CLÁUSULAS DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN PARA CONTRATOS DE TECNOLOGÍAS

Hospital de Tomé

Versión 4.4

Agosto 2026

ÍNDICE

A. MARCO DE DEFINICIONES

Para los efectos de la aplicación de este documento, los términos que a continuación se señalan tendrán el significado que se indica:

- **Activos de información**: toda información o recurso relacionado para la creación, almacenamiento, gestión o transmisión de dicha información. Podrán ser activos materiales (RRHH especializados, aparatos, equipos, redes, instalaciones, soportes y sistemas de almacenamiento) o intangibles (datos, aplicaciones, sistemas operativos, bases de datos, imagen, reputación, marcas de la organización)
- **Autenticación:** Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.
- **Anonimización:** Proceso de convertir los datos en una forma en que no se pueda identificar a la persona a la cual se refieren.
- **Pseudoanonimización:** Proceso para sustituir un atributo por otro en un registro, de tal forma que a pesar de que siga existiendo la posibilidad de vincular a la persona de manera indirecta con el conjunto de datos origen, se dificulta tal acción.
- **Ciberataque:** Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.
- **Ciberespacio:** El ciberespacio es un ambiente complejo resultante de la interacción de las personas, el software y los servicios de Internet, soportados éstos por el hardware y las redes de comunicaciones (ISO 27032).
- **Ciberincidente:** Todo evento, que afecte a un recurso disponible en, o expuesto al ciberespacio, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.
- **Ciberseguridad:** Conjunto de acciones destinadas a posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, disponibles o expuestos al ciberespacio, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.
- **Confidencialidad:** Atributo de seguridad que consiste en que los datos deberían únicamente ser accedidos por el personal autorizado a tal efecto.
- **Continuidad de servicios**: Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del sistema, reduciendo el riesgo de eventos que puedan dar lugar a una interrupción o inestabilidad en las operaciones de la entidad, manteniendo niveles aceptables y propiciando la recuperación de los servicios de las tecnologías de la información (TI) en el menor tiempo posible.
- **Disponibilidad**: Atributo de seguridad de la información que implica la capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.
- **Datos Personales o datos de carácter personal:** los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, con independencia de su soporte.
- **Datos Sensibles:** Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o

intimidad, tales como los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

- **Gestión de incidentes:** Procedimientos para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante ésta.
- **Incidente:** Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información (véase también ciberincidente)
- **Infraestructura crítica:** las instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud.
- **Integridad:** Atributo de seguridad que se atribuye a un sistema de información o a los datos que alberga, dando cuenta de su correctitud y completitud de los datos, información y sistemas, de forma que sea factible garantizar que los datos permanezcan intactos, que se puedan buscar y recuperar durante el transcurso de su ciclo de vida. La falta de Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.
- **Nube privada**: La infraestructura de la nube se aprovisiona para uso exclusivo de una única organización aun cuando comprenda múltiples unidades de dicha organización. Puede ser propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.
- **Nube pública:** La infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet. Suele ser propiedad de un Prestador de Servicios que gestiona la infraestructura y el servicio o servicios que se ofrecen.
- **Protección de los activos de información:** Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos.
- **Resiliencia:** Capacidad de los sistemas, equipos o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con presteza de una interrupción, por lo general con un efecto reconocible mínimo.
- **Riesgo de Ciberseguridad:** Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos.

- **Seguridad de la información:** Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.
- **Tratamiento de datos:** Cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.
- **Vulnerabilidad o brecha informática:** Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

B. CUMPLIMIENTO DE LAS POLÍTICAS Y PROCEDIMIENTOS VIGENTES DE SEGURIDAD DE LA INFORMACIÓN DEL SECTOR SALUD

Todo oferente, funcionario y proveedor del Sector Salud debe conocer y dar cumplimiento a las Políticas y Procedimientos vigentes de Seguridad de la Información del Ministerio de Salud y Hospital de Tomé, publicadas en el link https://hospitaldetome.cl/seguridad-de-la-informacion/ y cumplir con los estándares de seguridad de la información establecidos por el Hospital de Tomé para cada proyecto y/o tarea.[1]

1.- Política General de Seguridad de la Información del Ministerio de Salud.

Toda persona que desarrolle labores para el Sector Salud, ya sea por contratación directa o indirecta, debe dar estricto cumplimiento a la Política General de Seguridad de la Información, observando sus directrices y colaborando en su aplicación e implementación desde el ámbito de sus funciones y competencias.

Los proveedores e instituciones colaboradoras de las instituciones del Sector Salud, serán responsables por los incumplimientos a las normas y políticas de seguridad de la información, con independencia del régimen contractual en base al cual desarrollen sus labores, o que desarrollen las labores a través de personal de su dependencia o subcontratación.

En caso de incumplimiento, la institución del Sector Salud se reserva el derecho de veto sobre el personal que haya cometido la infracción y podrá perseguir las responsabilidades legales, administrativas y contractuales que surjan del referido incumplimiento, sin perjuicio de solicitar al proveedor el reemplazo de los profesionales vetados por otros cuya idoneidad y competencias sean aprobados por el organismo contratante.

[1] Las políticas publicadas en este sitio web, corresponden a las relacionadas directamente con los proveedores, dependiendo de la naturaleza de los proyectos o contrato, es posible que sean aplicables otras políticas, las que pueden ser solicitadas al Establecimiento una vez tramitado el contrato respectivo.

2.- Políticas específicas.

El proveedor deberá dar cumplimiento a las políticas específicas de seguridad de la información en los términos que señale la entidad contratante. Especialmente deberá dar cumplimiento a las políticas de control de accesos, de desarrollo seguro de software, de seguridad física y lógica, y todas aquellas que sean requeridas de acuerdo con la naturaleza del proyecto en el cual participe.

