

**Reglamento para el Uso de los Recursos
Tecnológicos de Información y Comunicación
de la Municipalidad de Zarceró**

CAPÍTULO I

Disposiciones generales

Artículo 1º — El presente Reglamento tiene como objetivo **establecer las normas y directrices para el uso adecuado de los Recursos Tecnológicos de Información y Comunicación (TIC) de la Municipalidad de Zarceró**. Aplica a todos los servidores municipales en el ejercicio de sus funciones, así como a aquellos que hagan uso de estos recursos, conforme a lo establecido en el ordenamiento jurídico administrativo y laboral vigente, el Código Municipal y el Reglamento Interno de Trabajo de la Municipalidad de Zarceró.

Artículo 2º — Para todos los efectos legales que se deriven de la aplicación de este Reglamento, se establecen las siguientes conceptualizaciones:

- a) Institución: Municipalidad de Zarceró.
- b) Usuario: Funcionario o colaborador de la Municipalidad de Zarceró, incluyendo personal temporal, contratistas o cualquier persona autorizada que utilice los recursos tecnológicos de la Institución.
- c) Área de Tecnologías de Información y Comunicación: Dependencia de la Municipalidad de Zarceró responsable de la **planificación, gestión, desarrollo, mantenimiento y seguridad de la infraestructura y servicios de tecnologías de información y comunicación** de la Institución, y de garantizar el soporte y la orientación sobre su uso adecuado
- d) Software: Programas o aplicaciones que se ejecutan en el computador.
- e) Equipo de cómputo: Incluye, pero no se limita a, computadoras de escritorio, portátiles, tabletas, teléfonos inteligentes, servidores, impresoras, escáneres, módems, punteros, proyectores, dispositivos de almacenamiento (internos o externos) y cualquier otro hardware o periférico que procese o almacene información digital.
- f) Telemática: Área o disciplina que integra las telecomunicaciones y la informática para el envío, recepción y procesamiento de datos.
- g) Contraseña (Password): Cadena de caracteres secreta utilizada para verificar la identidad de un usuario y controlar el acceso a recursos tecnológicos, sistemas o información.
- h) Recursos Tecnológicos de Información y Comunicación (TIC): Comprenden todos los activos tecnológicos de la Institución, incluyendo hardware (equipos de cómputo, dispositivos, periféricos, servidores), software (sistemas operativos, aplicaciones, bases de datos), servicios de red (intranet, internet, telefonía IP), comunicaciones electrónicas

- (correo, mensajería instantánea), almacenamiento de datos (local o en la nube) y la información digital gestionada por la Municipalidad." (Más completo y moderno).
- i) Almacenamiento en Nube: Modelo de servicio que permite a los usuarios almacenar y gestionar sus datos digitales (archivos, aplicaciones, bases de datos, etc.) en una infraestructura de servidores remotos e interconectados, la cual es propiedad y está operada por un proveedor de servicios de terceros.
 - j) Información Institucional: Todo dato, documento, registro o activo digital creado, procesado, almacenado o transmitido por la Municipalidad o en su nombre, independientemente de su formato o soporte, y que es propiedad o responsabilidad de la Institución."
 - k) Ciberseguridad/Seguridad de la Información: "Conjunto de medidas técnicas, organizativas y humanas destinadas a proteger los sistemas de información, la infraestructura tecnológica y los datos de la Municipalidad contra amenazas, vulnerabilidades, accesos no autorizados, daños, interrupciones o cualquier otra forma de uso indebido.
 - l) Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.
 - m) Incidentes de Seguridad: Cualquier evento adverso, confirmado o sospechado, que comprometa la confidencialidad, integridad o disponibilidad de los recursos tecnológicos o la información de la Municipalidad.
 - n) Autenticación de Múltiples Factores (MFA/2FA): Método de seguridad que requiere que un usuario proporcione dos o más formas de verificación para obtener acceso a un recurso, lo que añade una capa adicional de protección más allá de una simple contraseña.
 - o) DTIC: Departamento de Tecnologías de Información y Comunicación.
 - p) **BYOD (Bring Your Own Device)**: Práctica o modelo que permite a los usuarios emplear sus dispositivos tecnológicos personales (ej. smartphones, tabletas, laptops) para acceder a los recursos y sistemas de la Municipalidad, y para realizar actividades laborales. Esta modalidad requiere la adhesión a políticas específicas de seguridad y uso definidas por el DTI.
 - q) **Mesa de Ayuda o HelpDesk**: Servicio de soporte técnico centralizado que, mediante una plataforma diseñada para tal fin, asiste a los usuarios de la Municipalidad en la resolución de incidentes, problemas y consultas relacionadas con los recursos tecnológicos y sistemas institucionales.

