información involucrada: Identificar si el proveedor tendrá acceso, almacenará, procesará o transmitirá información institucional, especialmente cuando se trate de datos personales, datos sensibles o información confidencial o reservada.

2. Acceso a sistemas e infraestructura tecnológica: Determinar si el proveedor requerirá acceso a plataformas, aplicaciones, redes, servidores u otros componentes tecnológicos institucionales, considerando el tipo de acceso y los privilegios necesarios.

3. Criticidad del servicio contratado: Evaluar la importancia del bien o servicio para el funcionamiento del organismo y las consecuencias que podría generar su interrupción o indisponibilidad.

4. Impacto potencial de un incidente de ciberseguridad: Considerar las posibles consecuencias de un incidente sobre la confidencialidad, integridad y disponibilidad de la información, la continuidad de los servicios y los derechos de las personas.

5. Dependencia tecnológica del proveedor: Identificar si la contratación pudiera generar dificultades para recuperar información, migrar hacia otra plataforma o mantener la continuidad del servicio ante el término del contrato.

6. Capacidades de supervisión y control: Evaluar la necesidad de establecer mecanismos de seguimiento, auditoría, notificación y entrega de evidencias que permitan verificar el cumplimiento de las medidas de seguridad comprometidas.

A partir de estos criterios, cada organismo podrá identificar las cláusulas contractuales más adecuadas para abordar los riesgos de su contratación.

La incorporación de estas cláusulas deberá considerar su pertinencia, proporcionalidad y viabilidad, así como la normativa aplicable al proceso de compra.

Las cláusulas presentadas en esta Directiva constituyen modelos referenciales que podrán ser adaptados por cada organismo, sin perjuicio de las obligaciones legales y reglamentarias que resulten exigibles en cada caso.

VIII. Definiciones:

- **Activo de información:** Toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- **Adjudicatario:** Persona natural o jurídica que celebra un contrato con un OAE, obligándose al cumplimiento de las cláusulas de seguridad establecidas.
- **Administrador del contrato:** Persona designada por el OAE para supervisar la ejecución contractual, coordinar las obligaciones del adjudicatario y gestionar los requerimientos asociados al contrato.
- **Agencia Nacional de Ciberseguridad (ANCI):** Organismo público encargado de las funciones y atribuciones establecidas en la Ley N° 21.663, Ley Marco de Ciberseguridad.
- **Cambio significativo:** Cualquier modificación, alteración o ajuste en los sistemas, servicios, procesos, configuraciones tecnológicas o en la infraestructura asociada al contrato, que pueda tener un impacto relevante en la continuidad operativa, la seguridad de la información, la protección de datos personales, la interoperabilidad con sistemas del Estado, los niveles de servicio comprometidos (SLA), o los costos de operación y mantenimiento.
- Se considerarán cambios significativos, entre otros: Actualizaciones o migraciones de plataformas tecnológicas que alteren funcionalidades críticas, incorporación o eliminación de módulos, componentes o servicios esenciales, cambios en el modelo de provisión del servicio (ej: on-premise a nube), ajustes que requieran nuevas integraciones con sistemas estatales, modificaciones que impliquen riesgo de indisponibilidad, exposición de vulnerabilidades o afectación de datos sensibles.
- **Cláusulas de seguridad de la información y ciberseguridad:** Estipulaciones contractuales que regulan obligaciones específicas del proveedor en materias como confidencialidad, gestión de incidentes, acceso a sistemas, uso de equipos propios, auditorías, notificación de cambios, gestión de vulnerabilidades, entre otras.
- **Common Vulnerability Scoring System (CVSS):** Sistema estandarizado utilizado para evaluar y expresar numéricamente la severidad de vulnerabilidades de seguridad informática.
- **Contraparte de seguridad:** Profesional designado por el adjudicatario como responsable de coordinar con el Jefe(a) de Seguridad de la Información y Ciberseguridad o equivalente del OAE todos los aspectos relativos a la ejecución de las cláusulas contractuales en esta materia.
- **Dato personal:** Información concerniente a una persona natural, identificada o identificable, de acuerdo con lo dispuesto en la Ley N° 19.628.
- **Dato sensible:** Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual, de acuerdo con lo dispuesto en la Ley N° 19.628.

