

**DECRETO ALCALDICIO N° 2385 /**  
**APRUEBA POLITICAS DE PROHIBICION DE**  
**DE USO DE SOFTWARE NO AUTORIZADO.**

**REQUINOA,** 02 AGO 2024

Esta Alcaldía decretó hoy lo siguiente:

**VISTOS :**

Las Facultades que me confiere la Ley N° 18.695 de 1988, Orgánica Constitucional de Municipalidades, Texto refundido coordinado y sistematizado, fijado por el D.F.L N°1 del Ministerio del Interior año 2006.

La Ley N° 18.575, Sobre Bases Generales de la Administración del Estado.

La Ley N° 19.880, Sobre Bases de los procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

**CONSIDERANDO :**

La necesidad del Municipio de contar con una Política de prohibición de uso de software no autorizado que permita guiar los procesos de control del área informática.

El Pre informe de Auditoria N°128 de 2024, sobre Auditoria a las Tecnologías de la Información y Comunicaciones, en la Municipalidad de Requinoa.

El Memo N°519 de fecha 01.08.2024 de Dirección de Administración y Finanzas el cual remite "Política de prohibición de uso de software no autorizado", el cual deberá aplicarse a todas las Direcciones de la Gestión Municipal.

La Providencia del Sr. Administrador Municipal, quien indica que el Reglamento citado se encuentra revisado, por lo que se deberá proceder a la dictación del decreto Alcaldicio correspondiente.

**DECRETO :**

**APRUEBASE** la Política de prohibición de uso de software no autorizado de la Municipalidad de Requinoa, y déjese sin efecto cualquier acto administrativo anterior.

**ANOTESE, COMUNIQUESE Y ARCHIVESE.-**

  
**MARIO MENA NORIEGA**  
**SECRETARIO MUNICIPAL(S)**

  
**WALDO VALDIVIA MONTECINOS**  
**ALCALDE**

WVM/CAB/MMN/FNM/knc.

**DISTRIBUCION:**

Secretaría Municipal  
Dirección Administración y finanzas  
Dideco  
Dpto. de Tránsito y Transporte público  
Control  
Dirección de Obras Municipales  
Juzgado de Policía Local  
Secpla  
Dirección de Seguridad Pública  
Archivo

## Políticas de Prohibición de Uso de Software No Autorizado

### Objetivo

Estas políticas tienen como objetivo proteger los sistemas de información de la organización, garantizando que todo el software utilizado sea legal, seguro y aprobado por los responsables de tecnología.

### Alcance

Estas políticas se aplican a todos los empleados, contratistas, consultores y cualquier otra persona que utilice los recursos informáticos de la organización.

### Directrices Generales

#### 1. Definición de Software Autorizado:

- Solo se permitirá el uso de software autorizado y licenciado legalmente, el cual será instalado por los funcionarios de la unidad de informática de la municipalidad.
- El software debe ser aprobado por la unidad de informática o por los responsables designados para asegurar que cumple con los estándares de seguridad y compatibilidad.
- En caso de ser requerido un software específico este debe ser solicitado por medio de un correo electrónico, el cual debe ser autorizado previamente por el directivo a cargo del funcionario solicitante y deberá ser dirigido a la casilla [informatica@requinoa.cl](mailto:informatica@requinoa.cl).

#### 2. Prohibición de Software No Autorizado:

- Está estrictamente prohibido instalar, ejecutar o utilizar cualquier software no autorizado en los dispositivos de la Municipalidad.
- Esto incluye software descargado desde Internet, software de fuente desconocida, y software personal no aprobado por la unidad de Informática.

#### 3. Responsabilidades de los Usuarios:

- Los usuarios deben informar a la unidad de informática sobre cualquier necesidad de software adicional que no esté actualmente autorizado.
- No deben intentar eludir las políticas instalando o utilizando software no autorizado.
- Los usuarios que instalen softwares no autorizados o de origen desconocidos, deberán asumir las responsabilidades legales y/o sanciones económicas según sea el caso.

#### 4. Inspecciones y Auditoría:

- El departamento de informática se reserva el derecho de realizar inspecciones y auditorías para verificar el cumplimiento de estas políticas.
- Se puede requerir la eliminación inmediata de cualquier software no autorizado encontrado durante estas inspecciones.

- Se levantará un acta con las observaciones de los softwares encontrados en uso en el momento de la revisión, la cual será enviada al administrador municipal y al directivo a cargo del funcionario. Para su conocimiento y “posterior sanción administrativa.”

**5. Consecuencias por Incumplimiento:**

- El incumplimiento de estas políticas puede resultar en acciones disciplinarias, que pueden incluir advertencias, **suspensión o terminación del empleo**, según la gravedad del caso.

**6. Educación y Concientización:**

- Se proporcionará información y material educativo regular sobre la importancia del uso de software autorizado y los riesgos asociados con el uso de software no autorizado.

**Implementación**

- **Comunicación:** Estas políticas deben ser comunicadas claramente a todos los empleados y personal relevante. Se debe obtener un acuse de recibo para asegurar que todos estén informados y entiendan las consecuencias del incumplimiento.
- **Actualización:** Las políticas deben ser revisadas y actualizadas periódicamente para mantenerse al día con los cambios en la tecnología y las amenazas de seguridad.
- **Apoyo de la Alta Dirección:** Es crucial contar con el apoyo y respaldo de la alta dirección para asegurar la implementación efectiva de estas políticas y promover una cultura de seguridad de la información en toda la organización.