Departamento de Informática

OSORNO, 08 DE ABRIL DEL 2026

MAT: REGLAMENTO SOBRE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, DE LA ILUSTRE MUNICIPALIDAD DE OSORNO.

REGLAMENTO Nro. 419

VISTOS:

El Decreto N° 83, de fecha 12.01.2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

El Reglamento N°225 de fecha 13.08.2015 sobre Políticas de Seguridad de la Información de la I.Municipalidad de Osorno.

El Informe Nro. 965 de fecha 27 de enero 2026 de la Contraloría Regional de Los Lagos.

Las facultades que me confieren la ley Orgánica Constitucional de Municipalidades N° 18.695 del año 1988 y sus posteriores modificaciones.

Las facultades que me confieren las letras i) del artículo 63 de dicho texto legal.

CONSIDERANDO:

La necesidad de actualizar el Reglamento N°225 de fecha 13.08.2015 referente a las observaciones emitidas por la auditoria efectuadas y dadas a conocer según pre informe e informe nro. 965 de fecha 27 de enero del 2026 emitido por la Contraloría Regional de los Lagos, cuya fiscalización tuvo el objeto de evaluar el nivel de seguridad de la información considerando la respectivas políticas, normas y procedimientos relacionado con temas de seguridad de la información en resguardo de la confidencialidad, integridad y disponibilidad de la información dentro de la organización.

RESUELVO DICTAR EL SIGUIENTE REGLAMENTO:

Generalidades.

El acceso por medio de un sistema de restricciones y excepciones a la información y los controles de seguridad es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, base de datos, equipos computacionales y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren del acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar e instruir a los mismos acerca de sus responsabilidades por el mantenimiento de controles eficaces, en particular aquellos relacionados con el uso de contraseñas y seguridad en el uso de equipamiento.

Para complementar la aplicabilidad de las exigencias del reglamento, todos los procedimientos señalados en el documento se reforzarán con los contenidos expuesto en el Plan informático municipal.

D O C U M E N T O C O N F I R M A E L E C T R Ó N I C A S I M P L E

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

La institución deberá proveer los recursos y medios necesarios para la aplicabilidad de la presente política.

Objetivo.

El propósito del reglamento es validar la generación de una política de seguridad de la información para la municipalidad de Osorno más actualizada en relación a la ya existente para considerar las nuevas exigencias en el marco normativo con resguardo principal en la confidencialidad, integridad, disponibilidad de la información y protección de datos.

El uso inapropiado de los servicios de red y equipos informáticos expone a la institución municipal a posibles pérdidas de información, ataques de virus, compromiso de los sistemas y servicios de red, e incluso a problemas en el ámbito legal y presupuestario.

Alcance.

La presente Política de seguridad de la información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de información, los sistemas informáticos y todo el equipamiento computacional que se utilice en el ambiente tecnológico del organismo.

Debe ser conocida y cumplida por todos los funcionarios municipales, tanto de planta, como a contrata y además del personal a honorarios que cumple funciones en los diferentes programas que cuente el municipio.

El alcance en el ámbito tecnológico considerara toda la infraestructura tecnológica, uso de sistemas informáticos, uso de equipamiento informático de todo tipo, uso de correos electrónicos institucionales.

Responsabilidad.

Cada usuario de la información y funcionario relacionado con algún activo informático, jefaturas de las diferentes direcciones y/o departamentos, equipo profesional y técnico informático que resguarda los servicios de red de la institución deberá velar por el correcto cumplimiento de las normas aquí descritas, y de acuerdo a lo indicado en el respectivo informe de evaluación de riesgos vigente, cualquier omisión voluntaria o involuntaria será sometida a la normativa vigente del estatuto administrativo.

ARTICULO 1.- Gestión de Activos.

La identificación de los activos ayuda a garantizar que se logre la protección eficaz de los activos. El inventario de activos debería incluir toda la información necesaria en caso de tener que recuperar el activo luego de un desastre. Esto incluye tipo de activo, formato, localización, información del respaldo y resguardo del mismo con relación a su administración, etc.

