DIRECCIÓN DE SALUD MUNICIPAL OSORNO

OSORNO, 16 AGO. 2021

MAT.: APRUEBASE "POLITICA CONTROL DE ACCESO" DE LA DIRECCION DE SALUD MUNICIPAL.

DECRETO N° 5961 **/ VISTOS:**

La Dirección 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 de Control de Acceso** basado en las normas oficiales chilena Nch-ISO 27001/2013, con la finalidad de establecer lineamientos en los controles de acceso a los activos de información, evitando incidencias con el uso adecuado de acceso a instalaciones, plataformas y sistemas de cómputo fortaleciendo los principios de Confidencialidad, Integridad y Disponibilidad de la información.

CONSIDERANDO:

Que, la Dirección 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;

Que, la urgencia de aumentar los niveles de protección de la información que, como el resto de los activos, tiene valor para la institución;

Que, en Decreto 9336 de fecha 12 de agosto 2019 se constituye "**Comité de Seguridad de la Información (CSI)**" y Decreto 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,

El Decreto Municipal N° 6675 del 08/04/2019, que delega al Director de Salud Municipal Osorno, atribuciones, funciones y competencias concernientes a la Administración del personal del Departamento de Salud Municipal y de los Establecimientos de Salud Municipal de la Comuna de Osorno;

D E C R E T O:

APRUEBASE "POLITICA DE CONTROL DE ACCESO". SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN, que como anexo en texto íntegro se incorpora al presente Decreto.

ANOTESE, COMUNIQUESE, CUMPLASE Y ARCHIVESE

I. MUNICIPALIDAD SECRETARIA MUNICIPAL

YAMIL URAC ROJAS
SECRETARIO MUNICIPAL

DIRECCIÓN DE SALUD DIRECTOR DE SALUD I. MUNICIPALIDAD OSORNO

JAIME ARANCIBIA TORRES
DIRECTOR DIRECCIÓN DE SALUD

JAT/YUR/LVM

DISTRIBUCIÓN:

- Administradora Municipal I. Municipalidad de Osorno.
- Asesoría Jurídica I. Municipalidad de Osorno
- Unidad de Control de Gestión I. Municipalidad de Osorno.
- Departamento de Informática I. Municipalidad de Osorno.
- Encargado de Seguridad de la Información, Dirección de Salud Municipal.

POLÍTICA DE CONTROL DE ACCESO

DIRECCION DE SALUD

Elaborado por:	Aprobado por:
Luis Sergio Vidal Montiel Encargado de la Seguridad	Jaime Arancibia Torre Director Salud Municipal
	DIRECCION DE SALUD DIRECTOR DE SALUD MUNICIPALIDAD DE OSORNO

TABLA DE CONTENIDO

I.- INTRODUCCION

Limitar el acceso a la información y a las instalaciones de procesamiento de información será la gestión continua de la Política General de Seguridad de la Información de la Dirección de Salud Municipal. El acceso estará siempre prohibido para quienes no cuentan con credenciales, privilegios y/o autorizaciones adecuadas para el uso de la información, de esta forma, la **Política de Control de Acceso** determina las reglas de acceso a sistemas, servicios e instalaciones.

Los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y registro, de acuerdo con la política de control de acceso.

II.- OBJETIVO GENERAL

Definir reglas de acceso para diversos sistemas, equipos, instalaciones e información de la Dirección de Salud Municipal en base a los requerimientos del negocio y de seguridad de la información.

III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política es aplicable a la Dirección 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 A9 : CONTROL DE ACCESO.
ANEXO A9.1 : Requisitos de negocio para el control de acceso.
ANEXO A9.1.1 : Política de Control de Acceso.

IV. DEFINICIONES

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Dirección de Salud Municipal en un momento dado.

Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la entidad.

Custodio: Es cualquier persona que mantiene bajo su responsabilidad, **información** de la cual no es el Propietario.

ITO: Inspector Técnico de Obra.

