CONSIDERACIONES CONTRACTUALES

SEGURIDAD DE LA INFORMACION, CIBERSEGURIDAD Y TRATAMIENTO DE DATOS PERSONALES PARA PROVEEDORES Y CONTRATISTAS

Fecha de última actualización: *05 de agosto de 2025*

Versión: *1.0*

I. INFORMACIÓN GENERAL

El presente documento contiene los estándares y directrices que SAAM ha implementado para regular la seguridad de la información, la ciberseguridad y el adecuado tratamiento de datos personales, dentro del marco de la relación que sostiene con sus proveedores de servicios.

En virtud de lo anterior, se establecen las obligaciones y los criterios de funcionamiento y conducta que deberá cumplir todo proveedor que tenga acceso a información de SAAM, información de sus sistemas y/o de sus titulares de datos personales.

Las consideraciones contractuales establecidas en el presente instrumento serán aplicables a todos los proveedores, contratistas o subcontratistas que mantengan relaciones comerciales con empresas del Grupo SAAM, sin excepción, y se entenderán formar parte integrante del acuerdo que regula la relación contractual entre SAAM y el proveedor.

Las disposiciones del presente instrumento establecen los estándares mínimos de seguridad y protección con que deberán cumplir los proveedores, contratistas y subcontratistas de SAAM, y que deberán ser observados durante la ejecución de los servicios contratados, así como en el manejo de cualquier información a la que tengan acceso en virtud de su relación contractual.

Las consideraciones contractuales establecidas en el presente documento responden a las disposiciones y exigencias de la legislación vigente que regula las materias de seguridad de la información, ciberseguridad y tratamiento de datos personales, en particular, la Ley N° 21.663 (Ley Marco de Ciberseguridad), la Ley N°21.459 sobre Delitos Informáticos, la Ley N°19.628 sobre Protección de la Vida Privada, y las normas y directrices de la Agencia Nacional de Ciberseguridad (en adelante, "ANCI").

Para efectos de la presente normativa, se entenderá por "Contrato" el acuerdo de prestación de servicios entre SAAM y el proveedor; por "Cliente" la empresa del Grupo SAAM que haya contratado dichos servicios, y por "Proveedor" el proveedor, contratista o subcontratista que presta servicios a SAAM.

II. SEGURIDAD DE LA INFORMACIÓN

1. Obligaciones generales de seguridad.

En virtud de la ejecución de los servicios objeto del Contrato, el Proveedor tendrá acceso a información del Cliente, de sus titulares de datos personales y de sus sistemas (los "Activos de Información"), los que deberán ser custodiados diligentemente y bajo los más altos estándares de cuidado.

El Proveedor responderá por la confidencialidad y seguridad de los Activos de Información que posee, custodia o controla, debiendo tomar las medidas de seguridad administrativas, técnicas y físicas apropiadas, asegurando la confidencialidad, disponibilidad, integridad y seguridad de los Activos de Información del Cliente que posee.

En este sentido, el Proveedor deberá cumplir al menos con las siguientes exigencias:

(i) El Proveedor deberá ejercer la supervisión necesaria y apropiada sobre sus empleados y sobre cualquier otra entidad que actúe en su representación, con el objetivo de mantener la confidencialidad, integridad, disponibilidad y seguridad de los Activos de Información del Cliente, y sus dependientes deberán mantenerlos en estricta confidencialidad, independientemente de que haya sido identificado expresamente como confidencial, siempre que por su naturaleza pueda razonablemente entenderse como tal. Esta obligación subsistirá por un período mínimo de diez (10) años desde la terminación del Contrato, o por un plazo superior si así lo exigen normas especiales, o mientras la información mantenga su carácter confidencial.

