Anexo N°6

ANEXO CLÁUSULAS DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN EN CONTRATOS DE TECNOLOGÍAS

Ministerio de Salud

Versión 2.0.0

octubre 2018

Índice

1.- CUMPLIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Por el sólo hecho de participar en el presente procedimiento de compras, el oferente debe dar cumplimiento a las Políticas y Procedimientos vigentes de Seguridad de la Información del Ministerio de Salud, publicadas en el link:

http://web.minsal.cl/seguridad_de_la_informacion

las cuales se presumen conocidas por el oferente, para todos los efectos legales. Para estos efectos, el trabajo o proyectos realizados por el proveedor para el contratante, deben asimismo cumplir con los estándares de seguridad de la información establecidos por MINSAL.

Todo el personal que desarrolle labores para el contratante deberá dar estricto cumplimiento a la Política General de Seguridad de la Información, observando sus directrices y colaborando en su aplicación dentro de su ámbito de acción.

En caso de incumplimiento de cualquiera de estas obligaciones, el contratante se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como las sanciones legales y contractuales, que se consideren pertinentes en relación a la empresa o persona contratada. Bajo ninguna circunstancia este hecho relevará a la Empresa de las responsabilidades y obligaciones que le impone el Contrato.

2.- GESTION DE SEGURIDAD

a.- Plan de Gestión Integral de Seguridad

Se deberá contar con un plan de gestión integral de seguridad, que considere auditorías internas y externas con validación de resultados y metodologías de trabajo en este aspecto, de acuerdo a los estándares vigentes.

Todo proyecto de desarrollo o mantención de software contará con los mecanismos de auditoría de seguridad de la información, los registros, responsables y los periodos de revisión, debiendo conservar los registros de auditoría de las actividades que se realicen, incluyendo administradores y operadores, de las excepciones o incidentes de información y mantenerlos durante un período acordado para ayudar en investigaciones futuras y en el seguimiento y monitoreo del control de acceso.

MINSAL podrá realizar auditorías a los procesos, controles de desarrollo y soluciones de los proveedores para verificar su nivel de seguridad. Verificado un quiebre de seguridad, el proveedor deberá realizar las acciones de mitigación de los eventuales daños o fugas de datos, además de mantener un plan de acción que garantice la continuidad operacional.

Sin perjuicio de la obligación del proveedor de realizar acciones de monitoreo permanente de seguridad, MINSAL asimismo realizará auditorías de seguridad de los sistemas propios y de los proveedores.

Los proveedores deben contar con un sistema de gestión de vulnerabilidades, con un modelo ágil de solución de todas las vulnerabilidades detectadas aunque aún no hayan sido explotadas. El proveedor se compromete a informar a MINSAL sobre el nivel de riesgo y vulnerabilidades conocidas y/o de las que tome conocimiento durante la vigencia del contrato y las medidas de mitigación que se adopten.

Todo proveedor debe garantizar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a resguardar la confidencialidad de la información a la que tenga acceso y a cumplir las Políticas de Seguridad de la Información de MINSAL.

El Procedimiento de Gestión de Vulnerabilidades e Incidentes de Seguridad de la Información considerará como mínimo las siguientes actividades:

- El proveedor deberá realizar cada tres meses un escaneo de la plataforma y del propio software en busca de vulnerabilidades, manteniendo un registro de los resultados.
- Si se detectare alguna vulnerabilidad, deberá desarrollar las acciones correctivas y preventivas que sea necesario para mantener niveles altos de seguridad del sistema, lo que deberá quedar debidamente registrado en el sistema de gestión de incidentes.
- Si la vulnerabilidad detectada tuviere el carácter de crítica a juicio del Ministerio, según definición normativa que será informada al adjudicatario con la debida antelación, se deberá gatillar de inmediato una revisión preventiva general del sistema.

b.- Gestión de pruebas

Los sistemas nuevos y actualizaciones se deberán someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallado y entradas de pruebas y los resultados esperados bajo una variedad de condiciones. Las pruebas pueden ser ejecutadas por personal de MINSAL o por un tercero previamente seleccionado por MINSAL.

Pruebas de seguridad de los sistemas.

Los sistemas nuevos y actualizaciones se deberán someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallado y entradas de pruebas y los resultados esperados bajo una variedad de condiciones.

