MUNICIPALIDAD
OSORNO

OSORNO,

MAT.: APRUEBASE "POLITICA RELACIÓN CON PROVEEDORES" DEL DEPARTAMENTO DE SALUD MUNICIPAL.

DECRETO N° 15.943 **/ VISTOS:**

El Departamento de Salud de la Ilustre Municipalidad de Osorno atendiendo a la relevancia que implica alcanzar niveles adecuados de integridad, confidencialidad y disponibilidad de la información, considera necesaria la creación de la **Política Relación con Proveedores** basado en las normas oficiales chilena Nch-ISO 27001/2013, con la finalidad de establecer lineamientos y criterios para dotar al personal del Departamento de Salud de conocimientos, competencias y conciencia necesarios para cumplir sus roles como guardianes de los datos sensibles.

.

CONSIDERANDO:

Que, el Departamento de Salud de la I. Municipalidad de Osorno tiene como objetivo central brindar un servicio de calidad, aumentando su eficacia y eficiencia en sus procesos de modo de servir mejor a la comunidad beneficiaria y entregar información de calidad;

El decreto N° 6398 del 17.05.2023 que establece proceso de visación documental de forma excepcional en caso de ausencia temporal en el Departamento de Salud;

Lo dispuesto en la Ley N° 19.378 que establece Estatuto de Atención Primarias de Salud Municipal;

El Decreto N° 01 del 02.01.2024 que aprueba las subrogancias para el año 2024 de la Ilustre Municipalidad de Osorno;

Lo dispuesto en la Ley N° 18.575 Orgánica Constitucional sobre Bases Generales de la Administración del Estado;

El Reglamento N° 317 de fecha 28.07.2021, sobre subrogancia del Sr. alcalde;

Que, en Decreto N° 9336 de fecha 12 de agosto 2019 se constituye "**Comité de Seguridad de la Información (CSI)**" y Decreto N° 10093 de 30 agosto 2019 que nombra "**Política General de la Información del Departamento de Salud de la Ilustre Municipalidad de Osorno"** y;

Las facultades que me confiere la Ley 18.695 Orgánica Constitucional de Municipalidades,

D E C R E T O:

APRUEBASE "POLITICA RELACION CON PROVEEDORES", que como anexo en texto íntegro se incorpora al presente Decreto.

ANOTESE, COMUNIQUESE, CUMPLASE Y ARCHIVESE

I. MUNICIPALIDAD SECRETARIA MUNICIPAL OSORNO

YAMIL UARAC ROJAS
SECRETARIO MUNICIPAL

ALCALDIA MUNICIPAL OSORNO

HARDY VÁSQUEZ GARCÉS
ALCALDE (S) MUNICIPALIDAD OSORNO

HVG/YUR/ASCHB/LVM
DISTRIBUCIÓN:

- Administrador Municipal I. Municipalidad de Osorno.
- Encargado Seguridad de la Información DESMO.

I 1870 715

DIRECCIÓN JURÍDICA I. MUNICIPALIDAD OSORNO

RELACION CON PROVEEDORES

DEPARTAMENTO DE SALUD

Elaborado por:	Aprobado por:
Luis Sergio Vidal Montiel Encargado de la Seguridad	Alejandro Schulze Barrientos Subdepartamento de Gestión en Salud
I. MUNICIPALIDAD OSORNO UNIDAD TIC DEPARTAMENTO DE SALUD	JEFE SUBDEPTO GESTION EN SALUD DEPARTAMENTO DE SALUD

Contenido

I.- INTRODUCCION

Para el Departamento de Salud, los proveedores son muy importantes para llevar a cabo su misión y el compromiso como institución gubernamental, por lo que busca fomentar una relación comercial basada en el respecto mutuo, la responsabilidad, la honestidad, con altos estándares de calidad, ética y transparencia.

En virtud de lo anterior, el Departamento de Salud se compromete a dar a conocer clara y oportunamente las normas y procedimientos de seguridad relacionados con los "activos de información" a los que tendrán acceso los proveedores, prestando asesoría en la comprensión de dichos requisitos y aplicando los controles necesarios para su cumplimiento.

II.- OBJETIVO GENERAL

La presente política tiene como objetivo establecer requisitos, lineamientos y normas generales que regulen la relación entre el Departamento de Salud y sus proveedores, a fin de garantizar la seguridad de los activos de información a los que ellos pudieran tener acceso, en el marco de la prestación de sus productos y/o servicios.