C. GESTION DE SEGURIDAD.

1.- Plan de Gestión Integral de Seguridad.

Todo proveedor de instituciones del Sector Salud, debe contar con un plan de gestión integral de seguridad, que considere auditorías internas y externas con validación de resultados y metodologías de trabajo de acuerdo con los estándares vigentes y establecidos en las Políticas y Procedimientos vigentes de Seguridad de la Información del Ministerio de Salud / Hospital de Tomé y en la normativa relacionada con esta materia, la cual es recopilada y puesta a disposición del público por el Gobierno de Chile[2], a través del CSIRT[3] en conjunto con la Unidad de Coordinación de Ciberseguridad de la Subsecretaría del Interior y aplicada por las Unidades de Seguridad de la Información de los Hospitales y Servicios de Salud.

El proveedor deberá realizar acciones de monitoreo permanente de seguridad, a través de medios propios o a través de empresas de auditoría especializadas en seguridad de la información.

La entidad contratante podrá realizar auditorías de seguridad de los sistemas propios y de los proveedores. Asimismo, podrá realizar auditorías de los procesos, controles de desarrollo y soluciones de los proveedores para verificar su nivel de seguridad.

Todo proyecto de desarrollo y de mantención de software contará, como mínimo, con los siguientes mecanismos de auditoría de seguridad de la información:

- Actas de trabajo
- Certificación de conformidad de servicios
- Nombramiento de responsables
- Indicación de los periodos de revisión auditables

El proveedor deberá conservar los registros de auditoría de las actividades que se realicen, de las excepciones o incidentes de información identificadas, incluyendo la identificación de administradores y operadores. Estos registros deberán ser mantenidos durante el período de tiempo acordado con el MINSAL/HOSPITAL DE TOMÉ para ayudar en investigaciones futuras y con el objetivo de dejar antecedentes trazables relativos a los controles de accesos.

2.- Gestión de Incidentes de Seguridad.

Los proveedores deberán contar con un sistema de gestión de incidentes, que incluya al menos los siguientes componentes:

---

[2] https://www.csirt.gob.cl/decretos/

[3] Por sus siglas en inglés, Computer Security Incident Response Team. Tambien denominado Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

a.- Un modelo ágil de solución de todas aquellas vulnerabilidades que se detecten: Se entenderá por tales, las brechas o riesgos de seguridad que se identifiquen, con independencia de que hayan o no sido explotadas o de si les hayan sido alertadas por terceros o por la entidad contratante.

b.- Un protocolo de comunicaciones a la institución contratante, de las vulnerabilidades o incidentes de seguridad: El colaborador o proveedor que tome conocimiento de una vulnerabilidad que pudiere afectar a un sistema utilizado por la institución contratante deberá notificarlo a su jefatura o a la contraparte técnica designada en el acto administrativo correspondiente, dentro de las 12 horas, en que se tomó conocimiento de la vulnerabilidad, quien deberá adoptar las medidas que estén a su alcance para el resguardo de la información.

Una vez que la contraparte del contrato tome conocimiento de la vulnerabilidad deberá informarla inmediatamente al encargado de seguridad del Hospital de Tomé, quien deberá calificar su criticidad y notificar al CSIRT/ANCI del Ministerio del Interior.

El informe respectivo deberá indicar los antecedentes técnicos detallado la vulnerabilidad o riesgo detectado, impacto en los datos o sistemas, medidas de mitigación y recuperación adoptadas o en desarrollo y tiempos de resolución si es del caso, conforme con las recomendadas por la industria y expertos del área de ciberseguridad.

Asimismo, se informará si la vulnerabilidad fue explotada o no y si existe evidencia de su impacto en los servicios, o de la exposición o compromiso de sus activos de información.

Si la vulnerabilidad detectada tuviere el carácter de crítica a juicio del Ministerio, se deberá gatillar de inmediato una revisión preventiva general del sistema, que incluya un proceso de identificación y mitigación de vulnerabilidades explotadas, procurando no poner en peligro las investigaciones ni las actividades de respuesta.

c.- Plan de continuidad de negocios y recuperación de sistemas o bases de datos: el cual deberá contener el procedimiento que garantice la continuidad operacional de los sistemas de información y permita recuperar tanto los datos como las funcionalidades del sistema frente a incidentes de seguridad, emergencias y desastres. A estos efectos se incluirá un plan de gestión de respaldos, pruebas funcionales periódicas y otras medidas que se recomienden de acuerdo a los estándares generalmente aceptados.

d.- Auditorías de seguridad: Un plan proactivo de verificación de la seguridad del sistema que incluya la realización, al menos cada tres meses, de un escaneo de las plataformas, sistemas de comunicación y programas computacionales en busca de vulnerabilidades, debiendo mantener un registro de los resultados.

Adicionalmente, se deberán desarrollar las acciones preventivas y correctivas que sea necesario para mantener niveles altos de seguridad del sistema, lo que deberá quedar debidamente registrado y comunicado a la contraparte institucional a través de instrumentos que permitan realizar gestión del conocimiento.

e.- Plan de formación continua: Toda persona, colaborador o proveedor que interactúa con sistemas de información y comunicaciones que opere en las instituciones de salud o interopere con sistemas de salud utilizados en dichas instituciones deberá ser capacitado en seguridad de la información en el nivel requerido para las funciones que deberá ejercer, incluyendo aquellas capacidades y destrezas que le permitan desarrollar sus labores en las condiciones de seguridad concordantes con las políticas de seguridad generalmente aceptadas en el sector de la salud.

f.- Gestión de seguridad de recursos humanos: Todo el personal del proveedor o institución colaboradora deberá haber suscrito cláusulas de confidencialidad y de respeto a las políticas de seguridad del Ministerio de Salud y del Hospital de Tomé, las cuales deberán tener el carácter de condición esencial del respectivo contrato o convenio.