(ii) Para cualquier actividad que el Proveedor desarrolle dentro de instalaciones del Cliente, este acuerda cumplir con la totalidad de las medidas de seguridad respecto de los Activos Informáticos ya sean computadores personales, notebook, elementos de hardware o software, vigentes y con aplicación en los negocios del Cliente, o cualquiera de sus empresas relacionadas donde el Proveedor presta el Servicio, y respecto de cualquier Activo de Información al que tenga acceso. Toda vez que la prestación del Servicio tenga lugar en un inmueble donde el Cliente o cualquiera de sus filiales desarrolle actividades comerciales, el Proveedor cumplirá con el horario y disposiciones de trabajo, medidas de seguridad y esquema de acceso aplicables por el Cliente y cualquiera de sus personas relacionadas, según corresponda.

Cualquier acuerdo con terceros que presten servicios de *hosting* o *cloud* que el Proveedor use o en el futuro utilice para proveer servicios al Cliente, deberá sujetarse a los lineamientos del presente documento.

El Proveedor garantizará la trazabilidad continua de la información del Cliente y sus empresas relacionadas. Asimismo, cuando el Cliente solicite la eliminación o modificación de la información tratada por el Proveedor, éste cumplirá, y entregará evidencia, del cumplimiento de esta instrucción.

2. <u>Requerimientos externos de información</u>.

Si el Proveedor recibe un requerimiento de alguna autoridad o tribunal que solicite cualquier Activo de Información del Cliente o sus empresas relacionadas, el Proveedor deberá darle aviso de forma inmediata para que tenga opción de ejercer su derecho de defensa. Además, el Proveedor deberá cooperar razonablemente con el Cliente en dicha defensa.

Adicionalmente, el Proveedor deberá dar aviso de forma inmediata al Cliente si recibe:

(i) Solicitudes de titulares relacionadas con los Activos de Información del Cliente, incluyéndose solicitudes de Derechos ARCO de datos personales; o

(ii) Reclamos relacionados con materias de privacidad, confidencialidad o seguridad de la Información del Cliente.

Respecto a los avisos indicados en el numeral (i) y (ii) anterior, el Proveedor no deberá responder estas solicitudes o quejas sin la aprobación previa y por escrito del Cliente.

3. **Restitución o eliminación de información**.

El Proveedor deberá regresar o eliminar los Activos de Información del Cliente que posea, custodie o controle:

(i) Si el Cliente ya no la requiere para la prestación de los servicios, o bien, cuando concluya el Contrato, lo que suceda después; o

(ii) Cuando el Cliente así lo indique, lo cual podrá suceder en cualquier momento.

Cualquier eliminación de los Activos de Información del Cliente deberá garantizar que dicha información quede permanentemente ilegible e irrecuperable.

En la medida que el Proveedor tenga acceso o contacto con los Activos Informáticos del Cliente, deberá garantizar que ese acceso cesará en la fecha de terminación del Contrato.

A solicitud del Cliente, el Proveedor deberá proporcionar las certificaciones de un órgano externo que de fe del cumplimiento del Proveedor de la presente cláusula y de la entrega segura o eliminación y terminación de acceso de los Activos de la Información que posea en virtud del Contrato.

III. CIBERSEGURIDAD

1. **Estándares de ciberseguridad del Proveedor.**

Para efectos de este documento, se denominará "Activo Informático" a todos aquellos elementos relevantes para la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información del Cliente independiente de su formato, medio o soporte que la contenga, incluyendo hardware y software; y los equipos, redes y sistemas que soportan esta información y que permiten desarrollar las actividades comerciales y/o empresariales del Cliente, incluyendo las versiones en producción, de desarrollo, test, pre-producción o cualesquiera otras que fueran utilizadas con ocasión de la prestación de los servicios.

Con respecto a los Activos Informáticos del Cliente, el Proveedor se obliga a aplicar un grado de cuidado concordante con los más altos estándares de la industria en materia de ciberseguridad. En consecuencia, el Proveedor se obliga a implementar y mantener medidas de seguridad técnicas y organizativas que permitan prevenir, identificar, reportar y resolver adecuada y oportunamente cualquier vulnerabilidad o incidentes de seguridad durante la prestación de los servicios.