Pruebas de aceptación de los sistemas.

Se deberán establecer programas de pruebas de aceptación y criterios relacionados para los sistemas de información, actualizaciones y nuevas versiones.

Las pruebas de aceptación del sistema deberán incluir las pruebas de los requisitos de seguridad de la información y la adherencia a las prácticas de desarrollo del sistema seguro.

Protección de los datos de prueba.

Para los casos que se requieran datos de prueba, no se deberán usar datos operacionales que contengan información personal identificable o cualquier otro tipo de información confidencial.

En aquellos casos que el contratante autorice el uso de datos operacionales para la realización de pruebas, deberán utilizarse técnicas de anonimización o en su defecto de seudonimización, debiendo establecerse un sistema seguro de almacenamiento de los mecanismos y medios de reidentificación.

3.- CONFIDENCIALIDAD DE LA INFORMACIÓN

Cualquier tipo de intercambio de información, cualquiera sea su naturaleza que se produzca entre el contratante y sus organismos relacionados y el proveedor, sus dependientes, subcontratistas y personas relacionadas, cualquiera sea el formato y medio a través del cual se haga llegar al proveedor, tendrá el carácter de confidencial. Todo uso que realice el proveedor se deberá llevar a cabo dentro del marco establecido por el contrato de provisión de servicios correspondiente. Por tanto queda estrictamente prohibido cualquier uso de esa información fuera de dicho marco, o para finalidades distintas al cumplimiento de las obligaciones que emanan para las partes del respectivo contrato.

Cada parte deberá informar inmediatamente y en la forma más expedita posible a la otra, si tuviere conocimiento de cualquier incidente que pueda ocasionar la fuga, mal uso o apropiación indebida de la información, especialmente tratándose de los datos personales.

Consecuentemente, el proveedor está obligado a:

- Abstenerse de utilizar la información para su propio beneficio o con cualquier otro propósito distinto al de prestar los servicios en los términos y condiciones establecidos en el contrato.
- Jamás revelar información de los contratantes a terceros, excepto a aquellos de sus empleados o asesores, que requieran conocer dicha información a fin de poder prestar el referido servicio.
- Adoptar todas las medidas necesarias y conducentes para proteger la confidencialidad y evitar la divulgación y uso indebido de la información.

- Adoptar las medidas técnicas y organizativas conducentes a evitar el tratamiento de datos personales fuera del marco de la finalidad asociada al cumplimiento de las obligaciones que emanan del contrato, evitando realizar cualquier operación de tratamiento de datos personales no autorizado por el contratante.
- Hacerse responsable por los hechos de sus dependientes y personal asociado que hayan entrado en contacto con la información, que impliquen una infracción a los deberes de confidencialidad, reserva y secreto establecidos en el contrato y la legislación vigente.
- Informar al contratante sobre cualquier incidente que afecte la confidencialidad de la información y especialmente los datos personales a que se tenga acceso con ocasión del contrato.

La infracción a estos deberes será constitutiva de incumplimiento grave a las obligaciones del contrato.

Con todo, aún si la información fuera divulgada con antelación a la suscripción del contrato o posteriormente, como resultado de una exigencia de una autoridad judicial o administrativa, el contratante no podrá utilizar la información para finalidades ajenas al contrato. En el caso que por requerimiento de autoridad judicial y/o administrativa el proveedor se vea compelido a revelar la información confidencial, deberá notificar de esta circunstancia al contratante, por la vía más expedita posible.

Al momento del término, por cualquier causa, del contrato, la Empresa debe restituir, según lo indique el contratante, toda la información relevante y especialmente la información confidencial y toda copia, resumen o extracto de ésta, contenida en cualquier documento de trabajo, memorandos u otros escritos, medios magnéticos o archivos computacionales, sin retener copias, resúmenes o extractos de la misma, en ninguna forma, debiendo cancelar en sus sistemas toda la información a que haya tenido acceso con ocasión del contrato, quedando facultado desde ya el contratante para verificar esta circunstancia.

La obligación de confidencialidad de la información tiene una duración indefinida, a contar de la fecha de suscripción del Contrato.

En todo caso, el MINSAL dará una aplicación sistémica y concordante a la obligación de confidencialidad con la de transparencia, establecida en la ley 20.285.