Artículo 3º — El Departamento de Tecnologías de Información y Comunicación (DTIC) **será el ente técnico consultor y proponente de las políticas, estándares y procedimientos en**

materia de tecnologías de información y comunicación que regirán en la Institución. Dichas políticas, previa valoración y aprobación por parte de la Municipalidad de Zarceró, podrán ser modificadas, divulgadas y actualizadas de manera periódica para adaptarse a la evolución tecnológica y a las necesidades institucionales.

CAPÍTULO II

Deberes y atribuciones

Artículo 4º — **Del Departamento de Tecnologías de Información y Comunicación.** Para efectos del cumplimiento del presente reglamento, son funciones del Departamento de Tecnologías de Información y Comunicación:

- a) Planear, dirigir, coordinar y supervisar las labores y actividades, administrativas, técnicas, desarrollo de las plataformas tecnológicas e **implementación de ciberseguridad** y la **gestión de riesgos tecnológicos** como órgano administrativo municipal responsable por la adquisición, desarrollo y la aplicación de las herramientas, productos, servicios y proyectos relacionados con el uso de las Tecnologías de Información y Comunicación.
- b) Colaborar en la definición de políticas, estrategias, programas de trabajo, aspectos relacionados con los recursos humanos y otros, en el área de tecnologías de Información y Comunicación, en coordinación con las dependencias competentes.
- c) Determinar los requerimientos técnicos en el área de Tecnología de Información y Comunicación de la Institución.
- d) Elaborar y evaluar todos los planes y programas generales de trabajo en el área de Tecnologías de Información y Comunicación de las dependencias de la Municipalidad de Zarceró, prestando colaboración para que se establezcan las medidas de organización, coordinación e integración que permitan cumplir con los programas de acuerdo con las políticas de la municipalidad.
- e) Definir en el ámbito global los alcances y objetivos de los proyectos en el área de Tecnologías de Información y Comunicación por desarrollar.
- f) Coordinar y formular especificaciones técnicas y estratégicas para la adquisición de suministros, de equipo de cómputo, dispositivos, productos, telecomunicaciones y servicios relacionados, así como en el proceso de análisis, aprobación o rechazo de toda solicitud de compra o adquisición de recursos y **gestionar el ciclo de vida de los activos tecnológicos** relacionados con las Tecnologías de Información y Comunicación para la Municipalidad de Zarceró.
- g) Dirigir las funciones de control que garanticen el fiel cumplimiento de las normas estándares establecidos y las medidas de seguridad interna.