Para cumplir con este estándar general de cuidado, el Proveedor deberá contar con una estrategia, programa o política de ciberseguridad y seguridad de la información, o equivalente, que le permita llevar adecuadamente la información, contar con mecanismos de prevención de riesgos y vulnerabilidades, y la gestión de los mismos, procurando la continuidad de los servicios.

El Proveedor deberá informar anualmente al Cliente respecto de las prácticas de ciberseguridad y de seguridad de la información que tenga implementadas.

Adicionalmente, en caso de que el Proveedor posea certificaciones relativas a ciberseguridad, debe demostrar que obtuvo válidamente dicha certificación, así como su vigencia. Para estos efectos se considerará igualmente válida la acreditación por medio de informes de auditoría con vista externa o informes tipo SOC1 o SOC2.

Igualmente, el Proveedor deberá informar al Cliente respecto de todos los cambios en su entorno que afecten el negocio o la operación de sus servicios, tan pronto como tome conocimiento de aquellos.

2. **Cumplimiento de estándares de ciberseguridad y seguridad de la información del Cliente.**

El Proveedor declara conocer las disposiciones del presente documento y se obliga a cumplir con las obligaciones y exigencias de tratamiento de datos, ciberseguridad y seguridad de la información establecidas en el mismo.

Para dichos efectos, el Proveedor se compromete a capacitar al personal que destine para la prestación de los servicios, a fin de que conozcan las obligaciones y exigencias a la que estarán sujetos durante la prestación de los servicios y las cumplan íntegramente.

3. **Acceso a Activos Informáticos del Cliente.**

Cuando la prestación de los servicios requieran que el Proveedor acceda a equipamiento, redes, aplicaciones o cualquier Activo Informático del Cliente o sus filiales, el Proveedor se compromete a respetar las siguientes condiciones:

a) Utilizar el Activo Informático para el propósito exclusivo de ejecutar los servicios. En ningún caso, el Proveedor podrá utilizar dichos recursos para desarrollar programas o procesamiento de datos, para ninguna persona o entidad distinta al Cliente o sus filiales.

b) Los empleados del Proveedor, y los terceros por los que el Proveedor responde, no violarán, o intentarán violar, ninguno de los sistemas de seguridad del Cliente, u obtendrán, o intentarán obtener, acceso a ningún programa o dato fuera de lo que les pertenece o aquellos a los que se les ha otorgado acceso.

c) Utilizar todos los medios disponibles para evitar la introducción de virus en los Activos Informáticos del Cliente, e informar en forma inmediata de cualquier transgresión que detecte al respecto. El Cliente definirá el software de antivirus corporativo que se deba utilizar para tales efectos.

d) No intervenir el equipamiento ni el software básico bajo ningún aspecto que no sea el específico para el que fue contratado.

e) Mantener la política de "*un usuario, una cuenta*" para el acceso a todos los Activos Informáticos del Cliente, de forma que esta última pueda realizar las trazas de auditoría que estime pertinentes en los sistemas a los que ha otorgado permiso de acceso al Proveedor.

4. **Cumplimiento de estándares regulatorios de ciberseguridad.**

El Proveedor se obliga a cumplir con todas las exigencias regulatorias referidas a ciberseguridad, incluyendo las disposiciones de la Ley N°21.663 que le resulten aplicables en virtud de la naturaleza de los servicios que provee, o la calificación que le otorgue la Agencia Nacional de Ciberseguridad (la "ANCI" o "Agencia"), según corresponda.

El Proveedor deberá informar al Líder de Ciberseguridad del Cliente, a través del correo electrónico cybersegurity@saam.com, y dentro del plazo de cinco (5) días hábiles, cualquier modificación que sufra en cuanto a la calificación que le otorgue la Agencia. Cualquier incumplimiento en esta materia será concebido como un Incidente de Seguridad, en los términos establecidos en la presente cláusula.