III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política es aplicable al Departamento de Salud Municipal y todas sus áreas en donde el Sistema de Gestión de Seguridad de la Información (SGSI) genera control a través de su Política General de Seguridad de la Información; es decir, sus procesos, funcionarios (planta, contrata, honorario, reemplazo o suplencia) y terceros con ocasión de un contrato, acuerdo u otra negociación.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2013

A15 Relación con Proveedores

- A15.1. Seguridad en las relaciones con proveedores
  - A15.1.1.- Política de seguridad de la información para las relaciones con los proveedores.
  - A15.1.2.- Requisitos de seguridad en contratos con terceros.
  - A15.1.3.- Cadena de suministro de tecnología de la información y de las comunicaciones.

- A15.2. Gestión de la provisión de servicios del proveedor
  - A15.2.1.- Control y revisión de la provisión de servicios del proveedor.
  - A15.2.2.- Gestión de cambios en la provisión del servicio del proveedor.

IV. DEFINICIONES

- **Activos de Información**: Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para el Departamento de Salud.
- **Cadena de suministro:** Conjunto de actividades, instalaciones y medios de distribución necesarios para llevar a cabo el proceso de entrega de un producto o servicio en su totalidad.
- **Confidencialidad:** Propiedad de la información que no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de precisión y exhaustividad.
- **Disponibilidad**: Propiedad de estar disponible y utilizable según requisito de una entidad autorizada.
- **Incidentes**: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la **confidencialidad**, la **integridad** y la **disponibilidad de la información** y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.
- **Malware:** Software malicioso diseñado para causar daños o provocar mal funcionamiento a equipos computacionales independientes o conectados a la red.
- **Negocio:** Bien o servicio prestado por una organización.
- **Riesgo:** Efecto de la incertidumbre en los objetivos.
- **Riesgo de Seguridad de la Información:** Amenaza potencial que podría afectar activos de información vinculados a los procesos de soporte institucional.
- **Seguridad de la Información:** Preservación de la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Software:** Programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador.
- **Usuario:** Toda persona interna o externa que accede y utiliza activos de información institucionales.

V.- ROLES y RESPONSABILIDADES

Jefe Departamento de Salud

1. Velar por el cumplimiento de los procesos descritos en el presente protocolo.

Encargado Seguridad de la Información

1. Gestionar los incidentes de seguridad de la información relacionados a incumplimientos de la presente política.

Subdepartamento de contabilidad y finanzas

1. Velar por el cumplimiento de la siguiente política y de la inclusión de las cláusulas de Política de Seguridad y confidencialidad en contratos con terceros a través de la Unidad de Abastecimiento.

Personal externo que presta servicio para el Departamento de Salud

1. Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación del sistema de gestión de seguridad de la información y del ordenamiento jurídico.

Proveedor

1. Dar estricto cumplimiento a las normas de seguridad descritas en la presente política, en la documentación del sistema de Gestión de Seguridad de la Información y del ordenamiento jurídico.

Inspectores Técnicos de Servicio (ITS).

1. Velar por el cumplimiento de los procesos descritos en la presente política que tengan relación con los proveedores.
2. Dar a conocer la presente política a los proveedores de servicios.

VI.- POLITICA.

1. Seguridad en las relaciones con proveedores

1.1.- Política de seguridad de la información en las relaciones con los proveedores

A. Términos Generales

1. El personal externo que desarrolle trabajos para el Departamento de Salud o sus establecimientos adheridos deberá cumplir con la política de seguridad del Departamento de Salud.
2. El jefe del Departamento de Salud, los directores de los Centros de Salud, o encargados de Unidad, cada vez que formule un requerimiento de contratación de servicio debe especificar los requisitos mínimos de seguridad cuando:
    a. Durante el desarrollo del trabajo el proveedor deba tener acceso a recursos institucionales e información de procesos relevantes del Departamento de Salud.
    b. Si corresponde, se debe definir y gestionar en el tiempo los accesos del proveedor externo a las dependencias necesarias para el servicio.
3. El personal externo que tenga acceso a información deberá considerar que dicha información, por omisión, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos para tal efecto.
4. Todos los proveedores de servicios que impliquen el acceso (tanto privilegiado como no privilegiado) a los sistemas de información del Departamento de Salud que se realicen mediante el uso de infraestructura TIC independientemente del lugar en el que se presten, deberán considerar las normativas de Seguridad de la Información del

Departamento de Salud, particularmente en cuanto a los controles y cuidados con el acceso lógico y al procedimiento de gestión de incidentes.

