OSORNO, 26 ABR. 2021

MAT.: **APRUEBASE "POLITICA DE DESARROLLO SEGURO" DE LA DIRECCION DE SALUD MUNICIPAL.**

DECRETO N° 2783 **/ 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 Desarrollo Seguro** basado en las normas oficiales chilena Nch-ISO 27001/2013, con la finalidad de establecer lineamientos en la producción de programas computacionales internos y externos con una metodología que resguarde la información durante todo el ciclo de desarrollo seguro de aplicaciones, disminuyendo así los niveles de incidencias en las etapas del desarrollo.

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 DESARROLLO SEGURO". 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 OSORNO

YAMIL UARAC ROJAS
SECRETARIO MUNICIPAL

MUNICIPALIDAD DIRECTOR DE SALUD 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.

POLITICA DE DESARROLLO SEGURO

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

DIRECCION DE SALUD
ILUSTRE MUNICIPALIDAD OSORNO

Elaborado por:	Revisado por:	Aprobado por:
Sr. Luis Sergio Vidal Montiel Encargado de la Seguridad Dirección de Salud I. Municipalidad Osorno	Sr. Sigifredo Fajardo Alterhoff Encargado de Calidad Dirección de Salud I. Municipalidad Osorno	Sr. Jaime Arancibia Torres Director Dirección de Salud I. Municipalidad Osorno

INDICE

1. INTRODUCCION 3
2. OBJETIVO 3
3. ALCANCE 3
4. RESPONSABLES 3
5. DEFINICIONES 5
6. CONSIDERACIONES GENERALES 6
7. POLITICA 6
8. INCUMPLIMIENTO 11
9. REVISIONES 11
10. MECANISMOS DE DIFUSION DE LA POLÍTICA 11
11. TABLA DE MODIFICACIONES 11

1. INTRODUCCION

A lo largo de la historia de la evolución de las tecnologías de información, la seguridad casi siempre ha sido un aspecto rezagado. Es habitual que primero pensemos en la funcionalidad y luego, cuando alguna tecnología ya fue desplegada y tengamos evidencias de que hay vulnerabilidades, nos preocupemos de la seguridad. En el desarrollo de aplicaciones también ocurre: algo sucede en el desarrollo del software o aplicaciones, que termina finalmente en una vulnerabilidad.
Por esta razón, la Dirección de Salud Municipal Osorno desea implementar el desarrollo seguro en su modelo conceptual para el análisis de seguridad en cada una de las etapas de sus proyectos de programas computacionales.

2. OBJETIVO

Establecer lineamientos para las condiciones de seguridad que deben poseer los productos de software desarrollados de forma interna como por proveedores externos en la Dirección de Salud Municipal para las buenas prácticas en todas las etapas del Desarrollo.

3. ALCANCE

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), 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 A14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
    - ANEXO A14.2: Seguridad en el Desarrollo y en los procesos de soporte.
        - ANEXO A14.2.1: Política de desarrollo seguro

4. RESPONSABLES

Director Dirección de Salud Municipal

- Aprobar y permitir la difusión de la presente política.
- Proveer los recursos para la implementación y desarrollo seguro.

Unidad de Gestion de Personas

- Es responsable de insertar la cláusula de derechos de propiedad intelectual estipulados en la Ley 17.336 tratándose del desarrollo de programas computacionales con funcionarios contratados para tal efecto.

Encargado de la Seguridad de la Información

- Es responsable de la elaboración de la presente política, de su actualización y velar por el cumplimiento de sus disposiciones.

- Utilizar todos los medios a su alcance para la difusión de la política.
- Sugerir modificaciones para actualizar la política.
- Revisar, aprobar o rechazar procesos y controles tendientes a mitigar, eliminar o transferir los riesgos relacionados con el desarrollo de sistemas de información.
- Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para el desarrollo de sistemas de información.

Unidad TIC

- Es responsable de proporcionar la infraestructura TI adecuada para la ejecución del software destinados a la gestión de la Dirección de Salud Municipal.
- Responsable de la disponibilidad y continuidad de las plataformas destinadas al desarrollo seguro en sus 3 ambientes: Desarrollo, Prueba y Producción.

Unidad de Abastecimiento

- Es responsable de insertar la cláusula de derechos de propiedad intelectual estipulados en la Ley 17.336 tratándose del desarrollo de programas computacionales con terceros.