5. Prevención de delitos informáticos.

Para efectos del presente documento, se entenderá por "Delitos Informáticos", aquellos establecidos en la Ley N° 21.459 sobre delitos informáticos.

El Proveedor se obliga a implementar medidas técnicas y organizativas que permitan prevenir e identificar adecuada y oportunamente la comisión de delitos informáticos por parte del personal que designa para la prestación de los servicios, o por parte de terceros vinculados.

Para efectos de los servicios objeto del Contrato, el actuar del personal del Proveedor que constituya o pueda constituir una o más conductas tipificadas como delitos informáticos se considerarán Incidentes de Seguridad, por lo que el Proveedor deberá notificar al Cliente de dichas conductas dentro de los plazos y acorde procedimientos establecidos en el apartado siguiente sobre "Incidentes de Seguridad".

El Proveedor se obliga a capacitar periódicamente a su personal en relación con las conductas tipificadas como delitos informáticos y las sanciones consagradas en la Ley N°21.459 y los demás instrumentos normativos que la complementen, sustituyan y/o supriman. Asimismo, el Proveedor garantiza que capacitará en esta materia a todo nuevo dependiente, colaborador o tercero que se incorpore o intervenga en la prestación de los servicios, previo a que inicie la ejecución de sus funciones.

El Proveedor reconoce que el Cliente podrá exigir evidencia documental de la ejecución de las capacitaciones pertinentes, incluyendo los contenidos y evaluaciones asociadas.

6. Incidentes de Seguridad.

Para efectos del presente documento, se considerará "Incidente de Seguridad" a todos los eventos que afecten o potencialmente puedan afectar de manera negativa:

(i) La confidencialidad, disponibilidad o integridad de los Activos Informáticos o Activos de Información del Cliente;

(ii) La disponibilidad y resiliencia de los Activos Informáticos utilizados durante las operaciones del Cliente ya sean propiedad de este, del Proveedor o proporcionados al Cliente por terceros proveedores, así como de sus Activos de Información;

(iii) La autenticación de los procesos ejecutados o implementados en relación con los Activos Informáticos o el acceso a los Activos Informáticos;

(iv) Los estándares de cumplimiento y obligaciones establecidas por este Contrato en materia de ciberseguridad, seguridad de la información y prevención de delitos informáticos; y

(v) En general, cualquier hecho o circunstancia que afecte o pueda afectar de manera negativa al Cliente, ya sea desde el punto de vista de su operación o de los servicios convenidos en virtud del Contrato.

Cada vez que el Proveedor tome conocimiento de un Incidente de Seguridad deberá notificar al Cliente a través del Líder de Ciberseguridad, tan pronto tome conocimiento de esta circunstancia y, en cualquier caso, dentro del plazo máximo de doce (12) horas contadas desde la ocurrencia del Incidente de Seguridad, a través del medio más expedito con el que se cuente y, en caso de ser vía

oral, se deberá formalizar luego por escrito vía correo electrónico. Dicha notificación deberá contener, al menos, el siguiente detalle:

a) Fecha y hora de ocurrencia del Incidente de Seguridad.
b) Descripción detallada del Incidente de Seguridad, considerando especialmente la duración, los sistemas o recursos informáticos afectados, las categorías de información afectadas, incluyendo si existen datos personales involucrados, personas naturales y/o jurídicas afectadas, extensión geográfica y cualquier otro aspecto esencial.
c) Índices de compromiso del Incidente de Seguridad, en caso de encontrarse identificados y/o delimitados al momento de enviar la notificación.
d) Consecuencias posibles o identificadas para el Cliente, detallando la gravedad e impacto correspondientes.
e) Si procede, las repercusiones transfronterizas del incidente.

En caso de no contar con toda la información indicada previamente, el Proveedor deberá efectuar la notificación del Incidente de Seguridad, con la información que disponga, quedando obligado a complementar su contenido en reportes periódicos.