Los activos que se considerarán para el presente reglamento serán:

a) Información y archivos digitales
b) Infraestructuras de red
c) Activo de software
d) Activos físicos
e) Suministro de energía

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

f) Personal con acceso a algún activo informático.

Cada activo deberá contar con un responsable y será definido en la respectiva evaluación de riesgo vigente que la organización realice.

ARTICULO 2.- Políticas de control de acceso.

I. Gestión de usuarios y permisos.

Se limitará y controlara la asignación y uso de permisos a todos los sistemas informáticos, debido a que el uso inadecuado de los permisos del sistema resulta ser, frecuentemente, el factor que más contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuarios que requieran protección contra accesos no autorizados, deberán proveer una asignación de permisos, controlada mediante un proceso de autorización formal. Para ello se deben tener en cuenta lo siguiente:

a) Se contará con un sistema informático de solicitudes en línea (imoticket) que permitirá gestionar y actualizar los requerimientos de otorgamiento, revocación o cambios de permisos de accesos de los usuarios a las diferentes plataformas de gestión municipal. Dicho sistema será considerado como proceso formal de tramitación de autorización.

b) Identificar y mantener los usuarios y permisos asociados a cada uno de los sistemas, por ejemplo, sistema contabilidad, conciliación bancaría, imosgd gestión documental, Imodocs, Imoticket, sistema administración de base de datos y aplicaciones, etc., y las categorías de personal a las cuales deben asignarse los permisos.

c) Asignar los permisos a individuos sobre la base de la necesidad de uso y evento, por ejemplo, el requerimiento mínimo para su rol funcional, siempre y cuando cuente con la autorización de su jefe directo, o en su efecto por la autoridad competente según sea el caso.

Los permisos no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

e) Establecer un periodo de vigencia para el mantenimiento de los permisos, luego del cual los mismos serán revocados tanto en los sistemas de gestión como en los
respectivos equipamientos si fuese necesario.

Los propietarios de la información (jefaturas dueñas del proceso) serán los encargados de aprobar la asignación de permisos a usuarios y solicitar su implementación, lo cual será supervisado por el responsable o Encargado de la Seguridad de la Informática, decretado para tal efecto.

II. Clave de accesos.

Las claves de acceso son la **primera y principal línea de defensa** en cualquier sistema informático o aplicación. En un entorno institucional su importancia trasciende lo individual, ya que una clave débil puede comprometer datos de toda la organización.

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

La asignación de claves de acceso a cualquier plataforma deberá ser solicitada por Imoticket, siempre por la jefatura directa del funcionario, el cual una vez autorizado se le informará directamente al usuario a través de los medios que se estimen más seguros.

Dichas credenciales serán entregadas en calidad de temporales por lo cual será de responsabilidad de cada usuario actualizarla según lo instruido y recomendado, donde se deberá cumplir con lo siguiente:

a) Elegir claves que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos y no sean palabras de diccionario o nombres comunes;
b) Mantener en forma confidencial las claves que se le asignen;
c) No registrar sus claves en papel;
d) No almacenar clave en un computador de manera desprotegida;
e) No Compartir las claves con otros usuarios;
f) Cambiar las contraseñas a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que las claves normales; o en situaciones inmediata cuando haya indicios de un posible conocimiento o compromiso de la clave de acceso;

III. Acceso a la sala de servidores.

Otro activo de mayor importancia a resguardar será los servidores de datos el cual contendrá toda la información, estructuras de bases de datos y aplicaciones de las diferentes plataformas que el servicio cuente.

Se entiende por sala de servidores oficina cerrada en donde en su interior se encuentran todos los servidores de datos de la municipalidad de Osorno.

El acceso a dicha sala y el mecanismo de control se deberá especificar en un procedimiento claro de otorgamiento de acceso, eventos producidos y ejecutoriados dentro de la misma.

ARTICULO 3.- Revisión de los Derechos de acceso del usuario.

A fin de mantener un control eficaz en el acceso de los datos y servicios de información, el Encargado de Seguridad de la información de la Municipalidad, llevará a cabo un proceso formal, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios.

b) Revisar las autorizaciones de permisos de acceso total.

c) Revisar las asignaciones de permisos, a fin de garantizar que no se obtengan permisos no autorizados.