Encargado Desarrollo Sistemas

- Tiene la responsabilidad de definir normas, procedimientos y controles que permitan asegurar que, en los procesos de desarrollo de programas computacionales, se apliquen los controles necesarios para la seguridad de la información de estos.
- Es responsable de Implementar una metodología de desarrollo seguro evidenciando los procesos.
- Debe mantener un portafolio de Sistemas de Información Desarrollados y proponer a la Dirección de Salud Municipal una lista acotada de sistemas clasificados como críticos.
- Debe mantener la documentación del ciclo de desarrollo seguro como un respaldo evidente de propiedad intelectual de la Dirección de Salud Municipal.
- Se deben recolectar los requerimientos de los usuarios para realizar el documento inicial (requerimientos). En esta etapa es dispensable la participación de los usuarios directamente involucrados.
- Velar por la identificación de los requisitos de seguridad y consensuarlos previamente a su desarrollo y/o implantación.
- Velar que, en el estudio de factibilidad (Técnica, Operativa, Económica) se consideren aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.

Personal externo

- Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política.
- Realizar pruebas de seguridad técnica del aplicativo desarrollado.

5. DEFINICIONES

- **Desarrollador**: Programador o una compañía comercial que se dedica a uno o más aspectos del proceso de desarrollo de software. Se trata de un ámbito más amplio de la programación algorítmica
- **Desarrollo Seguro:** Requisito para generar un servicio, arquitectura, software y sistema seguro, desde la perspectiva del resguardo de la información.
- **Certificados SSL**: (Secure Sockets Layer). Es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo Secure Sockets Layer sí saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.
- **Código Fuente**. El código fuente de un programa está escrito en un lenguaje de programación determinado, sin embargo, este tipo de "lenguaje no puede ser ejecutado directamente por el computador, sino que debe ser traducido a otro lenguaje que el ordenador pueda ejecutar más fácilmente. Para esta traducción se emplean los llamados compiladores, ensambladores o intérpretes".
- **Ciclo de vida del desarrollo de Software**: Es una secuencia estructurada y bien definida de las etapas en Ingeniería de software para desarrollar el producto software deseado.
- **Hardware:** Conjunto de componentes físicos de un sistema informático
- **OWASP**: Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.
- **Programa Computacional:** Se define como programa computacional: "un conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener determinado proceso o resultado, contenidas en un diskette, cassette, cinta magnética u otro soporte material". Además, se establece que se entenderá por "conjunto de instrucciones" que constituye el programa computacional un grupo de instrucciones ya sea bajo la forma de "Programa Fuente" o de "Programa Objeto".
- **Software:** Programas y documentación de apoyo que permiten y facilitan el uso de la computadora además de automatizar procesos. El software controla el funcionamiento del hardware y el procesamiento de datos.
- **Sistema de información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
- **URL (localizador de recursos uniforme):** Es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que designa recursos en una red.

6. CONSIDERACIONES GENERALES

En cuanto al desarrollo de programas computacionales por terceros, los contratos deben contener cláusulas que resguarden los niveles de confidencialidad de la información en o los proyectos respectivos.

Los programas computacionales creados estando en la institución son propiedad intelectual de la Dirección de Salud Municipal, protegidos por la Ley 17.336 "Ley de propiedad intelectual"

- Art. N° 3/16: "Los programas computacionales, cualquiera sea el modo o forma de expresión, como programa fuente o programa objeto, e incluso la documentación preparatoria, su descripción técnica y manuales de uso". Ley 17.336 "Ley de propiedad intelectual".
- Art. N° 8: "Tratándose de programas computacionales, serán titulares del derecho de autor respectivo las personas naturales o jurídicas cuyos dependientes, en el desempeño de sus funciones laborales, los hubiesen producido, salvo estipulación escritas en contratos. Respecto de los programas computacionales producidos por encargo de un tercero, se reputarán cedidos a éste los derechos de su autor, salvo estipulaciones escrita en contrato.