- **Eliminación segura de datos:** Proceso mediante el cual se elimina información de soportes o sistemas tecnológicos, utilizando mecanismos que impidan su recuperación mediante medios razonablemente disponibles.
- **Incidente de seguridad:** Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- **Logs o registros de eventos:** Registros generados por sistemas, aplicaciones, dispositivos o servicios tecnológicos que permiten identificar y reconstruir actividades, accesos, operaciones y eventos relevantes para la seguridad.
- **Operador de Importancia Vital (OIV):** Institución pública o privada calificada como tal conforme a la Ley N° 21.663, sujeta a obligaciones especiales de ciberseguridad.
- **Organismo de la Administración del Estado (OAE):** Institución pública que realiza el proceso de contratación y establece las obligaciones de seguridad aplicables al adjudicatario.
- **Servicio esencial:** Servicio comprendido en las categorías establecidas por la Ley N° 21.663, cuya prestación resulta relevante para el funcionamiento de la sociedad y las actividades del país.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

IX. Medidas ante incumplimientos contractuales: Para favorecer el cumplimiento de las cláusulas de seguridad de la información y ciberseguridad incorporadas en los contratos, se recomienda contemplar medidas ante eventuales incumplimientos, claramente definidas en las bases del proceso de compra. Estas medidas pueden considerar multas frente a incumplimientos específicos, cobro de la garantía de fiel y oportuno cumplimiento del contrato, cuando corresponda, o el término anticipado del contrato en casos de incumplimientos graves, de conformidad con la normativa aplicable. La incorporación de estas medidas permite establecer mecanismos proporcionales a la naturaleza y criticidad de cada contratación, contribuyendo al cumplimiento de las obligaciones contractuales en materia de seguridad.

X. Cláusulas de Seguridad de la Información y Ciberseguridad recomendadas:

1) Cláusula Responsabilidad y confidencialidad: El adjudicatario y su personal deben guardar estricta confidencialidad sobre la información del OAE ya sea que esta provenga de la misma entidad, otro organismo o usuarios, tanto durante la vigencia del contrato como en forma posterior. Para datos personales, la obligación está normada en los términos de la Ley N°19.628 Sobre protección de la vida privada.

La información obtenida no podrá ser utilizada para fines distintos a la ejecución del contrato, y su divulgación no autorizada será sancionada con acciones legales.

Para garantizar este compromiso, el adjudicatario, posterior a la adjudicación del contrato, deberá firmar el “Anexo: Acuerdo de confidencialidad y uso responsable de activos de información; OAE y Adjudicatario”.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Consultorías estratégicas
- Servicios profesionales que acceden a información sensible
- Contratos de terceros para desarrollo de software

2) Cláusula Notificación de incidentes: El adjudicatario deberá informar a OAE cualquier incidente de seguridad que afecte o pueda afectar la información, sistemas, accesos, bienes

o servicios involucrados en el contrato, dentro de un plazo máximo de 3 horas desde que tome conocimiento del incidente.

Esta notificación tendrá carácter de alerta inicial y deberá contener únicamente la información disponible que permita identificar la naturaleza del incidente y su eventual afectación a OAE, sin exigir en esta etapa un informe técnico adicional.

El adjudicatario deberá mantener informada a OAE sobre antecedentes relevantes a medida que estén disponibles. Cuando se encuentre sujeto a la obligación legal de reportar el incidente a la ANCI, podrá utilizar la información reportada a dicha Agencia para cumplir esta obligación, evitando generar reportes paralelos.

Las notificaciones deberán realizarse a través de las casillas que OAE informe para estos efectos. Esta obligación contractual no reemplaza ni modifica las obligaciones de reporte establecidas en la Ley N°21.663.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Soporte TI remoto
- Comunicaciones o telecomunicaciones
- Monitoreo de infraestructura crítica (física o digital)

3) Cláusula Eliminación segura de datos: El OAE será titular de todos los datos y registros generados durante la ejecución del contrato. El proveedor no podrá utilizarlos sin autorización escrita ni almacenarlos fuera de infraestructura aprobada.

Al término del contrato, el proveedor deberá eliminar dicha información, garantizando su irrecuperabilidad. El mecanismo a utilizar deberá ser propuesto por el adjudicatario y aprobado por el OAE, así como dar cumplimiento a los lineamientos o instrucciones que la Agencia Nacional de Ciberseguridad pudiera dictar en el futuro.