3.- Gestión de pruebas y aceptación de sistemas.

Los sistemas nuevos y actualizaciones se deberán someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo. Para ello se debe preparar y ejecutar un programa de actividades detallado, entradas de pruebas y los resultados esperados bajo una variedad de condiciones. Las pruebas pueden ser ejecutadas por personal de la institución contratante o por un tercero previamente seleccionado y/o aprobado por el Hospital de Tomé. A estos efectos se deben seguir los siguientes lineamientos:

a.- Pruebas de seguridad de los sistemas.

Con el propósito de robustecer la seguridad y mejorar los mecanismos de protección de los productos de software desarrollados para la institución contratante y de mitigar o disminuir las falencias detectadas y con ello minimizar los riesgos tecnológicos que pudiera presentar el paso producción al ser expuestos a Internet, los sistemas nuevos y actualizaciones de los sistemas existentes se deberán someter a pruebas y verificaciones de seguridad exhaustivas durante su desarrollo e implementación, documentándose el desarrollo y los resultados de cada etapa.

Antes de entrar en producción el sistema de que se trate o su actualización, el Hospital de Tomé podrá verificar los resultados de las revisiones de seguridad o realizar por sí a través de terceros, revisiones de seguridad del sistema de que se trate.

En el caso que las revisiones de seguridad detecten fallas o brechas de seguridad imputables al proveedor, ya sea en los procesos de desarrollo e implementación o en las revisiones preventivas al aplicativo, las acciones de desarrollo para el cierre de la brecha se entenderán parte de la garantía del proveedor, por lo que deberán ser realizadas por éste sin costo adicional para la institución contratante.

b.- ambientes y datos de prueba.

Las pruebas de sistemas se realizarán en ambientes de prueba, diferenciados de los ambientes productivos.

Asimismo, en aquellos casos que se requieran datos de prueba, no se deberán usar datos operacionales que contengan información personal identificable o cualquier otro tipo de información calificado como información confidencial o dato sensible.

En aquellos casos que el Hospital de Tomé 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.

c.- Pruebas de aseguramiento de calidad.

El Aseguramiento de Calidad de Software es un proceso continuo y necesario para asegurar los niveles de calidad, seguridad y estabilidad de todo software que sea desarrollado o modificado para el Hospital de Tomé. Por lo anterior, es responsabilidad del Hospital de Tomé certificar la calidad del producto recibido antes de desplegarlo en un ambiente productivo. Para lo anterior, el Hospital de Tomé a través de su Área de Tecnologías de la Información y Comunicación utilizará metodologías y técnicas estándares en estas materias, con el propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo sobre el proceso de Aseguramiento de Calidad de Software.

El Área TIC del Hospital de Tomé, será responsable de certificar la calidad del nuevo software o la nueva versión de que se trate, requisito esencial para su implementación y puesta en producción.

d.- Pruebas de aceptación de los sistemas.

Sólo podrán entrar en fase de producción los nuevos sistemas o actualización de sistemas pre existentes, que hayan superado las pruebas de aceptación definidas por el Hospital de Tomé en conjunto con el proveedor, para cada proyecto o contratación. Estas pruebas deberán incluir aquellas verificaciones de los requisitos de seguridad de la información, aseguramiento de la calidad y la adherencia a las prácticas de desarrollo del sistema seguro.

Los criterios de aceptación incluirán al menos el cumplimiento de los aspectos normativos y técnicos que permitan dar cumplimiento a los estándares de seguridad de la información, compatibilidad con los sistemas de base, interoperabilidad y funcionalidad requerida por la unidad de negocio que lo requiera en sus procesos.

e.- Gestión de cambios.

Los objetivos de este proceso son:

- Minimizar los impactos sobre la disponibilidad del servicio y los riesgos operacionales.
- Responder a los requerimientos de cambios de negocio del Hospital de Tomé, para reducir incidentes, interrupciones o la reiteración de trabajos ya realizados (rework).
- Responder a los requerimientos de Negocio y de TI para que los servicios estén debidamente alineados con las necesidades de negocio del Hospital de Tomé.
- Reducir la severidad e impacto de un posible incidente asociado a un Cambio.

Existen dos clasificaciones de cambios:

- **Proactivos:** surgen de necesidades de Negocio o técnicas para reducir costos, mejorar la calidad de los servicios, para aumentar la efectividad o eficiencia del soporte.

- **Reactivos**: nacen para resolver errores o fallas, para realizar adaptaciones a requerimientos urgentes del negocio o a cambios normativos.

El proveedor realizará las actividades y tareas descritas para la entrega del Servicio de Gestión de Cambios, siendo de su responsabilidad las siguientes tareas principales:

- Participar de manera activa en la CAB (Change Advisory Board)
- Evaluar, planificar, aportar los antecedentes técnicos relevantes al cambio y aprobar o rechazar técnicamente el cambio.
- Interactuar con el Coordinador de Cambio. (Encargada de Tecnologías Digitales del Área TIC, Hospital de Tomé)
- Recepción, registro, seguimiento y escalamiento.
- Evaluación de impacto y riesgo en conjunto con la institución contratante.
- Categorización.
- Planificación en conjunto con la institución contratante.
- Seguimiento y revisión.
- Reportes estadísticos y de gestión del proceso (métricas).
- Proveer información de/para auditoría.

