

OSORNO,

7 ABR. 2024

**MAT.: APRUEBASE "POLITICA CONCIENCIACION, EDUCACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION" DEL DEPARTAMENTO DE SALUD MUNICIPAL.**

DECRETO N° 3762 / 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 Concienciación, educación y capacitación en seguridad de la información** 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;

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 de la Dirección de Salud de la Ilustre Municipalidad de Osorno" y;

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

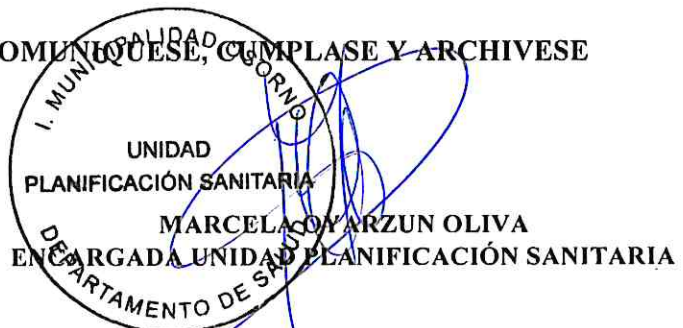
**DECRETO:**

**APRUEBASE "POLITICA CONCIENCIACION, EDUCACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION",** que como anexo en texto íntegro se incorpora al presente Decreto.

ANOTESE, COMUNIQUESE, CUMPLASE Y ARCHIVASE



ARMANDO HORMERO CARDENAS  
SECRETARIO MUNICIPAL (S)




UNIDAD  
PLANIFICACIÓN SANITARIA  
MARCELA COYARZUN OLIVA  
ENCARGADA UNIDAD PLANIFICACIÓN SANITARIA  
DEPARTAMENTO DE SALUD

**MOO/AHC/LVM**  
**DISTRIBUCIÓN:**

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


I-1748982

|   |   |   |
|---|---|---|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                                  |   |
|   | <b>POLITICA CONCIENCIACION,</b><br><b>EDUCACION Y CAPACITACION EN</b><br><b>SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | Versión      V.1.0<br>Fecha        12/04/2024 |
|   |   | Página 1 de 7                                 |

# POLÍTICA CONCIENCIACION, EDUCACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION


## DEPARTAMENTO DE SALUD

|   |  |
|---|--|
| <b>Elaborado por:</b>   | <b>Aprobado por:</b>   |
| <b>Luis Sergio Vidal Montiel</b><br>Encargado de la Seguridad de la Información     | <b>Marcela Oyarzún Oliva</b><br>Encargada Unidad Planificación Sanitaria             |
|  |  |

|   |   |  |         |       |       |            |
|---|---|--|---------|-------|-------|------------|
|  <p><b>SaludMunicipal<br/>OSORNO</b></p> | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                      |  |         |       |       |            |
|   | <b>POLITICA CONCIENCIACION,<br/>EDUCACION Y CAPACITACION EN<br/>SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | <table border="1"> <tr> <td>Versión</td> <td>V.1.0</td> </tr> <tr> <td>Fecha</td> <td>12/04/2024</td> </tr> </table> | Versión | V.1.0 | Fecha | 12/04/2024 |
|   |   | Versión  | V.1.0   |       |       |            |
| Fecha   | 12/04/2024  |  |         |       |       |            |
| Página 2 de 7   |   |  |         |       |       |            |

## Contenido

|   |   |
|---|---|
| I.- INTRODUCCION.....                             | 3 |
| II.- OBJETIVO GENERAL .....                       | 3 |
| III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO..... | 3 |
| IV. DEFINICIONES .....                            | 4 |
| V.- ROLES y RESPONSABILIDADES .....               | 4 |
| VI.- POLITICA. ....                               | 5 |
| VII. INCUMPLIMIENTO .....                         | 7 |
| VIII. REVISIONES .....                            | 7 |
| IX. MECANISMOS DE DIFUSION DE LA POLÍTICA .....   | 7 |
| X. CONTROL DE CAMBIOS. ....                       | 7 |

|   |   |  |         |       |       |            |
|---|---|--|---------|-------|-------|------------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                                  |  |         |       |       |            |
|   | <b>POLITICA CONCIENCIACION,</b><br><b>EDUCACION Y CAPACITACION EN</b><br><b>SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | <table border="1"> <tr> <td>Versión</td> <td>V.1.0</td> </tr> <tr> <td>Fecha</td> <td>12/04/2024</td> </tr> </table> | Versión | V.1.0 | Fecha | 12/04/2024 |
|   | Versión   | V.1.0  |         |       |       |            |
| Fecha   | 12/04/2024  |  |         |       |       |            |
| Página 3 de 7   |   |  |         |       |       |            |