- h) Asesorar, informar y orientar a los funcionarios de la Municipalidad de Zarceró en cuanto al correcto uso de las Tecnologías de Información y Comunicación y **promover la concienciación en ciberseguridad.**
- i) Realizar estudios e investigaciones que permitan instrumentar procedimientos que faciliten el uso de la información contenida en las bases de datos y sistemas de información que resulten de interés para la toma de decisiones.
- j) Implementar los proyectos de administración de información que requiera la Institución.
- k) Dirigir y coordinar el diseño, desarrollo, implantación y mantenimiento de páginas, portales y aplicaciones en ambiente Web.
- l) Dar mantenimiento preventivo y correctivo a los equipos de cómputo que posee la Institución, así como supervisar y controlar esta labor cuando por necesidad o conveniencia del departamento de tecnologías de información, sea adjudicada a terceros.
- m) Mantener un **inventario actualizado de todos los recursos tecnológicos** y de los usuarios asignados a los mismos, para identificar responsabilidades en caso de mal uso, daños o alteraciones no autorizadas.
- n) Establecer y gestionar los **mecanismos seguros de reseteo y recuperación de contraseñas de usuario**, garantizando su confidencialidad. Para credenciales de administración de sistemas y servicios críticos institucionales, el DTIC debe **implementar un sistema de gestión de credenciales que garantice su custodia, rotación, y acceso just-in-time bajo estricta supervisión.**
- o) Investigar sobre nuevas tecnologías de información y comunicación que ofrezca el mercado, a fin de evaluar la factibilidad de su aplicación en la institución.
- p) Administrar y controlar la Intranet Institucional.
- q) Administrar y promover los accesos a Internet de todos los funcionarios de la Municipalidad de Zarceró que así lo requieran para mejorar el desempeño de sus funciones.
- r) Guardar la confidencialidad en cuanto a la **información institucional sensible**, sistemas, respaldos de información, **y cualquier dato de carácter personal** al que tengan acceso en el ejercicio de sus funciones, así como los mecanismos de acceso privilegiado a los recursos.
- s) Administrar todos los sistemas municipales, financieros y administrativos.
- t) Establecer, mantener y ejecutar un plan de respuesta a incidentes de seguridad, incluyendo la detección, análisis, contención, erradicación y recuperación.
- u) Realizar auditorías periódicas y monitoreo constante de los sistemas y redes para identificar vulnerabilidades, accesos no autorizados y actividades sospechosas.
- v) Identificar, evaluar y gestionar las vulnerabilidades en los sistemas y aplicaciones de la Institución.
- w) Asegurar el cumplimiento de las licencias de software y la correcta administración de los contratos con proveedores de TIC.

- x) Colaborar con las instancias pertinentes en la implementación y cumplimiento de las normativas de protección de datos personales.
- y) Establecer y mantener operativa una Mesa de Ayuda (HelpDesk) que brinde soporte técnico a los usuarios para la gestión de incidentes, problemas y requerimientos relacionados con los recursos y servicios de Tecnologías de Información y Comunicación de la Municipalidad.
- z) Todas aquellas que se establezcan en el presente reglamento

Artículo 5° — **Del usuario.** El usuario es responsable de la adecuada conservación del equipo de cómputo y dispositivos que la Municipalidad de Zarceró le provea para el desempeño de sus labores, **así como de la protección de la información institucional bajo su custodia, de acuerdo con su clasificación y las políticas de seguridad.** Son deberes del usuario:

- a) Utilizar el equipo de cómputo y sus componentes únicamente para realizar trabajos funciones y actividades laborales vinculadas a los objetivos municipales, procurando la racionalidad en su uso y los suministros que se le otorguen en relación con éste.
- b) Procurar que el equipo de cómputo y sus componentes se mantengan en condiciones adecuadas de limpieza.
- c) Asegurarse de que el programa antivirus Institucional esté activo y actualizado en sus equipos, y **reportar de inmediato al DTIC mediante la Mesa de Ayuda (HelpDesk) cualquier sospecha de infección o mal funcionamiento del antivirus.** Verificar la existencia de software malicioso en dispositivos de almacenamiento externos antes de su uso.
- d) Realizar **copias de seguridad periódicas de la información crítica** que reside en los dispositivos asignados, siguiendo las políticas y procedimientos establecidos por el Departamento de Tecnologías de Información y Comunicación.
- e) Mantener la información almacenada en sus equipos de forma organizada, eliminando archivos temporales o no institucionales, y gestionando el almacenamiento de acuerdo con las directrices del DTIC.
- f) Asegurarse de que las copias de seguridad personales, cuando sean requeridas o autorizadas, se realicen y custodien de forma segura y de acuerdo con las directrices del DTIC.
- g) Garantizar la privacidad de sus claves de acceso al equipo de cómputo, a los sistemas municipales y archivos compartidos, así como evitar la difusión de estos y **no compartirlas con nadie bajo ninguna circunstancia, ni siquiera con el personal del DTIC. Utilizar contraseñas robustas y únicas para cada sistema o servicio, y cambiarlas periódicamente según las políticas de seguridad.** Las contraseñas robustas deben cumplir con con una longitud mínima de 12 caracteres, incluyendo al menos una letra mayúscula, una minúscula, un número y un carácter especial. Queda estrictamente prohibido el reuso de contraseñas anteriores y su divulgación a terceros, incluso al personal del Departamento de Tecnologías de Información y Comunicación

(DTIC). Asimismo, las contraseñas deberán ser cambiadas periódicamente según la política interna establecida por el DTIC y el uso de Autenticación de Múltiples Factores (MFA) será obligatorio para el acceso a los sistemas y servicios críticos que determine dicho Departamento. Cualquier sospecha de compromiso de una credencial deberá ser informada de inmediato al DTIC.

- h) Informar por escrito al Departamento de Tecnologías de Información y Comunicación sobre la presencia de cualquier equipo o dispositivo personal en el lugar de trabajo, **especialmente si se conecta a la red institucional o procesa información municipal**. El DTIC establecerá las políticas para el uso de equipos personales (BYOD).
- i) Acatar aquellas instrucciones divulgadas por el departamento de Tecnologías de Información y Comunicación en cuanto al uso de los distintos recursos tecnológicos.
- j) Responder por daños o atrasos ocasionados por la pérdida de información u omisión de respaldo o por el mal uso de los equipos de cómputo.
- k) Solicitar la autorización, por escrito y con visto bueno del superior inmediato, al departamento de Tecnologías de Información y Comunicación cuando requiera utilizar otro equipo de cómputo que no está bajo su responsabilidad.
- l) Solicitar la autorización, por escrito y con visto bueno del superior inmediato, al departamento de Tecnologías de Información y Comunicación, cuando su equipo va a ser utilizado por otro funcionario.
- m) Solicitar la autorización, por escrito y con visto bueno del superior inmediato, al Departamento de Tecnologías de Información y Comunicación, cuando su equipo va a ser trasladado de la posición asignada por el departamento de Tecnologías de Información.
- n) Informar de manera inmediata al departamento de Tecnologías de Información y Comunicación por medio de la Mesa de Ayuda (HelpDesk), cuando algún equipo de cómputo sufra algún problema técnico **o cualquier incidente de seguridad informática (ej. pérdida de datos, sospecha de acceso no autorizado, intento de phishing)**.
- o) Procurar que el equipo de cómputo asignado no sea utilizado por terceros sin autorización del departamento de Tecnologías de Información y Comunicación.
- p) Participar activamente en las capacitaciones y campañas de concienciación en ciberseguridad que promueva el DTIC.
- q) Cumplir con la normativa interna y externa sobre protección de datos personales al manejar información de ciudadanos, funcionarios o terceros.
- r) Reportar de forma inmediata al Departamento de Tecnologías de Información y Comunicación mediante la Mesa de Ayuda (HelpDesk) cualquier incidente de seguridad, actividad sospechosa o vulnerabilidad detectada.
- s) Activar y utilizar la autenticación de múltiples factores cuando esta esté disponible o sea requerida para acceder a los sistemas institucionales.
- t) Cerrar sesión en los sistemas y bloquear los equipos al ausentarse temporalmente del puesto de trabajo.