D. PROPIEDAD INTELECTUAL.

Todo proveedor del sector salud deberá dar estricto cumplimiento a los derechos de propiedad intelectual y garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual. 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.

Consecuentemente, el incumplimiento de esta circunstancia no podrá acarrear ningún tipo de responsabilidad para la institución contratante, debiendo el proveedor hacerse cargo de cualquier reclamo que efectuaren terceros en esta materia.

Todos los bienes y activos de propiedad intelectual del proveedor se mantendrán bajo la titularidad, salvo acuerdo expreso y por escrito que disponga lo contrario. En aquellos casos que se prevea esta circunstancia, las licencias correspondientes serán transferidas a la institución contratante una vez concluido este contrato, quedando prohibido al proveedor su uso posterior sin el consentimiento expreso de ésta.

Cualquier información que la institución contratante ponga a disposición del proveedor, ya sea en la fase de licitación, adjudicación o ejecución del contrato, se considerará de titularidad de la institución contratante y se regirá por lo dispuesto en el acápite de confidencialidad.

E.- ALOJAMIENTO DE DATOS EN SERVIDORES Y USO DE CLOUD COMPUTING.

Los contratos que consideren servicios en la nube deberán cumplir con los lineamientos previstos en la resolución exenta Nº 619 – B de 26 de noviembre de 2018, de la Dirección de Compras y Contratación Pública, que aprueba la directiva

de contratación pública Nº 32, "*Recomendaciones para la contratación de servicios en la nube*". Sin perjuicio de lo anterior y en particular, deberán cumplir las siguientes condiciones y requisitos:

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 de la institución contratante, 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 este, 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.

Los datos sensibles deberán ser seudonimizados antes de ser ingresados en sistemas "en nube", debiendo mantenerse en los servidores locales los datos de reidentificación, en archivos debidamente protegidos.

Consecuentemente, respecto de la contratación de servicios de esta naturaleza se deberán adoptar los siguientes resguardos:

a.- Medidas organizativas.

- **i.- Prohibición de uso** de la información más allá de las necesidades asociadas al cumplimiento y finalidad del contrato.
- **ii.- Auditabilidad:** Obligación de que el proveedor mantenga auditorías externas de seguridad y que entregue las evidencias correspondientes.
- **iii.- Notificación de incidentes de seguridad de la información o ciberserguridad:** Obligación de que el proveedor comunique los quiebres de seguridad que afecten a su servicio, indicando las evidencias que permitan informar a la red de Ciberseguridad del Estado.
- **iv.- Monitoreo y Cumplimiento:** Para una correcta operación de cualquier servicio tecnológico, es fundamental contar monitoreo de los servicios prestados.
- **v.- Condiciones contractuales:** Se deberá definir claramente en los contratos, el alcance de los servicios prestados y los márgenes de crecimiento o reducción elástica del mismo
- **vi.- Acuerdos de Nivel de Servicio (SLA) y las sanciones en caso de** incumplimiento, debiendo preverse expresamente la diferenciación entre tiempo de respuesta y tiempo de resolución.
- **vii.- Mantenimiento normativo,** para el caso en que, durante la ejecución del proyecto exista una reforma normativa que impacte en el diseño, desarrollo o implementación del sistema.

b.- Resguardos de legalidad de las cláusulas:

Los contratos no deberán considerar cláusulas que estén fuera de las competencias del Hospital, a saber:

i.- Prórroga de competencia a tribunales extranjeros o tribunales arbitrales.
ii.- Renuncia a las responsabilidades del proveedor.
iii.- Renuncia a las garantías.
iv.- Aceptación de cláusulas que representen cesiones de datos sensibles o datos personales en hipótesis no autorizadas por la ley.

c.- Medidas técnicas.

i.- Certificaciones de seguridad: Los proveedores deberán contar con certificaciones acordes a la criticidad de la información que se procese o se almacene en la nube. Tratándose de información crítica y de datos sensibles, como los datos de salud, se recomienda el nivel más alto de certificación de acuerdo al estándar generalmente aceptado, de acuerdo a lo que se informe por las áreas técnicas respectivas.

ii.- Encriptación de datos: Tratándose de datos confidenciales que no sean susceptibles de seudonimización deberán aplicarse técnicas de encriptación que permitan asegurar que no serán accedidos ilegítimamente.

iii.- Seudonimización: En caso de información sensible de personas naturales (datos sensibles) se recomienda aplicar técnicas de seudonimización, manteniendo en el servidor local los códigos que permitan la reidentificación de los datos. Esto para evitar que la localización de datos en países en que existan normas de desencriptación forzosa para las autoridades no judiciales, ponga en riesgo el deber de secreto que rige de acuerdo a la ley 19.628 y artículo 19 N°4 de la Constitución Política de la República.

iv.- Elasticidad: Se debe tener especial consideración en una planificación adecuada de la capacidad, reservar capacidad con anticipación o definir en el contrato valores de crecimiento flexibles, que no obliguen a realizar un nuevo proceso de compra.

d.- Seguridad en Nube.

Los usuarios de servicios en nube necesitan garantías de que los riesgos asociados al almacenamiento de sus datos y ejecución de sus aplicaciones en estos ambientes son comprendidos y gestionados adecuadamente. Al ser responsabilidad del Prestador de Servicios la implementación de algunas de las medidas de seguridad, se deberá prestar particular atención a que los criterios de seguridad utilizados por el mismo sean reconocidos, transparentes y verificables.