4.- PROPIEDAD INTELECTUAL

El proveedor, deberá garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual. Consecuentemente, el incumplimiento de esta circunstancia no podrá acarrear ningún tipo de responsabilidad

para el contratante, debiendo éste hacerse cargo de cualquier reclamo de tercero en esta materia.

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

Todos los bienes y activos de propiedad intelectual del oferente o adjudicatario se mantendrán bajo la titularidad, salvo acuerdo expreso y por escrito que disponga lo contrario. Asimismo, cualquier información que MINSAL ponga a disposición del proveedor, ya sea en la fase de licitación, adjudicación o ejecución del contrato, se considerará de titularidad del Ministerio y se regirá por lo dispuesto en el acápite de responsabilidad.

Sin perjuicio de lo dispuesto en esta cláusula, cuando se prevea esta circunstancia, las licencias correspondientes serán transferidas al Ministerio una vez concluido este contrato, quedando prohibido al proveedor su uso posterior sin el consentimiento expreso del MINSAL.

5.- CALIDAD DE TRATAMIENTO DE DATOS

Los datos personales tratados a través de los sistemas del MINSAL corresponden a sus titulares. Su protección se encuentra garantizada en el artículo 19 Nº 4 de la Constitución Política de la República de Chile. Toda persona que entre en contacto con un dato personal de un tercero deberá guardar la debida diligencia en su custodia, haciéndose responsable de las pérdidas, daños y quiebres de seguridad.

En el tratamiento de datos debe respetarse, además la normativa aplicable en relación al tratamiento de datos de salud, contenida en el DFL Nº 1, de 2006 del Ministerio de Salud, la ley 20.584 de derechos y deberes del paciente, 20.120 sobre investigación científica en personas humanas, y las demás leyes y normativa complementaria del sector salud. Esta información tiene el carácter de sensible y por tanto sólo puede ser objeto de tratamiento en las hipótesis que prevé y autoriza el legislador o con el consentimiento de los titulares.

1.- Mecanismos de control y seguimiento de datos

El proveedor deberá implementar sistemas de acceso seguro a los datos, debiendo cada usuario acceder sólo a aquellos respecto de los cuales tiene permisos habilitados a través de sus perfiles de usuario o las condiciones legales de acceso, de acuerdo a sus competencias, tratándose de información sensible, como la información de salud de pacientes.

El proveedor deberá establecer mecanismos de comunicación segura de datos, cualquiera que sea la el medio o técnica utilizada para su transferencia o comunicación desde el origen hasta el usuario requirente, utilizando mecanismos de seguridad consecuentes a un nivel alto de protección consistente con el medio en el cual se transferirá o comunicará la información.

Cualquiera que sea el medio o técnica de transferencia o comunicación de los datos, en el sistema deberá quedar registro auditable (log) con la identificación del usuario que accede a los datos (requirente), la descripción del contenido al que accede, el motivo o propósito del acceso y destinatario de la información. Esta información quedará a disposición del contratante de manera permanente.

2.- Formatos de salida

El proveedor deberá respetar los siguientes formatos para archivos electrónicos:

Informes: si el informe contiene sensible, deberá formatearse a un archivo que soporte la apertura con una contraseña segura que deberá contener caracteres alfanuméricos, la que deberá mantenerse bajo el estricto control del requirente. La información, deberá estar acotada según el perfil de acceso del usuario que esté realizando la solicitud.

Planillas: en el caso de que la información sea necesaria para realizar gestión, esa deberá entregarse en formatos que soporten una estructura de datos y la apertura con una contraseña segura que deberá contener caracteres alfanuméricas, la que deberá mantenerse bajo el estricto control del requirente.

3.- Medio de transporte

Móvil o correo electrónico: Si la información se transfiere a través de un dispositivo de almacenamiento móvil o enviada a través de un correo electrónico, esta deberá estar protegida por un sistema de encriptación (*). Sólo el requirente o receptor habilitado podrá desencriptar dichos datos de acuerdo al procedimiento establecido por el proveedor. No se podrá enviar información a correos que no sean los institucionales.

(*) Algoritmos o estándares de criptografía:

- PGP (Pretty Good Privacy)

- MD5 (Message-Digest Algorithm 5)

- CRC (Cyclic Redundancy Check)

- Sha (Secure Hash Algoritm)

Deben incluirse medidas técnicas y administrativas que permitan detectar de manera temprana cualquier vulneración al sistema de encriptación.

