



OSORNO, 20 AGO 2025

**MAT.: APRUEBASE “POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS”
DEL DEPARTAMENTO DE SALUD MUNICIPAL.**

DECRETO N° 10.149 / 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 Seguridad relativa a los recursos humanos** 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 y activos de información.

CONSIDERANDO:

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

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

La Ley 18.883 Estatuto Administrativo para Funcionarios Municipales;

La Ley 19.880 que establece las Bases de los Procedimientos Administrativos que Rigen;

Los actos de los Órganos del Estado, en especial su art. 52, que establece que los actos administrativos no tendrán efectos retroactivos, salvo cuando produzcan efectos favorables para los interesados y no lesionen derechos de terceros; y

Las facultades que me confiere la Ley 18.695 Orgánica Constitucional de Municipalidad

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**”;

D E C R E T O:

APRUEBASE “POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS”, que como anexo en texto íntegro se incorpora al presente Decreto.

ANOTESE, COMUNIQUESE, CUMPLASE Y ARCHIVESE


YAMIL UARAC ROJAS
SECRETARIO MUNICIPAL

JBV/YUR/MMM/LVM
DISTRIBUCIÓN:

- Administrador Municipal I. Municipalidad de Osorno.
 - Encargado Seguridad de la Información DESMO.
- I 1964029



JAIME BERTIN VALENZUELA
ALCALDE MUNICIPALIDAD OSORNO



| | | | | | | |
|---|--|--|---------|-------|-------|------------|
|  SaludMunicipal OSORNO | <p style="text-align: center;">SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</p> <p style="text-align: center;">POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION</p> <p style="text-align: center;">POLITICA SEGURIDAD RELATIVA A LOS</p> <p style="text-align: center;">RECURSOS HUMANOS</p> <p style="text-align: center;">PL-SGSI- 19 / CONTROL: A7</p> | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Versión</td><td style="padding: 2px;">V.1.0</td></tr> <tr> <td style="padding: 2px;">Fecha</td><td style="padding: 2px;">18/08/2025</td></tr> </table> | Versión | V.1.0 | Fecha | 18/08/2025 |
| Versión | V.1.0 | | | | | |
| Fecha | 18/08/2025 | | | | | |
| Página 1 de 8 | | | | | | |

POLÍTICA SEGURIDAD RELATIVA A LOS

RECURSOS HUMANOS

DEPARTAMENTO DE SALUD

| Elaborado por: | Aprobado por: |
|---|--|
| Luis Sergio Vidal Montiel Encargado de la Seguridad de la Información | Muriel Muñoz Moreno Jefa Departamento de Salud |
|  |  |

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | Versión V.1.0 Fecha 18/08/2025 |
| POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | | Página 2 de 8 |

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..... | 6 |
| 6.1.- ANTES DEL EMPLEO | 6 |
| 6.2.- DURANTE EL EMPLEO | 6 |
| 6.3.- FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO | 7 |
| VII. INCUMPLIMIENTO | 8 |
| VIII. REVISIONES | 8 |
| IX. MECANISMOS DE DIFUSION DE LA POLÍTICA | 8 |
| X. CONTROL DE CAMBIOS..... | 8 |

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| | POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 |
| | | Página 3 de 8 |

I.- INTRODUCCION

En materia de seguridad de la Información los recursos humanos cumplen un papel fundamental, ya que éstos, son el mayor activo y mayor riesgo en este ámbito. Una gestión adecuada del personal, alineada con los procedimientos de seguridad es clave para minimizar aquellas vulneraciones producidas por los humanos, como prevenir negligencias y mitigar posibles amenazas internas.

Durante el ciclo que abarca el proceso de selección y contratación, es fundamental las verificaciones de antecedentes y garantizar que los funcionarios comprendan y cumplan sus responsabilidades en materia de seguridad de la información. Además, durante el empleo, la formación continua y la concienciación son esenciales para fomentar buenas prácticas y garantizar el cumplimiento de las políticas internas.

Del mismo modo, en la finalización o cambio de empleo, la unidad de Gestión de las Personas debe asegurarse de la devolución de activos de información, eliminación de accesos y la continuidad de las obligaciones legales, como la confidencialidad. Esta estrecha relación entre la gestión de las personas y la seguridad de la información refuerza la protección de los activos del Departamento de Salud y contribuye a construir una cultura sólida de seguridad.

II.- OBJETIVO GENERAL

Asegurar que todos los funcionarios y terceros con ocasión de un contrato, acuerdo u otra negociación, estén calificados y comprendan sus responsabilidades y sean aptos para las funciones que desarrolle, reduciendo el riesgo de sustracción, fraude y mal uso de las instalaciones y medios.

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 el siguiente control definido en la norma NCh-ISO 27001:2013

ANEXO A7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

- A7.1 Antes del Empleo
- A7.1.1 Investigación de antecedentes

| | | |
|---|--|----------------------|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 | Página 4 de 8 |

- | | |
|--------|---|
| A7.1.2 | Términos y condiciones del empleo |
| A7.2 | Durante el empleo |
| A7.2.1 | Responsabilidades de gestión |
| A7.2.2 | Concienciación, educación y capacitación en seguridad de la información |
| A7.2.3 | Proceso disciplinario |
| A7.3 | Finalización del empleo o cambio en el puesto de trabajo |
| A7.3.1 | Responsabilidades ante la finalización o cambio |

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. Indicar directrices para normalizar las sanciones de seguridad de la información.
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 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

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| | POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 |
| | Página 5 de 8 | |

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 capacitación gestionadas por el Departamento de Salud en seguridad de la información.
7. Participar en el desarrollo y ejecución del Plan de Concientización y Sensibilización del SGSI del Departamento de Salud.