Para controlar este proceso, se llevará a cabo una reunión formal al finalizar el contrato, en la cual el proveedor deberá presentar evidencia de la eliminación segura de la información. Además, el proveedor deberá entregar un informe detallado que incluya la descripción de las acciones realizadas, el método utilizado para la eliminación, y cualquier otra evidencia necesaria para garantizar el cumplimiento de esta obligación.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- SaaS que almacenen o procesen información del OAE.
- Procesamiento de datos, analítica o inteligencia artificial.

4) Cláusula Acceso a sistemas del OAE: El proveedor deberá informar previamente al OAE los detalles del personal que accederá a los sistemas, incluyendo datos que identifiquen de manera única el 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 señaladas en la cláusula “Medidas de seguridad en el uso de equipos propios” de este contrato.

El OAE tendrá derecho ilimitado de acceso, inspección y auditoría, por sí o mediante un tercero designado, teniendo como único requisito dar un aviso previo de 1 día hábil. El ejercicio efectivo de este derecho no podrá verse obstaculizado o limitado por otros acuerdos contractuales o políticas del proveedor, quien, además tendrá la obligación de cooperar plenamente durante las inspecciones y las auditorías in situ *que* pudieran ser realizadas por la autoridad competente, el OAE o el tercero designado por este último.

Para controlar el cumplimiento de lo anterior, el proveedor deberá completar el “Anexo: Solicitud de Acceso a Sistemas” 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 el OAE a través del 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.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Mantenimiento de plataformas en la nube
- Software de gestión documental
- Integración de sistemas con plataformas estatales

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 el OAE:

- Tener un sistema operativo Windows, Linux o MacOS con actualizaciones continuas por parte del fabricante, incluyendo la recepción de parches de seguridad periódicos. Contar con un sistema de seguridad activo para proteger contra amenazas conocidas y mitigar el impacto de amenazas desconocidas.
- Implementar cifrado completo del disco duro utilizando BitLocker (Windows), FileVault (MacOS), LUKS (Linux) u otro que sea validado por el Departamento de Seguridad de la Información y Ciberseguridad o el equivalente del OAE.
- Aplicar parches de seguridad del sistema operativo en un plazo máximo de 7 días tras su liberación.
- Mantener el firewall local habilitado y configurado para restringir conexiones entrantes no autorizadas.
- Utilizar navegadores web actualizados a la última versión disponible.
- En el caso de que los equipos cuenten con sistemas de bloqueo biométricos, configurar su uso para que solo el trabajador asignado al equipo pueda desbloquearlo.
- Utilizar contraseñas robustas y configurar el bloqueo automático del dispositivo en caso de no uso por más de 2 minutos.
- Utilizar software original y descargado de fuentes oficiales y confiables.

Antes de autorizar el uso, el proveedor deberá presentar evidencia documentada de que cada dispositivo cumple con estos requisitos y estará sujeto a auditorías y evaluaciones por parte del OAE para verificar su cumplimiento durante la ejecución del contrato. La evidencia deberá ser enviada al Administrador del contrato del OAE y al Jefe de Seguridad de la Información y Ciberseguridad o similar del OAE, antes de la firma del contrato.

Estas medidas deberán ser declaradas como satisfactorias en el “Anexo: Solicitud de Acceso a Sistemas” y verificadas por el OAE dejando el resultado de esta verificación en el mismo anexo.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de auditoría o fiscalización en terreno
- Consultores externos que trabajan desde redes abiertas

6) Cláusula Auditorías y evaluaciones: El OAE podrá, eventualmente con el apoyo técnico de la ANCI (Agencia Nacional de Ciberseguridad), realizar auditorías, análisis forense o evaluaciones in-situ o remotas, previo aviso de 1 día hábil.

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 el OAE 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 del OAE. En este aviso se informará por parte del OAE, 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 del OAE.

En caso de que el proveedor no tenga disponibilidad para la actividad en la fecha propuesta, podrá solicitar, por una única vez, un día hábil adicional para su programación. Transcurrido dicho plazo, la inasistencia o falta de cumplimiento será considerada incumplimiento contractual y podrá dar lugar a la aplicación de las multas, amonestaciones e incluso del cese del contrato tal como está establecido en las presentes bases.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de mesa de ayuda
- Servicios de desarrollo de software

7) Cláusula Cooperación en incidentes de seguridad de la información y ciberseguridad: El proveedor deberá colaborar plenamente en la mitigación y resolución de incidentes que se originen en los bienes, servicios o entregables asociados al contrato.

El adjudicatario deberá entregar todos los antecedentes, registros y evidencias que le sean solicitados y que sean factibles de entregar en el marco de un incidente de seguridad que haya afectado a los sistemas involucrados en el contrato.