7. Obligaciones del Proveedor frente a Incidentes de Ciberseguridad.

En caso de identificarse o de existir una sospecha razonable de la ocurrencia de un Incidente de Seguridad, el Proveedor estará obligado a adoptar medidas dirigidas a resolverlo y evitar su repetición, y las medidas de mejora continua que se ejecutarán inmediatamente resuelto el Incidente de Seguridad con la finalidad de eliminar la vulnerabilidad.

En relación con estas obligaciones, el Proveedor deberá:

a) Permitir la participación y cooperación, continua y permanente, del personal que razonablemente designe el Cliente, tanto interno o externo, en la solución del Incidente de Seguridad.

b) Implementar medidas de mitigación temporales orientadas a solucionar el Incidente de Seguridad y/o reducir sus consecuencias perjudiciales para el Cliente. Una vez reportado el Incidente de Seguridad el Proveedor solicitará la autorización previa, específica y escrita del Cliente para la adopción de estas medidas.

c) Permitir el acceso a sus instalaciones, infraestructura y/o sistemas informáticos al personal que designe el Cliente para cooperar y/o gestionar la resolución del Incidente de Seguridad.

d) Enviar reportes periódicos al Cliente sobre el control, gestión y solución del Incidente de Seguridad. Estos reportes periódicos deberán ser enviados cada 12 (doce) horas a partir de la notificación del Incidente de Seguridad y deberán detallar, al menos, los siguientes aspectos:
   (i) la evolución del Incidente de Seguridad;
   (ii) la aplicación y eficacia de las medidas implementadas;
   (iii) actualizaciones respecto de la duración, sistemas o recursos informáticos afectados, personas naturales y/o jurídicas afectadas y extensión geográfica del Incidente de Seguridad; y
   (iv) cualquier otro elemento que resulte relevante para el control, gestión y/o solución del Incidente de Seguridad.

e) Proporcionar al Cliente toda la información, documentación y antecedentes que esta requiera para controlar, gestionar y/o solucionar el Incidente de Seguridad.

f) Adoptar las medidas permanentes necesarias para resolver de manera definitiva el Incidente de Seguridad, resguardar la integridad del Cliente, y asegurar la continuidad operativa de los servicios. El Cliente evaluará estas medidas y podrá sugerir modificaciones en consideración a las prácticas de la industria y su propio conocimiento de los servicios, las que deberán ser aplicadas por el Proveedor.

g) Adoptar las medidas de mejora continua necesarias para eliminar la vulnerabilidad que dio origen al Incidente de Seguridad. El Cliente evaluará estas medidas y podrá sugerir modificaciones en consideración a las prácticas de la industria y su propio conocimiento de los servicios, las que deberán ser aplicadas por el Proveedor.

h) Remover inmediatamente de la prestación de los servicios al personal (incluyendo mandatarios) del Proveedor que esté o pueda estar involucrado en conductas tipificadas como delitos informáticos por la regulación aplicable; y asociar estas conductas a causales de terminación de los contratos entre el Proveedor y su personal.

i) Participar activamente en el proceso de análisis forense que el Cliente, a su entera discreción, determine realizar para investigar las causas del Incidente de Seguridad. Para estos efectos, y sin que la siguiente enumeración sea taxativa, el Proveedor deberá:
   (i) instruir a su personal para que participe y coopere activamente en la entrega de la información que el Cliente requiera;
   (ii) permitir y facilitar al Cliente el acceso a los equipos o infraestructura en investigación, con el objetivo de encontrar la causa raíz y tomar acciones efectivas posteriores al Incidente de Seguridad.

   Lo anterior se entiende sin perjuicio del análisis forense que por su parte realice el Proveedor.

8. <u>Conductas riesgosas del Proveedor</u>.

El Proveedor deberá monitorear y controlar proactivamente el actuar de su personal, y adoptar las medidas necesarias para prevenir y evitar conductas riesgosas, entendidas como cualquier actividad no sea concordante con el grado de cuidado que debe emplear el Proveedor en virtud del presente documento.