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

d) En caso de contratación, remoción o término de contrato de algún usuario se actualizarán los derechos de accesos desde el recibo a través del sistema de solicitudes (imoticket) por parte del superior jerárquico o por el departamento de personal.

e) El encargado de seguridad de la información, una vez avisado por el sistema de solicitud de acceso de cualquier cambio de funcionarios dentro de servicio, hará la revisión pertinente según lo indicado en la letra a) a los permisos de dicho funcionario en los sistemas y el respectivo equipo para adecuarlos a su nueva función.

f) Cada jefatura de las unidades, o en su efecto la Dirección de Recursos Humanos deberá informar obligatoriamente al encargado de seguridad de la información cuando en cada unidad llegue un funcionario a cumplir nuevas funciones o deje de pertenecer a dicha unidad por razones cualquieras.

ARTÍCULO 4.- Asignación de equipamiento computacional a los usuarios.

Todo equipamiento computacional será asignado y quedará bajo la responsabilidad de un funcionario con responsabilidad administrativa el cual deberá garantizar que dicho equipo asignado será usado y protegidos adecuadamente contra cualquier tipo de acceso no autorizado o bajo cualquier riesgo que se presente. Dicha asignación se formalizará a través de un acta de asignación emitida por el departamento de informática.

El área de informática procederá a configurar cada equipo computacional con las sesiones de cada usuario y además dejará generado una sesión propia de la unidad de informática para su futura auditoria y administración.

Para la seguridad de la información, los usuarios finales deberán cumplir con las siguientes pautas:

a) Cerrar las sesiones activas al finalizar las tareas, no obstante, cada equipamiento quedara configurado y protegido mediante un mecanismo de bloqueo de protector de pantalla por contraseña.

b) Mantener apagados los equipos cuando no se esté ocupando.

c) No facilitar su equipamiento a terceros sin reportarlo en el sistema de solicitudes Imoticket para considerarlo en la respectivas bitacoras, de lo contrario cualquier situación anormal quedará bajo su responsabilidad.

d) Mantener un respaldo periódico de toda la información local de importancia.

Con relación a equipamiento que sea asignado a funcionarios que no cuente con responsabilidad administrativa, esta responsabilidad quedara asignada al jefe directo de la unidad al que pertenece el funcionario.

Si un funcionario es trasladado o desvinculado del servicio y tenga asignado un equipamiento computacional, este quedara asignado automáticamente al jefe de la unidad al cual pertenecía, la que será formalizada con la respectiva acta de asignación o se asignara al funcionario que lo reemplace.

Los equipamientos no podrán ser trasladados a las nuevas unidades sin la previa autorización de la jefatura respectiva y la autorización del departamento de informática.

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

Puede que un equipamiento sea ocupado por mas de un usuario, en ese caso la asignación y la responsabilidad quedara otorgada al jefe de la unidad y desde el punto de vista operacional se habilitara más de una cuenta de usuarios en el equipamiento para que cada usuario acceda a través de sus respectivas credenciales. De requerir que los usuarios accedan a una misma cuenta de usuario, los usuarios serán responsable de la información almacenada en dicho periférico.

El responsable de la seguridad Informática deberá coordinar con el Departamento de Personal las tareas de concientización a todos los usuarios a través de sesiones de capacitación, acerca de los requerimientos y procedimientos de seguridad para la protección de equipos asignados, así como de sus funciones en relación a la implementación de dicha protección.

ARTICULO 5.- Pantallas limpias en las estaciones de trabajo.

Adoptar una política de trabajo, considerando pantallas limpias para proteger documentos en almacenamiento digital a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se entiende por pantallas limpias, en mantener todos los componentes lógicos del equipo ordenado y estructurarlos por tipo de carpeta y archivos para facilitar la búsqueda, respaldo y mantenimiento del mismo, evitando el exceso de contar con duplicidad de archivos.

La misma política se debe aplicar al uso de gestores de mensajería y/o correos electrónicos o documentación almacenada en la nube.