- u) Cumplir con las políticas específicas para el uso de dispositivos móviles institucionales y personales que accedan a recursos municipales.
- v) Es obligación de cada usuario solicitar todo requerimiento de soporte técnico, sobre cualquier recurso o sistema institucional, utilizando la Mesa de Ayuda (HelpDesk) dispuesta para tal fin.
- w) Todas aquellas que se establezcan en el presente reglamento.

Artículo 6° — **Prohibiciones generales.** Queda absolutamente prohibido al usuario:

- a) Emplear los recursos tecnológicos asignados para actividades extralaborales y prohibida la reproducción, descarga, almacenamiento o difusión de cualquier tipo de material protegido por la Ley de Derechos de Autor sin la debida licencia o autorización, o para fines no institucionales.
- b) Abrir el equipo de cómputo para su revisión, reparación o instalar aplicaciones en el mismo, asimismo variar la configuración inicial provista para el equipo o **realizar modificaciones físicas o lógicas no autorizadas.**
- c) Los equipos de cómputo no podrán ser desmantelados, cambiados, abiertos ni reparados por los usuarios, y sus componentes (entiéndase “mouse”, disco duro, teclado, memoria, fuente de poder, tarjeta madre entre otros) no podrán ser removidos por personal no autorizado por el departamento de Tecnologías de Información y Comunicación.
- d) Utilizar únicamente dispositivos de almacenamiento externo que sean de procedencia conocida y que hayan sido previamente verificados mediante el sistema antivirus institucional o autorizados por el DTIC. Se prohíbe la conexión de dispositivos personales no autorizados que puedan comprometer la seguridad o integridad de la red.
- e) Ingerir alimentos o bebidas en las áreas donde se encuentran ubicados los equipos de cómputo.
- f) Utilizar el equipo de cómputo para generar mensajes anónimos obscenos u ofensivos, así como para divulgar material pornográfico o que ofenda la dignidad humana, **contenido ofensivo, discriminatorio, ilegal o que atente contra la dignidad humana o las políticas de la Institución.**
- g) Trasladar los equipos de cómputo fuera de las otras oficinas municipales, salvo que por razones de trabajo así se requiera y **siempre bajo la aprobación y registro del Departamento de Tecnologías de Información y Comunicación.**
- h) Instalar cualquier tipo de software, aplicación o extensión sin la previa autorización del Departamento de Tecnologías de Información y Comunicación.
- i) Deshabilitar, modificar o eludir las medidas de seguridad implementadas por el DTIC (antivirus, firewall, actualizaciones de sistema, etc.).
- j) Intentar acceder a sistemas, redes o información para la cual no se tienen permisos explícitos.

- k) Participar o colaborar en intentos de ingeniería social (ej. responder a correos de phishing, divulgar información sensible bajo presión).
- l) Conectar dispositivos personales a la red institucional sin la debida autorización (ej. routers personales, extensores Wi-Fi).
- m) Utilizar los recursos institucionales para la minería de criptomonedas, actividades de hacking, distribución de malware o cualquier otra actividad ilegal o no ética.
- n) Introducir información confidencial o datos personales de la Municipalidad en herramientas de Inteligencia Artificial generativa públicas (ej. ChatGPT, Bard, Copilot) sin la previa autorización y las salvaguardas establecidas por el DTIC
- o) Todas aquellas que se establezcan en el presente reglamento

CAPÍTULO III

Del equipo de cómputo

Artículo 7º — Es responsabilidad del usuario asegurar que el equipo de cómputo de escritorio asignado esté conectado a una fuente de energía ininterrumpida (UPS) y velar por el buen funcionamiento y el correcto uso de todos los componentes conectados a dicho equipo. Los equipos de cómputo portátiles no requerirán obligatoriamente el uso de UPS, **siempre y cuando dispongan de su propia batería en buen estado de funcionamiento.**

Artículo 8º— Todos los equipos de cómputo propiedad de la Municipalidad de Zarceros **deben ser inventariados** por el departamento correspondiente. El Departamento de Tecnologías de Información y Comunicación no prestará servicios de soporte o mantenimiento a equipos que no estén debidamente inventariados e identificados por la Institución.