Esto puede incluir auditorías o certificaciones externas que cumplan con estas características. Algunos principios de seguridad que los Prestadores de Servicios deben cumplir son:

- **Controles de acceso, identidad y autenticación robustos tanto en tránsito como en reposo:** El acceso a todas las interfaces de servicio deberán restringirse a personas autenticadas y autorizadas para prevenir cambios no autorizados en el servicio del consumidor, robo o modificación de datos o la denegación de servicio.

- **Protección de los activos de información y datos, tanto en tránsito como en reposo**: Los centros de datos deben estar construidos bajo estándares reconocidos de seguridad, para que los datos, activos y redes estén adecuadamente protegidos contra la manipulación, espionaje, pérdida, daño o incautación. Deben existir criterios claros sobre el uso de controles criptográficos

sobre los datos. Asimismo, debe existir una política clara de respaldo y retención de datos, y plazos específicos para su posterior eliminación. Es importante que la propiedad de un dato no sea modificada al ser tratada en entornos cloud.

- **Seguridad Operacional, del Personal y Proveedores:** El Prestador de Servicios debe tener procesos y procedimientos establecidos para garantizar la seguridad en la operación del servicio, incluyendo la gestión de su personal y proveedores, incluyendo la posibilidad de vetar personal o proveedores que tengan historiales de incumplimiento normativo o contractual en el ámbito de confidencialidad de la información.

- **Gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio:** El proveedor deberá promover el uso seguro de sus servicios en la nube, delimitando de forma clara las responsabilidades de cada parte. Adicionalmente. El proveedor deberá adoptar las medidas adecuadas para garantizar la separación lógica o física de sus distintos clientes, según sea necesario.

- **Proveer información de auditorías a los clientes:** El proveedor deberá proporcionar a la institución contratante, toda la información que le permita controlar el acceso a sus servicios. Especialmente deberá llevar registros de auditoría de accesos, sesiones y datos contenidos en los sistemas, sin perjuicio de la atribución de la institución realizar las comprobaciones que le permitan verificar el correcto cumplimiento de los contratos o acuerdos de servicio, ya sea a través de capacidades propias o de certificaciones y auditorías de terceros. Este acceso debe ser razonable y respetando las políticas de confidencialidad, esto podrá ser solicitado por la Unidad de Seguridad de la Información del Hospital de Tomé.

- **Marco de gobernanza:** El proveedor deberá tener un marco de gobernanza de seguridad que entregue suficiente coordinación y dirija su enfoque en la gestión del servicio y la información que éste contiene.

- **Reporte de incidentes de seguridad:** El proveedor debe transparentar a la contraparte institucional información detallada y oportuna sobre los incidentes de seguridad que afecten el servicio contratado o a la información de éste y adoptar medidas para mitigar los posibles daños resultantes.

F.- HERRAMIENTAS DE SEGURIDAD

En todo proceso de compra se exigirá que las soluciones a contratar consideren tanto herramientas que cubran la capa de telecomunicaciones, como la de aplicaciones y sistemas de base.

Las medidas de protección que se deberán considerar 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 del Hospital de Tomé 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.
- Sistemas de contraseña segura.

G.- INFRAESTRUCTURA PARA PRODUCCIÓN.

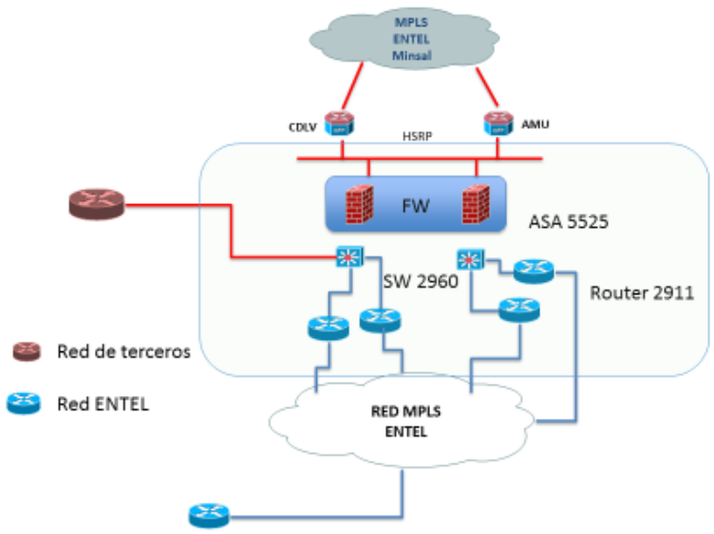
Los sistemas en producción deberán implementarse en un datacenter que cumpla con los estándares requeridos, conforme al grado de criticidad de la información, de manera tal que garantice la disponibilidad, integridad y confidencialidad de la información para los procesos que soporte.

En el caso de los sistemas de registro clínico electrónico, exámenes de laboratorio e imágenes identificadas, cuya información es de carácter reservada, la infraestructura mínima es TIER III u homologado, con un tiempo de disponibilidad de al menos 99.982% lo que implicará un máximo de 1,57 horas de tiempo de parada al año.

Tratándose de otros sistemas y aplicaciones, se determinará en cada caso los requerimientos de disponibilidad, acceso e integridad que requieran.

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 la institución contratante, como se muestra en la siguiente imagen, del diagrama de terceros:



H.- GESTIÓN DE DATOS PRODUCTIVOS.

Debe existir un control estricto sobre las modificaciones que se realizan a nivel de datos de producción, que incluya al menos:

1.- Identificación de la base de datos:

Todo sistema que incluya el tratamiento de datos personales deberá contener un documento que señale al menos los siguientes aspectos:

- Responsable del tratamiento Tipo de datos personales que serán objeto de tratamiento
- Tiempo mínimos y máximos de retención
- Procesos de negocio en que se utilizarán los datos personales
- Fuentes de datos personales que se consideran
- Destinatarios de la información.