5. Cualquier información que el Departamento de Salud 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 los acuerdos de confidencialidad.
6. Queda prohibido para los proveedores revelar, modificar, destruir o hacer mal uso de la información, cualquiera que sea el soporte en que se encuentre contenida.
7. Los proveedores no deberán divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera de las empresas, salvo autorización expresa de éstas, la información que les fuera proporcionada para la prestación del servicio y, en general, toda información a la que tenga acceso o la que pudiera producir con ocasión del servicio que presta, durante y después de concluida la vigencia del contrato.
8. Ante cualquier cambio en la prestación del servicio por parte de los proveedores, el Departamento de Salud deberá revalorar los riesgos de seguridad de la información, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, según corresponda.
9. Los proveedores no utilizarán la información del Departamento de Salud para beneficio propio o de terceros y solo debe ser utilizada para los fines establecidos en el contrato de prestación de servicios.
10. De existir subcontrataciones, estas deben regirse por los principios de seguridad de la información establecidas para los proveedores.
11. Es responsabilidad del proveedor dar a conocer incidentes producidos o en vías de ser producidos producto de los servicios que presta, durante y después de concluida la vigencia del contrato.
12. El proveedor deberá hacer devolución de todos los activos de información que fueron entregados por motivos de los servicios contratados.
13. Está prohibido usar software privados o softwares gratuitos sin la debida autorización.
14. El proveedor debe indicar el usuario titular o representante con quien se hará el intercambio de información y los posibles accesos a los Sistemas del Departamento de Salud.

B. Propiedad intelectual

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

C. Uso apropiado de los recursos informáticos, datos, software, redes, sistemas de comunicación, etc

1. Los recursos que el Departamento de Salud pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc), están disponibles exclusivamente para cumplir las obligaciones y propósitos de la operativa para la que fueron proporcionados, y de acuerdo con su

uso natural. El Departamento se reserva el derecho de implementar mecanismo de control y auditoría que verifiquen el uso apropiado de estos recursos.

2. Cualquier archivo o equipamiento introducido en la red del Departamento de Salud, o en su efecto, cualquier equipo conectado a ella a través de soportes automatizados, internet, correos electrónicos o cualquier otro medio, debe cumplir los requisitos establecidos en las políticas de seguridad del Departamento de Salud y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de malware.

1.2.- Requisitos de Seguridad en contratos con terceros

1. Los contratos sobre bienes y servicios deben incluir entre sus condiciones contractuales cláusulas de confidencialidad respecto de la información a la que puede acceder un proveedor con ocasión de la prestación del servicio contratado o de la utilización del bien adquirido, aun cuando haya finalizado la vigencia de la respectiva contratación. La cláusula referida es indispensable si se trata de datos personales.

2. En razón de lo anterior, y en atención a la naturaleza de la contratación, en el pliego de condiciones que rige la contratación se deberá exigir que el proveedor designe a un responsable de seguridad de la información o similar, quién servirá de interlocutor para cualquier tema asociado a dicha materia y será el responsable de que se cumplan los compromisos pactados entre el Departamento de Salud y el proveedor.

3. Asimismo, entre las condiciones contractuales se deberá disponer la obligación de mantener informado al Departamento de Salud de cualquier cambio de personal asignado por el proveedor para la prestación de los servicios contratados.

4. Los contratos que tengan por objeto la instalación y mantenimiento del hardware y software deberán incluir cláusulas de propiedad intelectual estableciéndose claramente la propiedad de los materiales preexistentes que aporta cada parte para la prestación de los servicios contratados y/o bienes adquiridos.

5. Si el personal del proveedor contratado requiere acceso a los sistemas del Departamento de Salud, el pliego de condiciones que regula la contratación deberá establecer un procedimiento para ello, indicando el tipo de información, sistemas, equipos y lugares sobre los que se autoriza y/o prohíbe el acceso por parte del proveedor y de sus dependencias.

6. Para incentivar el cumplimiento de los términos contractuales, el pliego de condiciones deberá contemplar medidas de incumplimiento objetivas en consideración de la naturaleza del servicio contratado y/o bien adquirido que serán aplicables a través de los procedimientos dispuestos en el pliego para dicho efecto.

7. Finalmente, el pliego de condiciones de cada contratación deberá establecer claramente que el Departamento de Salud estará facultada para auditar, monitorear y supervisar las actividades que involucren información reservada, en especial respecto de las unidades clasificadas como "de riesgo", tales como unidad Tics, Subdepartamentos, entre otras.

1.3. Cadena de suministro de tecnología de la información y de las comunicaciones.

1. La Unidad TICs, Comité de calidad y Gestión de riesgos, unidad de Calidad y seguridad del paciente, serán las encargadas de coordinar con las otras gestiones, los lineamientos mínimos de seguridad que deben cumplir los proveedores de bienes y servicios, de acuerdo con la naturaleza y particularidad de dichos bienes y servicios.