Artículo 9º — Todos los equipos y dispositivos tecnológicos, ya sean adquiridos por presupuesto institucional o donados a la Municipalidad, deben ser gestionados por el Departamento de Tecnologías de Información y Comunicación para su **revisión técnica, configuración inicial y aplicación de las políticas de seguridad**, previo a su asignación y puesta en operación.

Artículo 10 — La Alcaldía y la Jefatura del Departamento de Tecnologías de Información y Comunicación podrán, en cualquier momento y sin previo aviso, inspeccionar los equipos, dispositivos y el software instalado, así como los registros de actividad (logs) y archivos almacenados en los discos duros o en la nube institucional. **Esta inspección se realizará en estricto cumplimiento de la legislación vigente y no incluirá el acceso directo al contenido de los correos electrónicos, salvo que exista una orden judicial o una sospecha fundamentada de actividad ilícita o de incumplimiento grave de este reglamento, debidamente autorizada por la autoridad competente.** La información institucional en los equipos siempre es susceptible de inspección.

CAPÍTULO IV

Del Software

Artículo 11° — Los usuarios podrán utilizar exclusivamente el software debidamente instalado y autorizado por el Departamento de Tecnologías de Información y Comunicación. Queda estrictamente prohibido instalar cualquier software no autorizado, incluyendo programas, aplicaciones, juegos, protectores de pantalla o cualquier material protegido por la Ley de Derechos de Autor sin la licencia correspondiente.

Artículo 12° — Queda absolutamente prohibido al usuario alterar la configuración del software provisto por el Departamento de Tecnologías de Información y Comunicación. El DTIC mantendrá un registro del software instalado y de las configuraciones estándar. En caso de detectarse alguna anomalía en el uso del equipo o variación del software o su configuración inicial, se realizará el reporte correspondiente al superior inmediato del usuario, con copia a la Dirección respectiva, para el establecimiento de las responsabilidades del caso y la aplicación de las medidas disciplinarias pertinentes

Artículo 13° — Es deber del usuario velar por que el software antivirus de su equipo esté activo y actualizado. En este sentido, debe **reportar de inmediato** al Departamento de Tecnologías de Información y Comunicación cualquier sospecha de desactualización, mal funcionamiento o detección de amenazas.

Artículo 14° — Todo software protegido por derechos de autor que esté instalado o sea utilizado en equipos de la Municipalidad de Zarcero debe contar con la licencia de uso correspondiente. La custodia y gestión de estas licencias es responsabilidad del Departamento de Tecnologías de Información y Comunicación. En caso de que un usuario requiera la adquisición o uso de un programa para fines institucionales, deberá tramitar la licencia a través del DTIC. La instalación de dicho software será realizada exclusivamente por personal del Departamento de Tecnologías de Información y Comunicación, quien lo incorporará al inventario institucional de licencias.

CAPÍTULO V

Recursos Telemáticos

Uso de la Red de Institucional

Artículo 15° — La red institucional, incluyendo las conexiones alámbricas e inalámbricas (Wi-Fi), es de uso exclusivo para asuntos laborales y el desempeño de las funciones municipales.

Artículo 16° — Todo usuario deberá contar con un nombre de usuario (login) y una contraseña (password) personalizados para acceder a la red institucional y los sistemas. Estas credenciales son **estrictamente personales e intransferibles**, y es deber del usuario **mantener su confidencialidad, no compartirlas y modificarlas periódicamente de acuerdo con las**

políticas de seguridad. Las acciones realizadas desde una cuenta de usuario son de entera responsabilidad de su titular.