2.- Calidad de Datos:

Siempre que el proveedor detecte que se haya producido un cambio que afecte o pueda afectar la calidad de datos productivos deberá informar a la contraparte técnica TI del Hospital de Tomé, incluyendo el detalle del cambio, su origen, ya sea errores de ingresos de datos o incidencias de sistemas. Informe técnico de las causas que dieron lugar a los errores o incidencias de que se trate, incluyendo todos los antecedentes que permitan trazar la actividad que dio lugar al cambio, día y hora en que se produjeron, usuarios que participaron, bases de datos afectadas, procesos involucrados.

En el caso en que se detecten falencias de calidad en registro de datos imputables al proveedor, ya sea en los procesos de desarrollo e implementación o en las revisiones preventivas al aplicativo, las acciones de aplicación de calidad de datos como: validación de tipo de dato, patrones de escritura, formatos, rangos, aplicación de reglas de negocio, aplicación de validadores de esquemas, etc., se entenderán parte de la garantía del proveedor, por lo que deberán ser realizadas por éste sin costo adicional para la institución contratante.

3.- Procedimiento de modificación o restablecimiento de datos:

El proveedor no podrá adoptar decisiones en relación a la modificación de datos o al restablecimiento de datos modificados. A estos efectos se deberá contar con un procedimiento de solicitudes de análisis y calificación del cambio. Será de responsabilidad de la Contraparte TI del Hospital de Tomé, calificará si procede o no hacer tales modificaciones, o bien escalará para lograr las justificaciones o autorizaciones del caso. La autorización final para proceder, solo será generada por el Hospital de Tomé. En caso de autorizarse el cambio o restablecimiento de datos, el proveedor deberá proporcionar los antecedentes que aseguren el respaldo de la intervención efectuada.

4.- Procedimiento de notificación y reporte:

El proveedor o su representante institucional reportará aquellos casos en que sospeche que los datos de producción se encuentran en riesgo, proporcionando un informe detallado de los datos afectados, y las causas técnicas o de procesos que podrían impactar en la calidad de los datos.

5.- Migración de datos a nuevos sistemas o cambios de versiones de sistemas:

En el caso que se deban implementar nuevos sistemas o nuevas versiones de sistemas se adoptarán los resguardos que permitan preservar la calidad, integridad y disponibilidad de los datos. Por lo tanto, deberán realizarse los respaldos de la información que permitan su restablecimiento, copias de seguridad y procedimientos de gestión de cambio que aseguren estos objetivos, además de garantizar la continuidad de negocios.

6.- Modelos de Datos:

Todo proveedor o institución colaboradora del sector salud, deberá poner a disposición de la contraparte técnica de la entidad contratante, los modelos de datos que permitan la adecuada gestión de los datos asociados a los procesos. Estos modelos serán parte de los entregables obligatorios de toda solución que la institución encargue a terceros, cualquiera sea el modelo contractual en base al cual se hayan desarrollado.

7.- Esquemas de metadatos:

Las bases de datos que se desarrollen deberán contar con esquemas de metadatos aprobados por el Hospital de Tomé.

8.- Calidad de tratamiento de datos:

Los datos personales tratados a través de los sistemas de salud 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 respetar, 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, ley 20.120 sobre investigación científica en personas humanas, y las demás leyes y normativa complementaria del sector salud. Los datos relativos a la salud tienen 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. En esta calidad habrá de adoptarse los siguientes resguardos:

9.- 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 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.

10.- Formatos de salida:

El proveedor deberá respetar los siguientes formatos para archivos electrónicos:

- **Informes:** si el informe contiene datos sensibles, deberá almacenarse en un archivo que soporte el cifrado seguro, de acuerdo con los estándares vigentes, 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 gestiones o tratamientos automatizados o manuales de información, deberá entregarse en formatos que soporten una estructura de datos y de cifrado seguro de acuerdo a los estándares vigentes, la que deberá mantenerse bajo el estricto control del requirente.
- **Nube:** soportar herramientas de cifrado que funcione tanto en la nube como fuera de ella, para preservar los datos y a garantizar el cumplimiento en todo tu entorno. Tratándose de datos confidenciales que no sean susceptibles de seudonimización deberán aplicarse técnicas de encriptación sobre estándar de cifrado avanzado.

11.- Medio de transporte:

Si la información se transfiere a través de un dispositivo de almacenamiento móvil, enviada a través de un correo electrónico o almacenada en nube, 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 sensible a correos que no sean los institucionales.

12.- Algoritmos o estándares de criptografía aceptados:

- AES (Advanced Encryption Standard),128 bits y superior (192 y 256).
- Algoritmo de HASH, familia SHA-2 o 3 (Secure Hash Algoritm)
- PGP (Pretty Good Privacy) o similar.
- S / MIME (Secure/Multipurpose Internet Mail Extensions).

13.- Algoritmos no permitidos:

- DES (DEA), obsoleto. Remplazado desde el 2002 por el algoritmo AES.
- MD4 y MD5 (hash) No aprobado por el NIST.
- SHA1 (hash).

Además, las comunicaciones de los componentes que transporten información de los usuarios entre sistemas deberán siempre estar protegidas mediante la utilización de protocolo de transporte seguro TLS, idealmente la versión 1.3 y los Sistemas correctamente configurados para seleccionar el cifrado más fuerte

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

Sobre algoritmos criptográficos especialmente diseñados para almacenar contraseñas, se deben utilizar bcrypt, PBKDF2 y Argon2, con el fin de reducir las vulnerabilidades de los ataques de fuerza bruta.