2. Todos los lineamientos de seguridad que se establezcan para la provisión de bienes y servicios de tecnologías de información y comunicación, deberán ser parte de un acuerdo de niveles de servicio y/o el acuerdo de nivel operativo, o ser suscritos en un documento específico por las partes, previo a la provisión del bien o servicio.

3. Los responsables de las unidades mencionadas en los puntos anteriores se encargarán de efectuar un monitoreo permanente de los lineamientos de seguridad establecidos y suscritos con los diferentes proveedores de bienes y servicios.

4. Todos los lineamientos de seguridad que se establezcan para la provisión de bienes y servicios de tecnologías de información y comunicación deberán estar enmarcados en lo dispuesto en la Política de Seguridad.

2. Gestión de la provisión de servicios del proveedor

2.1.- Control y revisión de la provisión de servicios del proveedor

A) Acuerdos de niveles de servicios.

El Departamento de Salud considera relevante mantener la disponibilidad permanente de los servicios prestados por los proveedores, para lo cual se deberán establecer acuerdos de niveles de servicio que permitan garantizar razonablemente la continuidad de los servicios. Para la consecución del objetivo señalado, y en consideración de la naturaleza de los servicios contratados y/o bienes adquiridos, se deberán implementar medidas técnicas, tal como la inclusión de cláusulas de seguridad de la información en los contratos respectivos junto a otros controles de riesgos que amenacen la información.

Para el caso de los bienes y servicios relacionados con tecnología, se considerarán como criterios relevantes relacionados con el nivel del servicio la entrega continua del mismo, los tiempos de repuesta de atención para su entrega, los tiempos de resolución de problemas,

entre otros, los que serán aplicados por el área respectiva que solicita la adquisición y/o contratación del bien y/o servicio con asesoría de la unidad TICs del Departamento de Salud.

Por otra parte, el área requirente del servicio, juntamente con la unidad TICs del Departamento de Salud deberán verificar la existencia de planes de contingencia para efectos de validar el cumplimiento de los lineamientos referidos a fin de garantizar la continuidad operativa de los servicios contratados y la disponibilidad de bienes adquiridos.

B) Monitoreo de servicios tecnológicos externalizados.

Para el caso de servicios y bienes asociados a tecnologías y sistemas informáticos, será responsabilidad de la unidad TICs incorporar en su control de monitoreo la disponibilidad de los bienes y servicios tecnológicos, plataformas de infraestructuras y los sistemas de información que sean entregados por el proveedor, con la finalidad de medir los niveles del servicio y gestionar de manera oportuna cualquier incidente que pueda afectar el principio de disponibilidad.

En la medida que el área requirente necesite información detallada de un determinado bien y/o servicio, podrá solicitar un informe técnico sobre su respectiva disponibilidad dentro de un periodo determinado, incluyendo el rendimiento de los equipos en caso de que haya sido acordado.

C) Revisión de los servicios externalizados

El Departamento de salud, a través de la unidad TICs, llevara a cabo la revisión de los servicios contratados, comprobando su funcionamiento y adheridos a los términos de seguridad de la información establecidos en los contratos reduciendo incidentes y asegurando la continuidad de los procesos. De igual forma, la revisión contemplará la gestión de cambios que se hayan definidos en mutuo acuerdo entre el Departamento de Salud y el proveedor.

2.2.- Gestión de Cambios en la provisión del servicio del proveedor

Todos los proveedores de servicios que sean gestores de tecnologías / infraestructura, deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de cambios:

1. Todos los cambios en la infraestructura TIC deberán estar controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.
2. Se deberá verificar que todos los nuevos componentes introducidos en la infraestructura TIC del proveedor utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.

3. Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.
4. Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.
5. Los proveedores deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando al Departamento de salud de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

VII. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias que apliquen a la normativa de la institución, incluyendo lo establecido en las normas que competen a la Dirección de Salud en cuanto a seguridad y privacidad de la información se refiere.

VIII. REVISIONES

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política será revisada, al menos, una vez por año por parte del Comité de Seguridad de la Información, proponiendo a la Dirección del Departamento de Salud, las mejoras a implementar.

IX. MECANISMOS DE DIFUSION DE LA POLÍTICA

El presente protocolo, una vez aprobada, estará publicada en la página Web del Departamento de Salud (https://www.municipalidadosorno.cl/salud.php), en la intranet institucional (http://intranetosorno.cl) y será difundida para conocimiento y consulta de los funcionarios a través de difusión internas.

X. CONTROL DE CAMBIOS.

Versión	Fecha	Principales Modificaciones (pagina /sección)	Motivo del cambio	Elaborado por	Aprobado por
V.1.0	21.11.2024	Creación del documento	-	Encargado CSI	• Presidente CSI • CSI