Artículo 17°— El usuario podrá almacenar en los servidores de red únicamente información institucional, aplicaciones institucionales y archivos compartidos esenciales para las labores de la Municipalidad. Los archivos de carácter personal o no institucionales no deben almacenarse en la red ni en los equipos municipales. El Departamento de Tecnologías de Información y Comunicación realizará copias de seguridad (respaldos) periódicas y automatizadas de la información almacenada en los servidores institucionales, de acuerdo con las políticas de respaldo y recuperación de datos.

Artículo 18°— Es deber de cada Jefatura o Dirección solicitar al Departamento de Tecnologías de Información y Comunicación la inclusión o modificación de accesos a la red y a los sistemas de información, de acuerdo con los movimientos de personal (ingresos, traslados, ascensos) que se produzcan en su Departamento o Unidad. Así mismo, la Jefatura o Dirección es responsable de notificar por escrito y de forma inmediata al DTIC por medio de la Mesa de Ayuda (HelpDesk), sobre la salida o traslado de un usuario a su cargo, con el fin de que se inhabiliten, modifiquen o eliminen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes. El Departamento de Recursos Humanos deberá, además, notificar al DTIC mediante la Mesa de Ayuda (HelpDesk) la salida definitiva de cualquier funcionario de la Institución.

Artículo 19° — El acceso a la red o a cualquier sistema utilizando credenciales ajenas, o el uso indebido de las propias, constituirá una falta grave. El encargado del Departamento de Tecnologías de Información y Comunicación reportará por escrito esta situación al usuario, con copia a su superior inmediato y a la Alcaldía Municipal, para que se establezcan las responsabilidades del caso y se inicie el procedimiento disciplinario correspondiente.

CAPÍTULO VI

Del uso de Internet

Artículo 20°— El uso del servicio de Internet está limitado a atender las necesidades derivadas del desempeño de las labores del usuario y se regirá por las siguientes pautas:

- a) Los servicios de acceso a Internet permitidos de forma general son: Acceso a servidores WEB, acceso a correo electrónico, y otros servicios esenciales para las funciones municipales definidos por el DTIC.
- b) Cualquier acceso adicional a los citados en el punto anterior deberá solicitarse con la debida justificación y autorización de la Jefatura correspondiente, ante el Departamento de Tecnologías de Información y Comunicación. Será responsabilidad de este Departamento evaluar y autorizar o denegar el acceso a dichos servicios, basándose en criterios de necesidad laboral y seguridad.

Artículo 21°— El uso de Internet es de carácter laboral. Se prohíbe mantener sesiones de internet abiertas de forma continua si no se están utilizando activamente para fines institucionales, y su uso para asuntos personales queda estrictamente prohibido.

Artículo 22°— Es prohibido para los usuarios de internet:

- a) Utilizar programas de comunicación instantánea no autorizados o no provistos por la Institución para fines laborales. En caso de requerir el uso de estos servicios, se debe solicitar al DTIC con la debida autorización y justificación del jefe inmediato.
- b) El acceso a cualquier sitio pornográfico o erótico que pueda ofender la dignidad del ser humano o **que promueva la discriminación, la violencia o el odio.**
- c) El acceso a cualquier sitio de juegos o apuestas.
- d) El acceso a sitios de compras en línea para fines personales.
- e) El acceso a sitios para escuchar música o ver videos que no estén directamente relacionados con el desempeño de las labores del funcionario o que consuman un ancho de banda excesivo.
- f) El acceso a sitios de violencia
- g) La descarga, copia o distribución de material protegido por derechos de autor sin la debida licencia, o de cualquier contenido que no esté directamente relacionado con las funciones municipales, o que pueda comprometer la seguridad de la red institucional.
- h) Visitar sitios de redes sociales u otros similares, a excepción de que sea para efectos relacionados con su trabajo. En caso de uso laboral, debe seguirse la política de uso de redes sociales institucional.
- i) El acceso a sitios de entretenimiento para fines personales durante la jornada laboral o que afecten la productividad.
- j) El acceso para fines comerciales y otros ajenos a la actividad propia del funcionario o de terceros.