V. DIRECTRICES DE SEGURIDAD

- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.
- El control de acceso a sistemas en arriendo o comodatos será a través del Inspector Técnico de Obra asignado, previa autorización del responsable de la unidad solicitante.
- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones, los accesos a las aplicaciones y sistemas de la Dirección de Salud Municipal y la desvinculación a sistemas externos tan pronto el personal termine su vinculación.
- Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el encargado directo del proceso.
- El Director, Encargado de Unidad, Jefe Directo, Referentes Técnicos o en su defecto el Encargado de Seguridad de la Información son los únicos autorizados para solicitar o eliminar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario.
- Los funcionarios no deberán compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.
- Cada funcionario de la Dirección de Salud Municipal y sus Establecimientos dependientes deberán hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.

VI.- ROLES y RESPONSABILIDADES

Encargado de la Seguridad de la Información:

1. Velar por el cumplimiento de los procesos descritos en la presente política.
2. Informar a la Dirección de Salud las vulnerabilidades realizadas por accesos no autorizados.
3. Tiene la facultad de solicitar o eliminar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información de no ser gestionados por los directores, encargados o jefes directos de las unidades de la Dirección de Salud Municipal.

Funcionarios

1. El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.
2. Informar al Encargado de Seguridad de la información las vulnerabilidades por accesos no autorizados.

Unidad Tic

1. Se deberán realizar revisiones periódicas en los diferentes sistemas de la Dirección de Salud Municipal para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.
2. Monitorear los ingresos a sala(s) de servidores permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.
3. Brindar los medios y orientación para el acceso remoto autorizado.

Gestión de las Personas

1. Deberá informar a encargado TIC o Encargado Seguridad de la Información la desvinculación del o los funcionarios para proceder al bloqueo de cuentas y solicitud de dispositivos.

Director(es), Jefes, Encargados de Unidad, Referente Técnico

1. Son los únicos autorizados para solicitar o eliminar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario.

VII.- POLITICA.

Todos los funcionarios de la Dirección de Salud, incluso terceros, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la institución. La asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos.

A.- CONTROL DE ACCESO A LAS INSTALACIONES

1. Previa autorización e identificación del personal se podrá dar acceso a las instalaciones de la Dirección de Salud Municipal y sus Establecimientos dependientes, concediendo los privilegios necesarios para el acceso físico.

2. Debe existir una persona (rol o cargo) responsable de autorizar el acceso a las instalaciones de acceso restringido, a su vez, estas zonas deben estar debidamente señalizadas.

3. Se prohíbe el acceso a oficinas sin la debida autorización de alguno de los funcionarios que la ocupan.

4. El acceso deberá efectuarse dentro de la jornada de trabajo, cualquier excepción deberá ser autorizada y vigilada por el responsable directo del Establecimiento o unidad.

5. Cada visitante a las instalaciones debe tener una credencial que lo identifique como tal proporcionada por el Establecimiento garantizando su autenticidad y seguridad a los accesos.

B.- CONTROL DE ACCESO A ARCHIVADORES Y DOCUMENTOS

1. El acceso a los documentos archivados, está restringido excepto que haya sido autorizado por el encargado de la unidad responsable de la documentación.

2. Cualquier extracción de documentos en todas sus formas: fotocopia, fotos, escaneadas que no sea para el uso de la unidad o establecimiento debe estar debidamente autorizadas por el custodio directo dejando un registro de los documentos intervenidos.

3. Los terceros, sean profesionales, alumnos en práctica, docentes, etc., que por convenios y disposición de la Dirección de Salud Municipal deben tener acceso a los Archivadores o Documentos deberán estar debidamente identificados al momento de ejercer sus labores.

C.- CONTROL DE ACCESO A SISTEMAS

1.- Perfiles de Usuario

1.1.- Todo sistema debe tener debidamente documentado e identificado los perfiles de usuarios y las funciones respectivas del perfil en el sistema.

1.2.- No se podrá acceder a ningún nivel de información (Sistemas, Archivadores, Redes, Casillas, Instalaciones, etc.) con perfiles, privilegios de otros usuarios.