ARTICULO 6.- Uso de programas utilitarios de Sistema.

La mayoría de los equipos computacionales tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de seguridad de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deberán considerar lo siguiente:

a) Utilizar procedimientos de autorización para uso de programas utilitarios sean estos licenciados o no.

b) Queda estrictamente prohibido que personas internas o ajenas al organismo instalen programas utilitarios y haga uso, sin la debida autorización del usuario asignado al equipo, el responsable de seguridad de la información o del departamento de informática.
c) El encargado de la seguridad de la información deberá registrar y administrar todos los programas utilitarios que se utilicen en el servicio.

d) Remover todo el software basado en utilitarios y software de sistema innecesarios y que no se encuentren licenciados.

ARTÍCULO 7.- Computación y comunicaciones móviles.

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información municipal.

En este sentido, se deberá tener en cuenta cualquier dispositivo móvil y/o removible, incluyendo: notebook, tablet o PDA, teléfonos celulares y sus tarjetas de memoria,

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

dispositivos de almacenamiento removibles, tales como CDs, DVDs y cualquier medio de almacenamiento de conexión USB, tarjeta de identificación, dispositivos criptográficos, cámaras digitales, y además deberán incluirse todos los dispositivos que pudieran contener información relevante y confidencial del servicio.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarcarán los siguientes conceptos:

a) Uso y protección física necesaria.
b) El acceso seguro a los dispositivos.
c) La utilización de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios del organismo a través de dichos dispositivos.
e) En el caso que el dispositivo lo acepte, se mantendrá con contraseña mientras esté fuera de servicio.
f) Los mecanismos de resguardo de información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de incidentes del tipo de pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que lo utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales sobre la posesión de dispositivos móviles.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del municipio.

ARTICULO 8.- Uso de acceso Remoto.

Establecer un procedimiento normativo para el uso de la herramienta de acceso remoto dentro de la organización garantiza seguridad para la confidencialidad, integridad y disponibilidad de la información municipal. Esta norma es de cumplimiento obligatorio para cualquier conexión remota a activos tecnológicos institucionales.

Cualquier funcionario municipal, autorizado por el jefe del departamento al cual pertenece y/o por el encargado de la unidad de informática, que requiera tener acceso a la información de la institución desde redes externas, podrán acceder remotamente mediante un proceso de solicitud y autentificación formal, mediante el uso de conexiones seguras y utilizando la aplicación que el organismo disponga como activo de software para dicho fin y asegurando el cumplimiento de requisitos de seguridad del equipo al que se accede.

Dichos accesos se podrán realizar a modo de consulta o por razones de soporte como administrador de sistema, con la autorización formal del usuario quien tenga asignado el equipo al cual se quiere acceder.

ARTICULO 9.- Restricción del Acceso a la información.

Los usuarios de sistema de aplicación, incluyendo al personal de informática, tendrán acceso a la información y a las funciones de los sistemas de aplicación en conformidad con las Políticas de Control de Acceso definidas, sobre la base de los requerimientos de cada aplicación.

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El propietario de la información involucrada será responsable de la solicitud de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico más elevado, las mismas serán llevadas a cabo por personal del área de informática, conforme a una autorización formal emitida por el propietario de la información.
b) Controlar los derechos de acceso de los usuarios, por ejemplo, acceso modo consulta, acceso total o como administrador.

c) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan solo la información que resulte pertinente para el uso de la salida, y que, para el desarrollo de esta, se almacene en la respectiva base de datos el usuario, fecha y hora de la generación.

ARTICULO 10.- Almacenamiento de la Información.