4.- Alojamiento de datos en servidores

Los sistemas de acceso remoto a datos deberán ser diseñados de forma tal que sólo puedan ser accedidos desde dentro de la Red de comunicaciones del Ministerio, con canales de comunicación seguros y debidamente protegidos con nombre de usuario y contraseña segura. De todo proceso que se lleve a cabo sobre el sistema o los datos debe quedar registros detallados y auditables en el sistema, que contengan al menos la identificación del usuario que accede a los datos (requirente), la descripción del contenido al que accede, el motivo o propósito del acceso, operaciones de tratamiento realizadas y destinatarios de la información.

Los sistemas deberán considerar sistemas de respaldo que permitan la recuperación segura de la información en tiempos razonables para procesos críticos de información, desde la óptica de continuidad de servicios.

5.- Modificación y destrucción de datos

El proveedor realiza tratamiento de datos personales por mandato del contratante. En estas circunstancias, toda modificación, cancelación o destrucción de datos debe realizarse de acuerdo a estándares generalmente aceptados, siempre por instrucciones del mandante, debiendo dejarse acta de las operaciones realizadas.

Los dispositivos digitales y magnéticos deben ser sometidos a procedimientos de formateo seguro antes de ser descartados.

En los procesos de digitalización de información queda prohibido a los proveedores destruir o descartar los originales sin la autorización del mandante.

6.- HERRAMIENTAS DE SEGURIDAD

Como parte de las soluciones de seguridad que deben estar en los procesos de compra y ofertas de los proveedores se debe considerar tanto herramientas que cubran la capa de Telecomunicaciones, como la capa de aplicaciones y sistemas de base.

Las medidas de protección que se deberán considerar, deben cubrir los siguientes aspectos:

- Prevención de intrusiones ilegítimas
- Firewall de última generación para acceso.
- Firewall de aplicaciones

- Escáner de vulnerabilidades de los sistemas base (S.O., componentes de software del servidor, etc.)
- Herramientas para escáner de aplicaciones
- DLP con el fin de proteger información confidencial de Minsal y la propiedad intelectual almacenadas, en uso o en tránsito dentro de las dependencias del contratante o la red del proveedor.
- Protección antimalware.
- Certificados digitales
- Herramientas de seguridad que se correspondan con los estándares vigentes.

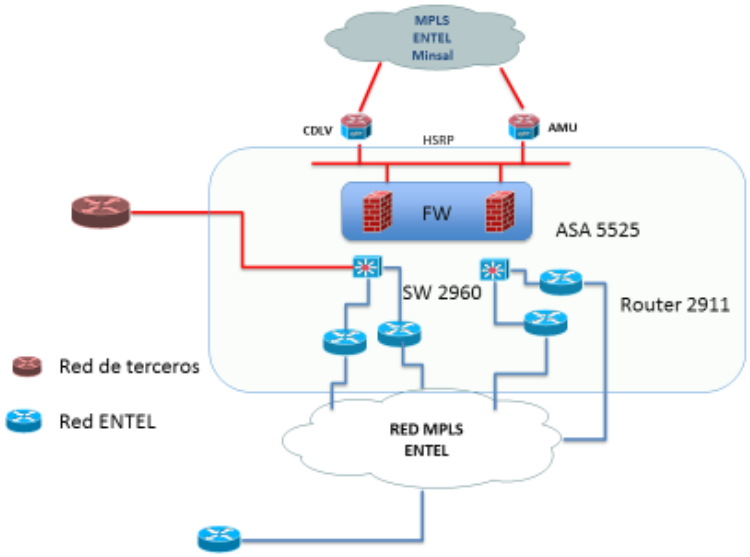
7.- INFRAESTRUCTURA PARA PRODUCCIÓN

Para la puesta en producción de los sistemas de información, se deberá implementar en un datacenter de acuerdo al grado de disponibilidad, acceso e integridad que la información requiera. En el caso de los sistemas de registro clínico electrónico, cuya información es de carácter reservada, la infraestructura mínima es TIER III u homologado, con un tiempo de disponibilidad de 99.982% lo que implicará un máximo de 1,57 horas de tiempo de parada al año.

Por la naturaleza del sistema, y los requerimientos de disponibilidad, acceso e integridad requiere contingencia, la cual podrá ser en un data center TIER III u homologado.