## I.- INTRODUCCION

Por concientización, nos referimos a un proceso de aprendizaje que busca modificar actitudes y percepciones tanto organizacionales como individuales, con el fin de desarrollar en el usuario de una red una formación de la importancia de la seguridad, así como demostrar los grandes problemas que acarrea el desconocimiento o la desobediencia de las normas de seguridad.

De esta forma, la presente política abarca un enfoque integral para dotar al personal del conocimiento, competencias y conciencia necesarios para cumplir sus roles como guardianes de los datos sensibles. El objetivo principal es cultivar una fuerza laboral que no solo esté bien versada en los protocolos de seguridad establecidos, sino también sintonizada con el panorama de amenazas en constante evolución. Esto se logra a través de una serie de sesiones de capacitación estructuradas que abarcan una variedad de temas, desde principios fundamentales de seguridad hasta estrategias avanzadas para identificar y mitigar riesgos emergentes, consiguiendo su compromiso con la seguridad de la información.

## II.- OBJETIVO GENERAL


Establecer los lineamientos para que todo el personal, funcionarios, y terceros que interactúan con la información del Departamento de Salud conozcan, apropien y apliquen sus roles y responsabilidades de frente a la Seguridad y Privacidad de la Información, mediante la implementación y mantenimiento de un programa de capacitación sensibilización y comunicación dentro de la Entidad.

## III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política es aplicable al Departamento 5de 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 el siguiente control definido en la norma NCh-ISO 27001:2013

ANEXO A7.2.2: Concienciación sobre la seguridad de la información, la educación y la formación”.

|   |   |   |
|---|---|---|
| <br><b>SaludMunicipal<br/>OSORNO</b> | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION<br/>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                      |   |
|   | <b>POLITICA CONCIENCIACION,<br/>EDUCACION Y CAPACITACION EN<br/>SEGURIDAD DE LA INFORMACION<br/>PL-SGSI- 15 / CONTROL: A7.2.2</b> | Versión      V.1.0<br>Fecha        12/04/2024 |
|   |   | Página 4 de 7                                 |

#### IV. DEFINICIONES

- **Amenaza.** Acción o evento que puede ocasionar consecuencias adversas en los datos.
- **Ataque:** Es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital
- **Concienciación:** Asegurar que los usuarios comprendan y sigan ciertas prácticas para ayudar a garantizar la seguridad de la información de una organización.
- **Entrenamiento:** Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.
- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.


#### V.- ROLES y RESPONSABILIDADES

##### Jefatura o directores

1. Autorizar y fomentar en el personal a cargo la participación en las jornadas de sensibilización, capacitación y charlas, con la posterior retroalimentación de los conocimientos adquiridos para el caso que se disponga y se actualicen sobre la normativa legal aplicable.
2. Proporcionar los recursos necesarios para mantener un Programa de Concientización de Seguridad de la Información en el Departamento de Salud.
3. Fomentar en el personal a cargo el cumplimiento de las directivas, disposiciones, procedimiento y recomendaciones, así como la aplicación de las buenas prácticas relacionadas con la Seguridad de la Información que puedan darse a conocer.