Unidad de Gestión de las Personas

1. Autorizar y fomentar en la unidad de Capacitación la incorporación de programa de capacitación en vías de la seguridad de la información.
2. Investigar antecedentes, indicar responsabilidades y coordinar sanciones de seguridad de la información.
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 brindando los tiempos necesarios para las actividades de formación.
4. Es deber comunicar las responsabilidades que tienen los funcionarios en materia de seguridad de la información.
5. Mantener firmado Acuerdo de Confidencialidad, sus responsabilidades y deberes que conlleva. Este acuerdo debe estar firmado por todos los funcionarios.

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.
3. Estar consciente de sus responsabilidades de seguridad de la información.

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| | POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 |
| | | Página 6 de 8 |

VI.- POLITICA.

Con la finalidad de evitar fraudes, sustracciones o accesos no autorizados, es necesario el estudio y análisis de los antecedentes presentados por los postulantes.

6.1.- ANTES DEL EMPLEO

6.1.1.- Investigación de Antecedentes

1. Los antecedentes presentados deben ser verificados para garantizar la credibilidad al momento de acceder a los activos de información del Departamento de salud distribuidos a través de sus establecimientos:
 - a. Confirmar titulaciones académicas.
 - b. Comprobar las referencias aportadas en el Curriculum Vitae.
 - c. Comprobar las certificaciones profesionales.
 - d. Comprobar la identidad del candidato mediante cedula de identidad, pasaporte u otro documento.

6.1.2.- TERMINOS Y CONDICIONES DEL EMPLEO

1. Se deben respetar los términos establecidos en el ACUERDO DE CONFIDENCIALIDAD en cuanto al resguardo de los activos de información.
2. Se deben aplicar todas las sanciones dictadas en ACUERDO DE CONFIDENCIALIDAD en caso de ser vulnerados.
3. Se deben mencionar las responsabilidades de seguridad de la información que van más allá del ámbito del Departamento de salud y el horario laboral.

6.2.- DURANTE EL EMPLEO

6.2.1.- Responsabilidades de Gestión

1. Establecer y verificar que existan mecanismos de ayuda a funcionarios en puestos especialmente críticos que pueda afectar el trabajo.
2. Se debe dar hincapié que los funcionarios cumplan las normas y políticas establecidas por el Departamento de Salud en favor de las buenas prácticas.
3. Se debe firmar la recepción y conocimiento de normas, políticas, reglamento y normativa antes de iniciar su función laboral en el Departamento de Salud.
4. Se deben mantener actualizadas y correctamente distribuidas las normas, políticas, reglamentos y normativas a todos los funcionarios.
5. Se deben revisar y aprobar periódicamente los procedimientos del personal por empleados de más categoría.

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| | POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 |
| | | Página 7 de 8 |

6. Debe existir asesoría profesional ante eventuales cambios que puedan perjudicar la eficiencia en la gestión de Salud y la seguridad de los activos de información:
 - a. Problemas financieros.
 - b. Cambios de comportamiento.
 - c. Cambio de estilo de vida.
 - d. Ausencias recurrentes del puesto de trabajo.
 - e. Situaciones de depresión.
 - f. Situaciones de Stress.
7. Revisar de forma aleatoria el trabajo desarrollado por el personal.

6.2.2.- Concienciación, educación y capacitación en seguridad de la información

1. Concientizar el acceso no autorizado a través de charlas, revistas, circulares, etc.
2. Antes de acceder a los sistemas se debe concientizar el uso adecuado de la información.
3. La unidad de Gestión de las Personas debe crear las instancias necesarias de capacitación en seguridad de la información para el resguardo y uso de los activos de información.
4. La unidad de capacitación debe crear las instancias de aprendizaje de seguridad de la información.

6.2.3.- Proceso disciplinario

1. Se debe notificar de forma periódica las consecuencias de infringir las normas de seguridad como recordatorio.
2. Debe existir un proceso disciplinario para tratar las violaciones de las políticas y procedimientos de seguridad.
3. Todos los funcionarios deben conocer las sanciones que se incurran en caso de vulneraciones de los activos de información del Departamento de Salud.

6.3.- FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO

6.3.1.- Responsabilidades ante la finalización o cambio

1. Se deben definir las responsabilidades de todas las partes implicadas en la finalización o cambio en los contratos y puestos de trabajos.
2. Todas las responsabilidades deben ser incluidas en los contratos laborales de los funcionarios y terceros con ocasión de un contrato, acuerdo u otra negociación.

| | | |
|---|--|---|
|  SaludMunicipal OSORNO | SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION | |
| | POLITICA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS PL-SGSI- 19 / CONTROL: A7 | Versión V.1.0 Fecha 18/08/2025 |
| | | Página 8 de 8 |

3. Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos del Departamento de Salud deben realizarse de acuerdo a los procedimientos vigentes para la solicitud y atención de cuentas de acceso.

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 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.municipalidadesorno.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 | 18.08.2025 | Creación del documento | - | Encargado CSI | <ul style="list-style-type: none"> • Presidente CSI • CSI |
| | | | | | |