7. POLITICA

A. DESARROLLO INTERNO

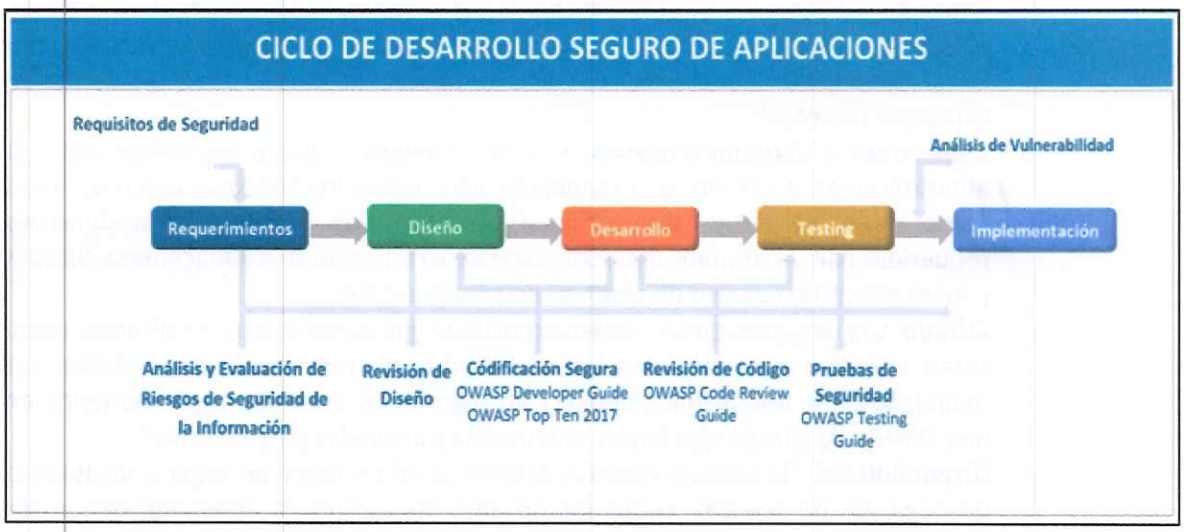
Para el desarrollo de software interno, la Dirección de Salud Municipal a través de su unidad de desarrollo deberá seguir los siguientes lineamientos:

1. **Separación de Ambientes de Desarrollo, Prueba y Producción.**

- Se deben tener tres ambientes delimitados, uno de desarrollo, otro de pruebas y otro de producción con el propósito de reducir los riesgos del acceso o cambios no autorizados al entorno operacional, asegurando un entorno de desarrollo seguro. Los ambientes a gestionar son:
    - Ambiente de Producción: Es la plataforma tecnológica dispuesta para alojar las aplicaciones que usan los usuarios para realizar sus funciones.
    - Ambiente de Desarrollo: Es donde se instalan los sistemas informáticos para el desarrollo de aplicaciones o sistemas de información. También es la infraestructura para instalar software de propietario que debe ser personalizado para posterior uso en la Dirección de Salud Municipal.
    - Ambiente de Pruebas: Es un ambiente que están disponible los Sistemas de Información recientemente desarrollado o Personalizado para que sea medido por los usuarios finales desde el punto de vista funcional y por la Unidad TIC para pruebas de estrés, rendimiento y seguridad. Las pruebas son la última etapa de un software en desarrollo o personalización antes de pasar a la etapa de implementación y posterior puesta en producción.

2. **Requerimientos y controles de seguridad.**

- El desarrollo seguro debe evidenciar la seguridad de las aplicaciones en el uso de principios y/o buenas prácticas de seguridad durante el ciclo de desarrollo del software (Requerimientos, Diseño, Desarrollo, Pruebas (Testing) e Implementación).



- Establecer requerimientos y controles de seguridad para el ciclo de vida de desarrollo de software, los cuales deben ser medibles en sus fases de Requerimiento y Control:

  - **Validación de entradas y codificación**: Los requerimientos deben especificar las reglas para validación y codificación de cada dato de entrada a la aplicación, ya sea de usuarios, sistemas de archivos, bases de datos o sistemas externos. La regla predeterminada debe ser que todas las entradas sean validadas a menos que cumplan con una especificación detallada de que está permitido. "Además, los requerimientos deben especificar las acciones a tomar cuando se reciben entradas no válidas. Específicamente, la aplicación no debe ser susceptible a inyecciones, desbordamientos, manipulación y otros ataques con entradas de usuario corruptas.
  - **Autentificación y manejo de sesiones**: Los requerimientos deben especificar como se protegerán las credenciales para autentificación y los identificadores de sesión a través del ciclo de desarrollo de software. "Los requerimientos para todas las funciones relacionadas deben ser agregados incluyendo recuperar contraseñas, cambio de contraseñas, recordar contraseñas, desconexión y conexión múltiple".
  - **Control de acceso**: Los requerimientos deben incluir una descripción detallada de todos los roles (grupos, privilegios, autorizaciones) usadas en la aplicación. Los requerimientos deben indicar todos los activos y funciones que provee la aplicación. "Los requerimientos deben especificar detallada y exactamente los derechos de acceso para cualquier activo y función de cada rol. Se sugiere utilizar un formato de matriz de control de acceso para documentar estas reglas".
  - **Manejo de errores**: "Los requerimientos deben detallar como se van a manejar los errores que ocurran dentro del procesamiento. Algunas aplicaciones deberían