##### Encargado de la Seguridad de la Informacion:

1. Definir, actualizar y ejecutar acciones de capacitación, documentación y charlas con el propósito de concientizar a los funcionarios sobre riesgos y vulnerabilidades con respecto a la seguridad de la información en el Departamento de Salud y establecimientos adheridos.
2. Brindar capacitación continua sobre Seguridad de la Información a los funcionarios.
3. Participar en la elaboración del Plan de Concientización y Sensibilización del SGSI.
4. Identificar las necesidades del personal de la institución en materia de sensibilización y capacitación en el SGSI.
5. Participar en el diseño de las estrategias y el material necesario para el desarrollo del Plan de Concientización y Sensibilización del SGSI.
6. Participar en el desarrollo y ejecución del Plan de Concientización y Sensibilización del SGSI.
7. Proponer iniciativas e identificar oportunidades de mejora para el diseño e implementación del Plan de Concientización y Sensibilización del SGSI.

|   |   |  |         |       |       |            |
|---|---|--|---------|-------|-------|------------|
| <br><b>SaludMunicipal<br/>OSORNO</b> | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                      |  |         |       |       |            |
|   | <b>POLITICA CONCIENCIACION,<br/>EDUCACION Y CAPACITACION EN<br/>SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | <table border="1"> <tr> <td>Versión</td> <td>V.1.0</td> </tr> <tr> <td>Fecha</td> <td>12/04/2024</td> </tr> </table> | Versión | V.1.0 | Fecha | 12/04/2024 |
|   | Versión   | V.1.0  |         |       |       |            |
| Fecha   | 12/04/2024  |  |         |       |       |            |
| Página 5 de 7   |   |  |         |       |       |            |

#### Unidad de Gestión de las Personas

1. Autorizar y fomentar en el personal de unidad Capacitación la incorporación de programa de capacitación en vías de la seguridad de la información.
2. Mencionar que, junto a la creación de correo electrónico, se hará llegar Manual y Cuestionario de concienciación, educación y capacitación de Seguridad de la Información la que deberán responder y hacer llegar a [seguridad.información@salud.imo.cl](mailto:seguridad.información@salud.imo.cl)
3. Brindar el apoyo ante las acciones de capacitación, documentación y charlas con el propósito de concientizar a los funcionarios sobre riesgos y vulnerabilidades en seguridad de la información brindado los tiempos necesarios para las actividades de formación.

#### Funcionarios


1. Dar cumplimiento a lo establecido en la presente Política y en las que la complementen y aplicarlo en su entorno laboral, dedicando el tiempo necesario en la formación de la seguridad de la información.
2. Aplicar en sus actividades diarias las disposiciones, directivas, procedimiento, recomendaciones y en general las buenas prácticas relacionadas con la Seguridad de la Información.

### VI.- POLITICA.

El Departamento de Salud debe establecer un programa que permita divulgar, generar, fortalecer y apropiar, de forma permanente y continua, la cultura y la conciencia en términos de Seguridad y Privacidad de la Información en todas las personas y de forma transversal a la Entidad.


#### 6.1. LINEAMIENTOS

1. Establecer un programa de concientización, capacitación y comunicación sobre la Seguridad y Privacidad de la Información que garantice que todos los funcionarios (planta, contrata, honorario, reemplazo o suplencia) y terceros con ocasión de un contrato, acuerdo u otra negociación apropien y mantengan al menos un nivel aceptable de entendimiento de Seguridad y Privacidad de la Información, así como de las obligaciones y responsabilidades de frente al uso de la información.
2. Generar cambio organizacional y del comportamiento de las personas, que permita lograr la apropiación de la Seguridad y Privacidad de la Información del Departamento de Salud.
3. Establecer planes de formación que garantice el desarrollo de las capacidades y las competencias específicas de Seguridad y Privacidad de la Información del personal del Departamento de Salud que tienen responsabilidades específicas de planeación, implementación, operación, mantenimiento y gestión dentro de los marcos establecidos por el Sistema de Gestión de Seguridad de la Información. Los requisitos particulares de

|   |   |  |         |       |       |            |
|---|---|--|---------|-------|-------|------------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                                  |  |         |       |       |            |
|   | <b>POLITICA CONCIENCIACION,</b><br><b>EDUCACION Y CAPACITACION EN</b><br><b>SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | <table border="1"> <tr> <td>Versión</td> <td>V.1.0</td> </tr> <tr> <td>Fecha</td> <td>12/04/2024</td> </tr> </table> | Versión | V.1.0 | Fecha | 12/04/2024 |
|   | Versión   | V.1.0  |         |       |       |            |
| Fecha   | 12/04/2024  |  |         |       |       |            |
| Página 6 de 7   |   |  |         |       |       |            |

formación reflejarán la experiencia previa, la formación y las cualidades profesionales pertinentes de los funcionarios, así como las necesidades laborales previstas.