NOTA: Para las definiciones de las infraestructuras se deberán referir al estándar TIA-942 y sus actualizaciones.

La solución debe estar conectada a través de la Red de comunicaciones privada de MINSAL, como se muestra en la siguiente imagen, del diagrama de terceros:



8.- CONTROL DE CAMBIOS EN LOS SISTEMAS.

Los cambios a los sistemas dentro del ciclo de vida de desarrollo deben ser controlados mediante procesos de control de cambios formales.

La introducción de nuevos sistemas y cambios importantes a los sistemas existentes debe seguir un proceso y registro de documentación, especificación, pruebas, control de calidad e implementación administrada.

9.- ENTREGA DE SISTEMAS Y DATOS AL TÉRMINO DEL CONTRATO.

En los contratos de provisión de Software como Servicio (SaaS), como actividad de cierre de contrato y cumpliendo con el compromiso de garantizar la continuidad de servicio, el Proveedor deberá efectuar todas las actividades necesarias para dejar operativos los aplicativos, bases de datos y software base en la plataforma entregada por MINSAL, equivalente a la que se encuentre en operación en ese momento.

Para ello, el proveedor saliente deberá realizar al menos las siguientes actividades:

a) Entrega de la totalidad de la información pertinente que el MINSAL o terceros determinados por el proveedor entrante le requieran para garantizar la continuidad operacional.
b) Entrega de todos los datos que son tratados por el sistema; las aplicaciones funcionando y envasadas, junto con procedimientos de instalación garantizados.
c) La especificación de cada componente del sistema.
d) MINSAL podrá requerir que el Proveedor deje el ambiente operativo funcionando y con procedimientos de instalación de plataforma de software garantizado, o el ambiente operativo y las aplicaciones y los datos instalados en una plataforma diferente, pero equivalente a la de la operación vigente.
e) Cualquier otro elemento necesario para mantener la continuidad operacional del MINSAL de manera comparable al período de vigencia del contrato correspondiente.

10.- NORMATIVA SOBRE SEGURIDAD DE LA INFORMACION

El proveedor deberá dar cumplimiento a la normativa vigente aplicable al contrato. En especial deberá dar cumplimiento a los siguientes cuerpos normativos:

- Normativa del sector salud: DFL Nº 1, de 24 de abril de 2006, Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley Nº 2.763, de 1979 y de las leyes Nº 18.933 y 18.469; DFL Nº 725, Ministerio de Salud, Código Sanitario; la Ley N°20.584, referida a Deberes y Derechos que tienen las Personas en relación con acciones vinculadas a su Atención de Salud; Decreto Nº 41, de 24 de

julio de 2012, del Ministerio de Salud, Reglamento de Ficha Clínica; Decreto Nº 31 de 15 de junio de 2012, del Ministerio de Salud, Reglamento sobre entrega de información y expresión de consentimiento informado en las atenciones de salud; la ley 20.724, de 2014, que modifica el Código Sanitario en materia de regulación de medicamentos; ley 20.850, de 2016, que crea un sistema de protección financiera para diagnósticos y tratamientos de alto costo y rinde homenaje póstumo a don Luis Ricarte Soto Gallegos; ley 19.966, de 2004, que establece un régimen de garantías de salud; ley 19.650, que perfecciona normas del área de la salud; ley 20.120 de 22 de septiembre de 2006, sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana y demás normativa del área de la salud.

- En materia de documentos electrónicos: Ley 19.799 de 12 de abril de 2002 y su normativa complementaria, especialmente el Decreto Supremo N°83, del Ministerio secretaría General de la Presidencia, publicado el 12 de enero de 2005 en el Diario Oficial; El Decreto Nº 14, de 2014, del Ministerio secretaría General de la Presidencia, el decreto Nº 1 de 2015, del Ministerio secretaría General de la Presidencia.

- En materia de protección de datos personales: el art. 19 Nº 4 de la Constitución Política de la República y la ley de protección de datos personales N° 19.628 y su normativa complementaria;

- En materia de delitos informáticos: lo dispuesto en la ley 19.223 sobre delitos informáticos.

En caso de que alguna de estas normas sea modificada o sustituida el proveedor deberá adaptarse a los requerimientos de la nueva normativa.