Asimismo, deberá implementar las medidas técnicas necesarias para generar, recolectar y conservar los logs y registros de eventos de los componentes de la solución o servicio contratado que resulten relevantes para la detección, análisis e investigación de incidentes de ciberseguridad. Estos registros deberán mantenerse disponibles por un período mínimo de un año y ser entregados a el OAE cuando sean requeridos en el contexto de un incidente.

Los registros deberán conservarse de manera que se resguarde su integridad, trazabilidad y disponibilidad, considerando que podrán constituir evidencia digital para el análisis de incidentes y, cuando corresponda, para procesos investigativos posteriores.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de datacenter
- Arriendo de notebooks

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 o equivalente del OAE todos los temas relacionados con la seguridad establecidos en este contrato. En caso que el adjudicatario sea un Servicio Esencial u Operador de Importancia Vital según la Agencia Nacional de Ciberseguridad, la persona designada debe encontrarse registrada en el portal de reportes de incidentes de la ANCI.

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”.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Desarrollo de software a medida
- Ciberseguridad administrada (NOC/SOC)

9) Cláusula Hallazgo y notificación de amenazas y vulnerabilidades: El proveedor deberá implementar mecanismos adecuados para identificar, evaluar y gestionar amenazas y vulnerabilidades de seguridad que puedan afectar a los sistemas, aplicaciones, servicios o componentes tecnológicos objeto del contrato.

En caso de detectarse una vulnerabilidad o amenaza de ciberseguridad que pueda comprometer la seguridad de los sistemas o servicios involucrados en el contrato, el proveedor tendrá la obligación de:

- Notificación inmediata: Informar al Contratante, dentro de un plazo máximo de 3 horas desde la detección, sobre la amenaza o vulnerabilidad encontrada, incluyendo un detalle preliminar de su naturaleza, alcance y riesgos potenciales.
- Análisis y plan de acción: Presentar, en un plazo no superior a 2 días hábiles, un análisis técnico que describa el impacto potencial de la vulnerabilidad o amenaza, las medidas de mitigación propuestas y un plan con plazos para su tratamiento.
- Ejecución de medidas: Corresponderá al adjudicatario implementar las acciones de corrección o mitigación, siempre que dichas acciones se encuentren comprendidas dentro del alcance y las obligaciones establecidas en el contrato. Estas deberán ejecutarse dentro de los plazos acordados con el OAE, dando prioridad a las vulnerabilidades clasificadas como críticas o de alto riesgo según estándares internacionales, tales como CVSS, y a las amenazas que representen un riesgo significativo para la seguridad o continuidad de los servicios contratados.
- Seguimiento y evidencia: Proveer evidencia de las acciones realizadas y resultados obtenidos, a solicitud de OAE.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Ethical hacking o pentesting con remediación
- Mantenimiento de software propio o de terceros
- Soporte de aplicaciones

10) Cláusula Notificación de cambios de infraestructura: El proveedor deberá notificar a OAE sobre cualquier cambio significativo en su infraestructura técnica, con al menos 10 días de antelación. Para controlar este proceso, el proveedor deberá informar estos cambios utilizando el formato de notificación definido en el “Anexo 4: Notificación de cambios de infraestructura” del contrato.

OAE se reserva el derecho de poner término al contrato, si el cambio en la infraestructura propuesta por el proveedor le genera grave riesgo en la seguridad de la información.

La notificación deberá enviarse a la o las casillas que serán proporcionada por OAE en la reunión de inicio sobre Seguridad de la Información y Ciberseguridad.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de hosting o housing
- Servicios de telecomunicaciones que administran enlaces

11) Cláusula Notificación de cambios en el personal con acceso a la información: El Proveedor deberá notificar a el OAE sobre cualquier cambio en el personal (ingresos,

reemplazos o egresos) que tenga acceso a la información del OAE, con al menos 24 horas de antelación. Para controlar este proceso, el Proveedor deberá informar estos cambios utilizando el formato de notificación definido en el “Anexo 5: Notificación de cambios en el personal con acceso a la información” del contrato.

La notificación deberá enviarse a la o las casillas que serán proporcionadas por el OAE en la reunión de inicio sobre Seguridad de la Información y Ciberseguridad.