El respaldo de información o Backup es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica, un error en su estructura lógica, perdidas de información ya sea por equivocación involuntaria o por acceso de tercero no autorizado, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

En relación al manejo de respaldo de la información se deberá:

a) Realizar respaldos periódicos, ya sea semanal y/o mensual de los respectivos servidores y estaciones de trabajo, el cual deberá ser de responsabilidad de la unidad de informática y del funcionario responsable de equipo asignado respectivamente.
b) La información de los servidores se extraerá en unidades y medio externos dentro de los que se encuentran servidores secundarios, unidades físicas de disco externo las cuales son trasladadas a un sitio diferente de donde fue generada. Dicha ubicación corresponde a una caja fuerte instalada en otra unidad municipal.
c) De dichos respaldos se dejará constancia a través del módulo de bitácora de la plataforma imoticket certificada por el funcionario responsable de la recepción y almacenamiento de dicha información.
d) Así mismo se exigirá que los servidores principales cumplan con todas las políticas de seguridad y almacenamiento existente como pueden ser backup progresivo, copia en servidores de respaldo, en disco espejos u equipos remotos, realizado preferentemente en horarios nocturnos para no afectar la performance del servicio.
e) Además, periódicamente y a medida que se realizan los respectivos soportes al equipamiento municipal se deberá ir efectuando los respectivos respaldos de cada una de las máquinas de los usuarios si corresponde, no obstante, la responsabilidad de mantener los respaldos actualizados de cada estación de trabajo (equipamiento de usuario) será siempre del funcionario asignado a dicho periférico.

D O C U M E N T O C O N F I R M A E L E C T R Ó N I C A S I M P L E

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

ARTICULO 11.- Mantenimiento de activos, equipos computacionales y servidores.

El departamento de informática será el responsable de realizar las respectivas mantenciones preventivas y correctivas cuando corresponda, las cuales se procederá de forma remota o presencial ya sea en el lugar de ubicación de la estación de trabajo o en las dependencias de la unidad técnica.

Toda mantención correctiva y preventiva se podrá efectuar remotamente previa autorización del funcionario asignado a dicha maquina o en su efecto de la respectiva jefatura, dejando constancia en la plataforma que gestiona las bitácoras del servicio.

Las mantenciones preventivas se calendarizarán de acuerdo a la disponibilidad de personal y/o presupuesto, o bajo situaciones de urgencia operativas si se diera el caso.

Las mantenciones de servidores serán efectuadas y calendarizadas por personal del municipio o a petición de proveedores de servicios contratados, el cual quedara registrado en la respectiva bitácora del servicio.

Cualquier otra mantención de algún activo que sufra algún desperfecto se realizará de acuerdo a la disponibilidad de repuesto, personal, tiempo o presupuesto disponible.

ARTICULO 12.- Gestión de dispositivos electrónicos para bajas o reutilización.

Para la reutilización el equipamiento computacional dentro de la organización se debe realizar la respectiva mantención preventiva y si es necesario también la mantención correctiva del activo, según el procedimiento establecido en el plan informático municipal.

Para dar de baja un activo informático según lo individualidad en el artiBasado en el informe técnico entregado por el departamento de informática
Para proceder con la baja de cualquier activo tecnológico que contenga información relevante, se procederá a remover y resguardar previamente dicha información en otro medio tecnológico y posteriormente se eliminara de forma segura tanto la información contenida, como también las aplicaciones licenciadas que esta contenga.

ARTICULO 13.- Control de cambios de sistemas informáticos.

El departamento de informática es el encargado de gestionar, evaluar, aprobar e implementar modificaciones en los sistemas informáticos, todo eso para minimizar riesgos y asegurando la estabilidad operativa de la información de la municipalidad.

Todo cambio deberá ser solicitado mediante la plataforma de ImoTicket, permitiendo su registro, seguimiento y control.

Antes de la implementación, los cambios deberán ser evaluados considerando su impacto, riesgos y posibles afectaciones a la disponibilidad del servicio.

Se deberá considerar lo siguiente:

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

a) Registrar toda la solicitud de cambio

b) Evaluar el impacto del cambio en los sistemas existentes
c) Contar con la aprobación del encargado de la unidad informática y, cuando corresponda el caso, de la jefatura solicitante respectiva
d) Realizar pruebas previas la implementación del cambio, esto para asegurar su correcto funcionamiento
e) Respaldar la información antes de ejecutar cambios que puedan afectar el software o información institucional
f) Registrar la implementación del cambio en la bitácora
g) Evitar la realización de cambios no autorizados o fuera de los procedimientos establecidos.

ARTICULO 14.- Intercambio de Datos entre Sistemas y Servidores.