Se considerarán como conductas riesgosas, sin que el siguiente listado sea taxativo, las siguientes:

(i) Uso de redes inseguras o conexiones públicas sin cifrado.
(ii) Acceso a sitios web maliciosos desde dispositivos de trabajo o dispositivos personales que utilicen credenciales provistas por el Proveedor.
(iii) Uso de medios de almacenamiento no autorizados por el Cliente, según los términos y condiciones de los servicios.
(iv) Utilización de equipos no protegidos con antivirus o con softwares de seguridad desactualizados.
(v) El compartir con terceros, información crítica, tales como claves, contraseñas, nombres de usuarios, firma electrónica u otros, cuyo mal uso pueda generar perjuicio al Cliente.
(vi) El incumplimiento de políticas de escritorio limpio, incluyendo la falta de bloqueo del equipo al dejarlo desatendido, o el descuido de los equipos personales, dejándolos en

lugares inseguros tales como espacios compartidos de trabajo sin candado de seguridad, al interior de vehículos, entre otros.

(vii) La ausencia de mecanismos o la implementación inadecuada de mecanismos de prevención, capacitación y control en relación con conductas tipificadas como delitos informáticos por parte de la regulación aplicable.

IV. TRATAMIENTO DE DATOS PERSONALES

Para efectos de la presente cláusula, se entenderá por "Datos Personales" o "Datos de Carácter Personal" aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

1. Cesión de Datos Personales de Interlocutores.

En virtud de los servicios, el Proveedor, en calidad de responsable del tratamiento, cederá al Cliente datos personales de representantes, trabajadores e interlocutores ("Datos de los Interlocutores"). Esta cesión se realiza en virtud del interés legítimo del Cliente, en su calidad de cesionario.

La cesión incluirá datos de contacto de los interlocutores e información relativa a las funciones o puestos desempeñados por aquellos.

En relación con los Datos de los Interlocutores cedidos, el Proveedor:

(i) Declara expresamente que los Datos de los Interlocutores objeto de esta cesión han sido recopilados, almacenados, tratados y, especialmente, cedidos al Cliente en cumplimiento de las disposiciones de la regulación aplicable en materia de protección de datos personales, especialmente aquellas contempladas en la Ley N°19.628 sobre Protección de los Datos Personales (la "Regulación Aplicable").

(ii) Declara y garantiza que cuenta con las bases de licitud necesarias para ceder al Cliente los Datos de los Interlocutores y permitir el posterior tratamiento por parte de ésta y, cuando sea necesario en conformidad a la legislación aplicable.

(iii) Se obliga a mantener indemne y a asumir la defensa del Cliente frente a cualquier reclamación que se origine o relacione, directa o indirectamente, con cualquiera de las declaraciones y obligaciones consagradas en esta cláusula.

Los Datos de los Interlocutores serán tratados por el Cliente con la exclusiva finalidad de gestionar la celebración, ejecución y cumplimiento de la prestación de los servicios, la relación comercial entre ambas partes y las disposiciones de este Contrato.

Cada Parte es plenamente responsable del tratamiento de los Datos de los Interlocutores que realice en calidad de responsable independiente; y no existirá corresponsabilidad entre las Partes.

2. Tratamiento de Datos Personales de Proveedor Persona Natural.

En caso de que el Proveedor sea una persona natural, ésta declara conocer y aceptar que el Cliente, en su calidad de responsable de datos deberá recolectar, almacenar, comunicar, transferir y, en general, hacer tratamiento de los datos personales que le sean entregados con ocasión de la celebración y ejecución de este contrato ("Datos Personales del Proveedor").

El Cliente tratará los Datos Personales del Proveedor cuando resulte estrictamente necesario para la ejecución de los derechos y obligaciones establecidos en el Contrato y llevará a cabo el tratamiento con sujeción a lo establecido en la Regulación Aplicable.