De manera excepcional, en aquellos casos en que el cambio de personal constituya un evento que no pudo ser planificado (por ejemplo, renuncia imprevista, término inmediato de contrato u otra situación de fuerza mayor), el Proveedor deberá justificar debidamente esta circunstancia y notificar al OAE a la mayor brevedad posible, manteniendo en todo momento la trazabilidad y la seguridad del acceso a la información.

Asimismo, el proveedor deberá comunicar de manera inmediata al OAE, tan pronto como una persona autorizada cese su participación en el proyecto, y en ningún caso transcurridas más de tres (3) horas desde su desvinculación, a fin de que se proceda a la revocación oportuna de sus credenciales y privilegios de acceso. Cualquier incidente o perjuicio que derive del incumplimiento de esta obligación será de exclusiva responsabilidad del proveedor.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Call centers con acceso a datos de usuarios
- Soporte funcional a aplicaciones

12) Cláusula Declaración y validación de software utilizado en el proyecto: El adjudicatario deberá proporcionar al OAE un listado detallado de todo el software y librerías que utilizará para el desarrollo del proyecto, incluyendo el nombre, versión, propósito y titularidad de las licencias de cada uno de los softwares mencionados. Este listado deberá ser entregado antes del inicio del proyecto y actualizado en caso de cualquier modificación durante su ejecución.

Para controlar este proceso, el OAE requerirá que el adjudicatario complete, posterior a la adjudicación del contrato, el “Anexo 6: Declaración y validación de software utilizado en el proyecto”.

Además, el OAE podrá realizar auditorías periódicas para verificar la vigencia y legalidad de las licencias declaradas. En caso de incumplimiento, se aplicarán las sanciones establecidas en el contrato.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Desarrollo de software
- Servicio de herramientas de analítica de datos
- Servicios de automatización de procesos (RPA)

13) Cláusula Reuniones de inicio y coordinación periódica sobre Seguridad de la Información y Ciberseguridad: Al inicio del proyecto se realizará una reunión de inicio entre el Departamento de Seguridad de la Información y Ciberseguridad o el equivalente del OAE y el equipo del adjudicatario. Esta reunión inicial tendrá como propósito coordinar todos los temas relacionados con las distintas cláusulas de seguridad de la información y ciberseguridad estipuladas en el contrato, definir los procedimientos de trabajo y establecer los canales de comunicación y escalamiento para cualquier incidencia o consulta durante la ejecución del proyecto.

Durante la ejecución del contrato y hasta la finalización de éste, el Departamento de Seguridad de la Información y Ciberseguridad o el equivalente del OAE podrá solicitar una reunión de coordinación con el adjudicatario, a través del administrador del contrato. Estas

reuniones tendrán como objetivo coordinar y revisar temas generales relacionados con las cláusulas de seguridad de la información y ciberseguridad estipuladas en este contrato.

Las reuniones deberán contar, de manera obligatoria, con la participación del Jefe de Seguridad de la Información y Ciberseguridad o un cargo equivalente designado por el adjudicatario.

Para garantizar el cumplimiento, la solicitud de estas reuniones se realizará con un aviso previo de al menos 10 días hábiles.

El OAE llevará un registro de las minutas de estas reuniones, incluyendo acuerdos y acciones a realizar, para dar seguimiento a su cumplimiento.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Proyectos de infraestructura tecnológica
- Servicios de implementación de ERPs
- Servicios de consultoría en transformación digital

14) Cláusula Comunicación oficial entre adjudicatario y el OAE: Toda comunicación entre el adjudicatario y el OAE deberá realizarse exclusivamente a través de las herramientas de colaboración que el OAE disponga para estos fines. Asimismo, cualquier intercambio de información por correo electrónico deberá realizarse utilizando únicamente casillas de correo electrónico corporativas del adjudicatario, previamente registradas y autorizadas por el OAE.

Para garantizar el cumplimiento de esta directriz:

1. Las herramientas de colaboración serán comunicadas por el OAE, posterior a la adjudicación del contrato, y su uso será obligatorio para reuniones, intercambio de documentos y seguimiento de actividades relacionadas con el proyecto.
2. El adjudicatario será responsable de garantizar la integridad, confidencialidad, disponibilidad y autenticidad de la información comunicada mediante estas herramientas y sus casillas de correo corporativas.
3. El OAE se reserva el derecho de auditar las comunicaciones para asegurar que se ajusten a los estándares de seguridad establecidos en el contrato. Cualquier incumplimiento será reportado al administrador del contrato para la toma de acciones correctivas.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de gestión de proyectos
- Soporte de aplicaciones