14.- Ejercicio de Derechos del Titular de Datos:

El Hospital de Tomé debe cumplir con los derechos de las personas en relación al tratamiento de datos personales. Todo proveedor e institución colaboradora tendrá a estos efectos el carácter de procesador o mandatario para el tratamiento de datos personales. Por lo tanto, el establecimiento podrá formularle requerimientos que le permitan responder a los derechos de acceso, rectificación, supresión o cancelación, bloqueo, o portabilidad de datos personales, los cuales deberán ser respondidos dentro de las 8 horas hábiles siguientes desde que se comunique a la contraparte técnica respecto de la solicitud y la información que le permita al proveedor responder adecuadamente.

15.- Supresión, cancelación o destrucción de datos:

Toda modificación, cancelación o destrucción de datos debe realizarse de acuerdo con los estándares generalmente aceptados, siempre por instrucciones del mandante, debiendo dejarse acta de las operaciones realizadas.

En su calidad de procesador o mandatario, el proveedor o la institución colaboradora será responsable de la ejecución del proceso, y de dejar constancia de los distintos pasos y resultados obtenidos.

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.

Durante la operación del servicio por parte del proveedor, se deba considerar que se cumplan las políticas y procedimientos de gestión de incidentes establecidos durante la contratación, incluyendo la generación de registros de incidentes y su comunicación oportuna a las partes interesadas.

16.- Mecanismos de control y trazabilidad:

Se deberán establecer mecanismos para medir al menos los siguientes aspectos:

- Cumplimiento de las medidas de seguridad acordadas.
- Cumplimiento de los niveles de servicio acordados.
- Cumplimiento de las políticas del prestador de servicios.
- Cumplimiento de las medidas asociadas a la destrucción de datos al final del contrato.

17.- Tratamiento de los datos sensibles:

Toda persona que desarrolle labores para el Hospital de Tomé, ya sea por contratación directa o indirecta deberá conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones, de acuerdo con la normativa general de salud, la ley 19.628 y los documentos relacionados.

Sin perjuicio de lo anterior, el personal que trabajan en el tratamiento de los datos personales o sensibles estarán obligados a guardar secreto sobre el mismo, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como, asimismo, sobre los demás actos y antecedentes relacionados con ley 19.628 artículo 7°, sobre Protección a la Vida Privada. Por lo tanto, los datos personales o sensibles, indistintamente del medio en que estén contenidos, deberán ser protegidos y resguardados adecuadamente por quienes tienen el deber de manipularlos, garantizando razonablemente su privacidad a través de la implementación de procedimientos y controles para su tratamiento.

18.- Privacidad por diseño:

Todo sistema o aplicación en que se traten datos personales deberá ser diseñado y desarrollado de manera tal que se dé cumplimiento a las obligaciones de reserva o secreto, de acuerdo con la naturaleza de la información. De esta manera, los sistemas que tengan por objeto el tratamiento de datos sensibles deberán cumplir las reglas siguientes:

Los sistemas y aplicaciones deberán ser desarrollados de forma tal que incluyan sistemas de verificación permanente de brechas de seguridad. Asimismo, los sistemas deberán estar diseñados para adoptar las medidas urgentes y necesarias para el resguardo de los datos personales en caso de un incidente de seguridad que pudiere afectarlos.

19.- Seguridad por defecto:

Los sistemas y aplicaciones, por defecto, guardarán la privacidad de los datos, debiendo requerirse una acción consciente y trazable para cambiar el modelo de acceso a los datos. En este ámbito, los sistemas y aplicaciones deberán incluir sistemas de resguardo de la privacidad tales como anonimización, seudonimización o encriptación de datos, de acuerdo con los requerimientos funcionales que se definan.

20- Responsabilidad demostrable:

Los sistemas y aplicaciones deberán permitir trazar las operaciones de tratamiento de datos personales que se realicen a través de los mismos de forma tal que sea posible verificar y demostrar aquellas operaciones realizadas.

21.- Segregación datos y de funciones:

El diseño de los sistemas deberá considerar perfiles diferenciados por competencias, de forma tal que sólo puedan acceder a los datos personales los profesionales que se encuentren legalmente facultados para acceder a ellos.

22.- Política de reemplazo de medios magnéticos y de almacenamiento de información:

En el caso de reemplazos de medios magnéticos de almacenamiento de información, el proveedor deberá realizar un borrado permanente de la información almacenada una vez que esta haya sido restaurada en su completitud y certificada su integridad por la contraparte del Hospital de Tomé.

I.- INTEROPERABILIDAD.

Para las aplicaciones o software que requieran la capacidad de interoperar con el medio ambiente tecnológico existentes en el Ministerio de Salud y el Hospital de Tomé, deben asegurar las condiciones que permitan contar con la validación de los equipos de tecnologías existentes, soportar las políticas de seguridad de la información, tratamiento de información sensible, movilidad del sistema con relación a lograr con otras fuentes de datos, utilizando estándares de la industria de salud tales como HL7 v2 o superior, Dicom (Digital Imaging and Communication in Medicine), Loinc (Logical Observation Identifiers Names and Codes), y, la norma técnica aprobada por decreto N° 820, de 2011, de “Estándares de Información en Salud, servicios terminológicos y maestros de pacientes”, entre otros, y de preferencia adoptar o soportar IHE (Integrating the Healthcare Enterprise). Los que deberán estar avalados por el Hospital de Tomé y su Área de Tecnologías de la Información y en base a las normativas vigentes.

Con el fin de que puedan integrarse e interoperar, resguardando la seguridad de la información según las políticas del Establecimiento.

J.- 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 el Hospital de Tomé, equivalente a la que se encuentre en operación en ese momento.