El intercambio de datos entre los sistemas, aplicaciones y servidores, deberá realizarse de manera controlada, segura y debidamente autorizada, resguardando en todo momento la confidencialidad, integridad y disponibilidad de la información institucional.

Para estos efectos, todo flujo de información entre plataformas tecnológicas deberá ajustarse a procedimientos formales definidos en el Plan Informático, el cual establecerá los mecanismos técnicos, protocolos de comunicación, formatos de datos y medidas de seguridad aplicables a las integraciones, interoperabilidad de sistemas, servicios digitales y transferencias de información tanto internas como externas.

ARTICULO 15.- Control de Logs de Transacciones en Sistemas y Servidores.

La Municipalidad deberá mantener un control permanente y sistemático de los registros de actividad generados por sus sistemas, aplicaciones y servidores, con el propósito de resguardar la seguridad de la información, facilitar la detección de incidentes y asegurar la trazabilidad de las operaciones realizadas sobre los recursos tecnológicos institucionales.

La generación, almacenamiento y administración de estos registros deberá regirse por procedimientos definidos por el Departamento de Informática, los cuales deberán encontrarse documentados y actualizados. Dichos procedimientos establecerán las condiciones de registro, conservación, resguardo y revisión de los logs, considerando la criticidad de los sistemas y la sensibilidad de la información tratada.

ARTICULO 16.- Uso de Técnicas de Cifrado de Datos.

El resguardo de la información institucional deberá ser mediante el uso de técnicas de cifrado que permitan proteger los datos frente a accesos no autorizados, pérdida, alteración o divulgación indebida, tanto en su almacenamiento como durante su transmisión entre sistemas, servidores y aplicaciones. El cifrado deberá ser aplicado de acuerdo con la criticidad de la información y los riesgos asociados a su tratamiento, priorizando especialmente aquellos datos de carácter sensible o confidencial.

DOCUMENTO CON FIRMA ELECTRÓNICA SIMPLE

Escanear QR para Validar ó ingrese a https://verificacionsimple.imodigital.cl
CODIGO DE VERIFICACIÓN:212026249804817040

El uso de mecanismos de cifrado deberá regirse por procedimientos definidos por el Departamento de Informática. Dichos procedimientos establecerán los estándares, herramientas y prácticas autorizadas para el cifrado de información, así como los criterios para su implementación en sistemas, bases de datos, respaldos, dispositivos de almacenamiento y canales de comunicación.

ARTICULO 17.- El presente Reglamento regirá a partir de la fecha de su dictación. Déjese sin efecto el reglamento N°225 de fecha 13.08.2015 sobre Políticas de Seguridad de la Información, de la ilustre Municipalidad de Osorno, a contar del presente reglamento.

Publíquese en forma destacada el presente Reglamento en el sitio electrónico o página web de esta Municipalidad, a disposición permanente de los usuarios
.

ANÓTESE, COMUNIQÚESE EL PRESENTE REGLAMENTO A TODAS LAS UNIDADES DE LA I. MUNICIPALIDAD DE OSORNO, PUBLÍQUESE EN NUESTRO SITIO WEB, SIN PERJUICIO DE PERMANECER UN EJEMPLAR DEL MISMO A DISPOSICIÓN Y PARA CONOCIMIENTO PUBLICO EN LA SECRETARIA MUNICIPAL DE OSORNO, CÚMPLASE Y ARCHÍVESE.

JABV/YJUR/CGGM/LODP/jvhl/

D O C U M E N T O C O N F I R M A E L E C T R Ó N I C A S I M P L E

Escanear QR para Validar
o ingrese a https://verificacionsimple.imodigital.cl
FECHA DE EMISIÓN: 09-04-2026 18:29:15
CODIGO DE VERIFICACIÓN: 212026249804817040

JAIME ALBERTO BERTIN VALENZUELA
ALCALDE
jaime.bertin@imo.cl
09-04-2026 18:29:15

YAMIL JANNA UARAC ROJAS
SECRETARIO MUNICIPAL
yamil.uarac@imo.cl
10-04-2026 07:53:50