1.4.- El Director, Encargado de Unidad, Jefe Directo, o Referente Técnico son los únicos autorizados para solicitar el acceso o eliminación a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario.

2.- Gestión de Privilegios

2.1.- Debe existir una persona (rol o cargo) responsable de autorizar la concesión o eliminación de privilegios o derechos de acceso para los sistemas o servicios.

2.2.- El responsable de asignar privilegios debe tener en cuenta los requerimientos de negocio y de seguridad para el acceso, como también la clasificación de la información establecida en nuestra Política de Clasificación de la Información a la que se accede con esos derechos de acceso. Deberá existir un registro de aquellos privilegios entregados a funcionarios o terceras partes.

3.- Cambios de estado

3.1.- Cuando se produce un cambio o finalización del contrato, la Unidad de Gestión de las Personas debe informar inmediatamente al Encargado Unidad TIC y Encargado Seguridad de la Información, para realizar los cambios respectivos en los sistemas e informar a quienes corresponda de la desvinculación de la Dirección de Salud Municipal y exigir, cuanto antes, la modificación o eliminación de los derechos de acceso.

4.- Acceso Remoto

4.1.- Aquellos funcionarios que requieran acceso remoto a los sistemas y servidores de la Dirección de Salud Municipal que sólo se encuentran disponibles en la red Interna, deberán solicitarlo al Encargado Unidad TIC justificando el motivo de la solicitud. El Encargado de Unidad TIC aprobará, rechazará o solicitará más antecedentes respecto de la solicitud. El acceso puede ser VPN, ANYDESK u otra aplicación, que permite acceder a máquinas remotas a través de una red), en el caso de los funcionarios que ejercen funciones relacionadas con Tecnologías de Información o aquellos que por disposición de la Dirección de Salud Municipal ejercen funciones en modalidad Teletrabajo.

4.2.- En caso de aprobar la solicitud, será responsabilidad del Encargado TIC la generación de las credenciales de acceso, las cuales deberán ser entregadas al funcionario.

4.3.- En caso de que terceros (proveedores, consultores, etc.), por motivos de desarrollo, mantención, soporte o auditoría, tanto de sistemas, servicios, servidores o infraestructura de red, requieran acceso remoto a servidores de la Dirección de Salud Municipal, será el Encargado de Unidad TIC quien podrá aprobar, rechazar o solicitar más antecedentes respecto de la solicitud.

5.- Acceso a Cámaras de Vigilancia

5.1.- Un CCTV o **circuito cerrado de televisión** es una instalación de equipos conectados que generan un circuito de imágenes que solo puede ser visto por un grupo determinado de personas. Los objetivos principales de la función de los sistemas de seguridad son:

- Reducir perdidas.
- Reducir incidentes de inseguridad.
- Mejoramiento de la efectividad en los trabajadores de la organización.

5.2.- El acceso a las imágenes y videos generados por el circuito CCTV está restringida a la autorización directa del Director del establecimiento.

5.3.- Está prohibido entregar imágenes o videos que el circuito CCTV de cámaras de vigilancia haya captado que pueda beneficiar a terceros de forma directa o indirecta, tales como: accidente vehicular, atropellos, robo, etc., de ser así, la solicitud de acceso debe provenir de alguna institución de orden público, judicial o investigativo estando sujeto al criterios y disponibilidad de los accesos de la Dirección de Salud Municipal.

VIII. 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.

IX. 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.

X. MECANISMOS DE DIFUSION DE LA POLÍTICA

La presente política, 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), la página oficial de la Dirección de Salud Municipal (www.desmo.cl) y será difundida para conocimiento y consulta de los funcionarios y terceros que prestan servicios, a través de difusión internas.

XI. CONTROL DE CAMBIOS.

Versión	Fecha	Principales Modificaciones (pagina /sección)	Motivo del cambio	Elaborado por	Aprobado por
V.1.0	11.08.2021	Creación del documento	-	Encargado CSI	• Presidente CSI • ESI