hacer lo mejor posible en caso de un error, mientras que otras deberían terminar su procesamiento inmediatamente".

- **Historial**: Los requerimientos deben especificar que eventos son relevantes para la seguridad y necesitan ser registrados, como ataques detectados, intentos de conexión fallidos e intentos de exceder la autorización. "Los requerimientos deben especificar también que información registrar con cada evento, incluyendo hora y fecha, descripción del evento, detalles de aplicación, y otra información útil en esfuerzos forenses".
- **Conexiones a sistemas externos**: Los requerimientos deben especificar como la autentificación y cifrado será manejado para todos los sistemas externos, tales como bases de datos, directorios y servicios Web. "Todas las credenciales requeridas para la comunicación con sistemas externos deben almacenarse cifradas y fuera del código dentro de archivos de configuración".
- **Cifrado**: Los requerimientos "deben especificar qué datos deben ser cifrados, como serán cifrados y como todos los certificados y otras credenciales deben ser manejados. Las aplicaciones deben usar algoritmos estándar implementados en una librería de cifrado que hayan sido usadas y probadas ampliamente".
- **Disponibilidad**: "Los requerimientos deben especificar como protegerse de ataques de negación de servicio. Todos los posibles ataques en la aplicación deben ser considerados, incluyendo bloqueos de autentificación, agotamiento de conexiones y otros ataques de agotamiento de recursos".
- **Configuración segura**: Los requerimientos deben especificar que los valores predeterminados para todas las configuraciones relacionadas a seguridad deben ser seguras. "Para propósitos de auditoría, el software debería ser capaz de producir un reporte sencillo de leer que muestre los detalles de todas las configuraciones relacionadas con seguridad".

- Se debe estandarizar los criterios de seguridad y calidad a ser considerados durante cada fase del ciclo de desarrollo de los sistemas dejando una evidencia técnica en guías o formularios.
- Debe existir control y restricción al acceso del código fuente.
- Se debe considerar aspectos de riesgo y elementos como los siguientes:
  - La sensibilidad de los datos que el sistema ingresa, procesa, almacena y transmite.
  - El grado de externalización y confiabilidad asociado al proyecto de desarrollo.
  - Control de acceso al entorno de desarrollo.
  - Control sobre el movimiento de datos desde y hacia el entorno.
- En la identificación de controles de seguridad, deben participar las áreas de negocio que serán usuarios del sistema en desarrollo y deben quedar declarados en los requerimientos.

3. Seguridad en el desarrollo seguro COVID-19.

- Los programas computacionales (aplicaciones, sistemas, apps o herramientas informáticas) que tengan como misión el registro de contagios locales o procesos de trazabilidad COVID-19, deberán presentar atención en la información confidencial o

sensible amparada por la ley de protección a datos de carácter personal o clínico evidenciando los niveles de seguridad y control seguro en la entrada, proceso y salida de datos en todos sus formatos.

- Se deberá indicar las iniciales de responsabilidad en todos los informes extraídos de la trazabilidad COVID-19.
- Deberán existir mensajería de alerta al acceder a información considera Confidencial y Sensible con el objetivo de evitar su divulgación.
- Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.
- Serán los profesionales calificados quienes revisarán las aplicaciones móviles, asegurando el cumplimiento de los protocolos de calidad y las políticas de seguridad de la información de la Dirección de Salud Municipal antes de permitir que los funcionarios las usen en los dispositivos móviles que se conectan a su red interna.