4. Programar las actividades de capacitación y sensibilización sobre Seguridad y Privacidad de la Información, desde el mismo inicio de la relación o vinculación de las personas y de forma continua y permanente hasta su desvinculación o finalización de su relación con la entidad, garantizando un conocimiento razonable y consistente en esta materia.
5. Realizar y dar acceso a los diferentes tipos de materiales de capacitación y concientización sobre Seguridad y Privacidad de la Información, y adaptarlos de acuerdo con el programa y a los planes estructurados y definidos para los destinatarios o tipos de auditorio objetivo, considerando tanto el contenido técnico y de complejidad, como los formatos y estilos a ser utilizados.
6. Utilizar los diferentes medios de comunicación que el Departamento de Salud pueda tener a su alcance, con el fin de tener la cobertura a todos los funcionarios y de emplear diferentes mecanismos para los procesos de sensibilización y formación del personal. Esto incluye, pero no limita a canales internos, intranet, capacitaciones formales, capacitaciones no formarles, transferencia de conocimiento, charlas presenciales, seminarios, videoconferencias, juegos, simulaciones, ejercicios, formación en línea, esquemas presenciales y/o virtuales, soluciones tecnológicas, y cualquier tipo de recurso tecnológico, procedimental y/o humano que permita difundir, apropiar y madurar el conocimiento y el comportamiento de las personas.
7. Implementar un recurso de información en el que se pueda difundir y publicar toda la información relacionada a Seguridad y Privacidad de la Información. Este recurso debe ser la fuente definitiva y formal de la publicación de políticas, estándares, procedimientos y buenas prácticas de Seguridad y Privacidad de la Información actuales y de cumplimiento que debe seguir todo el personal.
8. Mantener informado a todo el personal de las actualizaciones y cambios relacionados con la Seguridad y Privacidad de la Información, tomando en cuenta las lecciones aprendidas resultantes de la gestión y operación del Sistema de Gestión de Seguridad de la Información.
9. Realizar de forma continua y periódica actividades de seguimiento, gestión, revisión y auditorías, con el fin de establecer una valoración y métricas específicas de los resultados de la implementación del programa y de la apropiación de la Seguridad y Privacidad de la Información en el Departamento de Salud.
10. Los planes y actividades de capacitación, sensibilización y comunicación deben realizarse de forma continua, garantizando que se incluye a todo el personal del Departamento de Salud.

|   |   |  |         |       |       |            |
|---|---|--|---------|-------|-------|------------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b><br><b>POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</b>                        |  |         |       |       |            |
|   | <b>POLITICA CONCIENCIACION,<br/> EDUCACION Y CAPACITACION EN<br/> SEGURIDAD DE LA INFORMACION</b><br><b>PL-SGSI- 15 / CONTROL: A7.2.2</b> | <table border="1"> <tr> <td>Versión</td> <td>V.1.0</td> </tr> <tr> <td>Fecha</td> <td>12/04/2024</td> </tr> </table> | Versión | V.1.0 | Fecha | 12/04/2024 |
|   | Versión   | V.1.0  |         |       |       |            |
| Fecha   | 12/04/2024  |  |         |       |       |            |
| Página 7 de 7   |   |  |         |       |       |            |

#### 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 al Departamento 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 al Departamento de Departamento de Salud, las mejoras a implementar.

#### IX. MECANISMOS DE DIFUSION DE LA POLÍTICA

La presente política, una vez aprobada, estará publicada en la página Web del Departamento de Salud (<https://www.municipalidadesosorno.cl/salud.php>; <https://www.desmo.cl/>), en la intranet institucional (<http://intranetosorno.cl>) y será difundida para conocimiento y consulta de los funcionarios y terceros que prestan servicios, 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   | 12.04.2024 | Creación del documento                       | -                 | Encargado CSI | <ul style="list-style-type: none"> <li>• Presidente CSI</li> <li>• CSI</li> </ul> |
|         |            |  |                   |               |   |