15) Cláusula Política de Seguridad de la Información y Ciberseguridad del adjudicatario: El adjudicatario deberá disponer de medidas, herramientas y políticas de seguridad de la información que proporcionen un nivel adecuado de seguridad para la prestación de sus servicios y de los prestados por el OAE, de ser el caso. La política de seguridad de la información y ciberseguridad del adjudicatario deberá encontrarse aprobada, publicada y firmada por la máxima autoridad de su organización. Esta política deberá estar alineada con prácticas de los principales estándares de seguridad (ISO 27001, NIST, entre otros) y contemplar medidas específicas para la protección de la información, la gestión de incidentes de seguridad, y el cumplimiento de las obligaciones contractuales relacionadas con los clientes a los que presta servicios o disponibiliza un producto.

El adjudicatario deberá compartir con el OAE las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.

Para verificar el cumplimiento de esta directriz, el adjudicatario deberá:

1. Proporcionar una copia oficial de la política, firmada por la máxima autoridad de su organización, dentro de los 10 días hábiles posteriores a la firma del contrato.
2. Asegurar que la política se mantenga actualizada durante la vigencia del contrato y notificar a el OAE cualquier modificación relevante.
3. El OAE se reserva el derecho de revisar la política para garantizar que cumpla con los estándares requeridos y de solicitar ajustes si se detectan deficiencias o incumplimientos.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de cloud y almacenamiento

16) Cláusula Acreditación de inscripción ante la Agencia Nacional de Ciberseguridad (ANCI): En aquellos procesos de contratación en que el oferente tenga la calidad de Operador de Importancia Vital (OIV) o corresponda a una institución privada que preste servicios esenciales, conforme a lo establecido en la Ley N° 21.663, Ley Marco de Ciberseguridad, deberá acreditar su inscripción en el portal de notificación de incidentes de la Agencia Nacional de Ciberseguridad (ANCI).

Para estos efectos, el oferente deberá presentar, junto con su oferta, el certificado o comprobante oficial que acredite dicha inscripción, cuando corresponda conforme a la normativa aplicable.

Ejemplos de tipos de servicio o productos que podrían incluir esta cláusula:

- Servicios de telecomunicaciones y conectividad.
- Servicios de infraestructura digital, centros de datos y alojamiento de sistemas (hosting).

17) Cláusula Disponibilidad, portabilidad y restitución de la información: El adjudicatario deberá garantizar al OAE el acceso, disponibilidad y recuperación de toda la información almacenada, procesada o generada en el marco del contrato, durante su vigencia y al término de este, independientemente de la causa de su finalización.

El adjudicatario no podrá bloquear, restringir ni condicionar el acceso o la entrega de dicha información a la renovación del contrato, contratación de servicios adicionales o pagos distintos de aquellos expresamente establecidos en el contrato.

Para garantizar el cumplimiento de esta obligación, el adjudicatario deberá:

Restitución de la información: Entregar al OAE, cuando este lo solicite y al término del contrato, la totalidad de la información correspondiente, incluyendo los datos, documentos, registros y archivos asociados al servicio contratado.

Formato de entrega: Proporcionar la información en formatos abiertos, estructurados y de uso común, que permitan su lectura, utilización y migración hacia otras plataformas, sin generar dependencias tecnológicas innecesarias.

Continuidad del acceso: Mantener disponibles los mecanismos necesarios para consultar y recuperar la información durante el proceso de término o transición del servicio, conforme a los plazos y condiciones establecidos en el contrato.

Costos de restitución: Considerar dentro del precio del contrato todas las actividades necesarias para la extracción y entrega de la información, sin aplicar cobros adicionales por estos conceptos.

2. **PÚBLIQUESE** la presente resolución en el portal de transparencia de la Dirección para su debido conocimiento y difusión.

Anótese y Comuníquese

CRISTIAN CÉSPEDES VIÑUELA
DIRECTOR (S)
DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

VPC/CUE/PJR
REQ. 19021

Distribución:

- Dirección
- Fiscalía
- D. Comunicaciones
- D. Gestión Usuaria
- D. Compradores

Firmado electrónicamente por:

Cristian Céspedes Viñuela

Director (S)

Fecha: 20-10-2026 - 15:55:54



Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.

Para verificar la integridad y autenticidad de este documento inserte el código de verificación: DCCP-1921237218-140463

En: <https://gestorderequerimientos.azurewebsites.net>