4. Seguridad de la información en el desarrollo seguro

- Cuando un sistema tenga previsto el envío de datos (interoperabilidad) que contengan información clasificada como privado(a) o reservado(a), se debe implementar mecanismos de cifrado de los datos.
- Se debe verificar el cumplimiento de los requerimientos asociados a la seguridad de la información, al cumplirse los hitos relevantes del ciclo de desarrollo.
- Considerar guía técnica para Desarrollo de Software para el Estado (versión diciembre 2018), que entrega los lineamientos generales y recomendaciones específicas que debe seguir todo equipo que desarrolle de software al interior de la Administración del Estado y los grupos de desarrollo de los proveedores, contribuyendo a la construcción de sistemas de alta calidad en todas las instituciones.
- Considerar guía metodológica de OWASP Top 10 para la seguridad en el Desarrollo Seguro.
- La información involucrada en los servicios de la Dirección de Salud Municipal y que pasa por redes públicas se debe proteger contra toda actividad posible que pueda ser realizada por personal no autorizado y con propósitos dañinos para la operatividad de la Dirección.
- El encargado de Calidad o en su defecto el Encargado de Seguridad de la Información también pueden optar por revisar las aplicaciones móviles y asegurarse de que cumplan los protocolos de calidad y las políticas de seguridad de la Dirección de Salud Municipal antes de permitir que los empleados las usen en los dispositivos móviles que se conectan a su red interna.
- Se debe contar con repositorios para código que permitan controlar el acceso al mismo, junto con un historial de los cambios realizados. Estos repositorios deben estar debidamente respaldados. Cada proyecto informático tendrá 3 repositorios, uno por cada ambiente: desarrollo, prueba y producción.
- Toda mantención del software (actualizaciones o modificaciones), deberá ser analizada con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación. De efectuarse, deberán iniciar el ciclo nuevamente, comenzando con el levantamiento de requerimientos.

- Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.
- Según el proyecto se definirán los tiempos de la marcha blanca.
- Se deben revisar y auditar los controles de seguridad definidos en la etapa de diseño.
- El equipo de desarrollo debe revisar y auditar sus propios sistemas antes de pasar a la etapa de pruebas formales.
- Los programas computacionales que utilicen transacciones en línea deberán contar con los certificados de seguridad.

B. DESARROLLO EXTERNO

En materia de desarrollo de software externalizado, se debe considerar:

1. Seguridad en el Desarrollo

- El desarrollo seguro debe evidenciar la seguridad de las aplicaciones en el uso de principios y/o buenas prácticas de seguridad durante el ciclo de desarrollo del software (Requerimientos, Diseño, Desarrollo, Pruebas (Testing) e Implementación).
- Establecer requerimientos y controles de seguridad para el ciclo de vida de desarrollo de software, los cuales deben ser medibles en sus fases de Requerimiento y Control (ver A.2 "Requisitos y Controles de Seguridad).

2. Desarrollo Seguro

- Todo producto de software que sea utilizado por la Dirección de Salud Municipal debe encontrarse con sus licencias vigentes y las cláusulas de derechos de propiedad intelectual establecidos en los contratos vigentes.
- El desarrollador externo, debe realizar pruebas de seguridad técnica del aplicativo desarrollado, las cuales deben comunicarse a la unidad de Desarrollo de la Dirección de Salud Municipal para su aprobación.
- Se debe incorporar dentro de los requisitos de adjudicación la certificación de seguridad de dicho sistema.
- Todos los sitios tienen que tener certificado de seguridad y esto tiene que quedar definido en términos contractuales.
- Los programas computacionales que utilicen transacciones en línea deberán contar con los certificados de seguridad.
- En general, es deber, proporcionar todos los medios que estén a su alcance para impedir cualquier forma de divulgación de la Información Confidencial proporcionada por la Dirección de Salud Municipal o sus establecimientos dependientes.

8. 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.

9. 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 de Salud Municipal, las mejoras a implementar.

10. MECANISMOS DE DIFUSION DE LA POLÍTICA

La presente política, una vez aprobada, estará publicada en la página Web de la I. Municipalidad de Osorno (https://www.municipalidadosorno.cl/salud.php), en la página web de la Dirección de Salud Municipal (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.

11. TABLA DE MODIFICACIONES

VERSION	FECHA	PRINCIPALES MODIFICACIONES (PAGINA/ SECCIÓN)	MOTIVO DEL CAMBIO	MODIFICADO POR