Para ello, tanto los colaboradores como los proveedores salientes deberán realizar al menos las siguientes actividades:

- Entrega de la totalidad de la información pertinente que el Hospital de Tomé o terceros determinados, tales como proveedores entrantes le requieran para garantizar la continuidad operacional.
- Entrega de todos los datos que son tratados por el sistema en un formato estructurado que permita mantener las relaciones entre tablas, datos maestros, librerías y demás aspectos esenciales para su portabilidad a un nuevo sistema; las aplicaciones funcionando y envasadas, junto con procedimientos de instalación garantizados.
- Entrega de todos los componentes necesarios que hagan posible su migración y almacenamiento histórico, como el modelo de datos, arquitectura, librerías, frameworks utilizados, etc., con el fin de garantizar la continuidad de servicio.
- La especificación de cada componente del sistema, incluyendo los diccionarios de datos.
- El Hospital 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.
- Cualquier otro elemento necesario para mantener la continuidad operacional del Hospital de manera comparable al período de vigencia del contrato correspondiente.

- Una vez que se reciban los datos por el Establecimiento, la contraparte institucional dará la orden de cancelación de los datos que se encuentren almacenados en los sistemas del proveedor, lo que deberá ejecutarse sin dilaciones indebidas por éste.

K.- NORMATIVA SOBRE SEGURIDAD DE LA INFORMACION.

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

1.- 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;
- Ley N°19.966, de 2004, que establece un régimen de garantías de salud;
- Ley N° 19.650, que perfecciona normas del área de la salud;
- Ley N° 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.
- Ley N°20.584, referida a Deberes y Derechos que tienen las Personas en relación con acciones vinculadas a su Atención de Salud;
- Ley N° 20.724, de 2014, que modifica el Código Sanitario en materia de regulación de medicamentos;
- Ley N° 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 N° 21.258, de 2020, que crea la ley nacional del cáncer, que rinde homenaje póstumo al doctor Claudio Mora.
- Ley 21.541, de 17 de marzo de 2023, que modifica la normativa que indica para autorizar a los prestadores de salud a efectuar atenciones mediante telemedicina.
- 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;
- Decreto N° 38, de 2005, del Ministerio de Salud, Reglamento Orgánico de los establecimientos de salud de menor complejidad y de los establecimientos de autogestión en red.
- Decreto N° 38, de 26 de diciembre de 2012, del Ministerio de Salud, que aprueba Reglamento sobre derechos y deberes de las personas en relación a las actividades vinculadas con su atención de salud.
- Decreto N° 38, de 2013, del Ministerio de Salud, que modifica decreto N° 466 de 1984, Reglamento de Farmacias, Droguerías, almacenes farmacéuticos, botiquines y depósitos autorizados.
- Decreto N° 6, de 16 de abril de 2021, del Ministerio de Salud, Reglamento sobre acciones de vinculadas a la atención de salud realizadas a distancia.
- Decreto N° 820, 2011, Ministerio de Salud.

2.- En materia de documentos electrónicos:

- Ley N° 19.799 de 12 de abril de 2002, de firmas y documentos electrónicos.
- Decreto N° 181, que aprueba Reglamento de la ley N° 19799 sobre documentos electrónicos. Firma electrónica y la certificación de dicha firma.
- Decreto N°83, de 2005, del Ministerio secretaría General de la Presidencia,
- 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.
- Decreto N° 4, 2021, Ministerio Secretaría General de la Presidencia, Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley nº 21.180 sobre transformación digital del estado.
- Decreto N° 24, 2019, Ministerio de Economía, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada.
- Decreto N° 1, 2015, Ministerio Secretaría General de la Presidencia, aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del estado.

3.- En materia de seguridad de la información:

- Decreto Supremo N° 83, 2005, Aprueba norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto N°273, 2022, Ministerio del Interior y Seguridad Pública, Establece obligación de reportar incidentes de ciberseguridad.
- Instructivo Presidencial N° 1, 19 de febrero de 2018, Instructivo Presidencial que entrega directrices sobre la evaluación y adopción preferente de servicios en la nube por parte de los órganos de la administración central del Estado.
- Instructivo Presidencial N° 8, 23 de octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado.

4.- En materia de protección de datos personales:

- Art. 19 Nos. 1 y 4 de la Constitución Política de la República.
- Ley N° 19.628 de protección de datos personales.
- Ley N° 20.575 sobre el principio de finalidad en el tratamiento de datos personales.
- Decreto N° 779, de 2000, que Aprueba Reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos.
- Resolución Exenta N° 489, 2022, Consejo para la Transparencia, Aprueba procedimiento para la tramitación de solicitudes de ejercicio de derechos de la ley N° 19.628, sobre protección a la vida privada

5.- En materia de delitos informáticos:

- Ley N° 21.459 sobre delitos informático.
- Ley N°20.009, sobre clonación de tarjetas de crédito.

6.- En materia de propiedad Intelectual:

- Ley N° 19.039, de Propiedad Industrial
- Ley N° 17.336, de Propiedad Intelectual

7.- Normas de aplicación general:

- Ley 21.542, Que modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o inminente
- Ley N° 21.180, de transformación digital del Estado;
- Ley N° 19.880 de bases de los procedimientos administrativos;
- Ley N° 20.285 de transparencia y acceso a la información pública;
- Ley N° 19.886 de compras públicas.
- Decreto N° 250, de 2005, del Ministerio de Hacienda, Reglamento de Compras Públicas.
- Resolución Exenta Nº 619 – B de 26 de noviembre de 2018, de la Dirección de Compras y Contratación Pública
- Decreto N° 273, del Ministerio del Interior y Seguridad Pública, de 13 de septiembre de 2022.

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