Artículo 23°— La Municipalidad de Zarceró, a través del Departamento de Tecnologías de Información y Comunicación, monitorea el tráfico de correo electrónico y otras comunicaciones para proteger la red de amenazas (malware, phishing, spam) y asegurar el cumplimiento de las políticas de uso. No obstante, se respeta la privacidad de las comunicaciones personales en la medida que la ley lo permita y no exista sospecha fundada de incumplimiento de este reglamento, actividad ilícita o incidente de seguridad, en cuyo caso se procederá de acuerdo con el artículo 10 de este reglamento.

Artículo 24° — De ser necesario, el Departamento de Tecnologías de Información y Comunicación podrá establecer horarios o limitaciones de ancho de banda para el uso de determinados servicios, a fin de garantizar el buen desempeño de la red y los recursos relacionados, y asegurar la continuidad operativa de los servicios prioritarios.

Artículo 25° — El Departamento de Tecnologías de Información y Comunicación implementará herramientas de monitoreo y control para detectar, analizar y bloquear accesos no permitidos o actividades que pongan en riesgo la seguridad de los recursos informáticos, comprometan la información institucional o atenten contra su desempeño y las políticas de uso establecidas.

Artículo 26° — En caso de que el Departamento de Tecnologías de Información y Comunicación identifique una falla de seguridad, una vulnerabilidad crítica o un incidente que comprometa los recursos tecnológicos o la información institucional, podrá suspender de forma temporal y sin previo aviso el acceso a los servicios de red, comunicaciones electrónicas e Internet a un usuario, grupo de usuarios o a toda la red, mientras la situación es corregida o contenida, con el objetivo de prevenir problemas adicionales o la propagación de la amenaza.

Artículo 27° — El Departamento de Tecnologías de Información y Comunicación **tiene la facultad de consultar los historiales (logs), bitácoras y sus respectivos respaldos de actividad** en los sistemas, la red y el uso de Internet de todos los usuarios, con el fin de garantizar el cumplimiento de este reglamento, la seguridad de la información institucional, la investigación de incidentes de seguridad o actividades sospechosas, y la optimización de los recursos.

CAPÍTULO VII De los Procedimientos

Artículo 28° — El Departamento de Tecnologías de Información y Comunicación establecerá y mantendrá actualizados los procedimientos internos que detallan la implementación y gestión de las normas establecidas en este reglamento, así como el uso específico de las diversas tecnologías de información y comunicación de la Municipalidad de Zarceró.

Artículo 29° — Una vez establecidos y divulgados, los procedimientos específicos definidos por el DTIC serán de acatamiento obligatorio para todos los usuarios de las tecnologías de información y comunicación de la Municipalidad de Zarceró.

CAPÍTULO VIII Administración de la Información Institucional

Artículo 30° — La información, documentos y software generados por los funcionarios en el ejercicio de sus funciones y mediante la utilización de los recursos institucionales, son propiedad intelectual y patrimonial de la Municipalidad de Zarceró. El autor conservará el derecho moral que la ley le confiere.

Artículo 31° — La información institucional es un activo valioso y su uso es discrecional para el usuario exclusivamente para fines laborales. Queda estrictamente prohibido permitir o propiciar

el acceso de personas no autorizadas o ajenas a la Institución a dicha información. Cualquier persona externa que requiera acceso a información institucional deberá contar con el permiso expreso de la Alcaldía Municipal o de la Jefatura del Departamento titular de la información, especificando el tipo de información requerida, la justificación y la finalidad de dicho acceso, y siempre bajo los mecanismos de seguridad y registro establecidos por el DTIC.

Artículo 32° — El daño, alteración, destrucción o pérdida intencional de la información institucional, ya sea almacenada en servidores de red, en la nube, en equipos locales o en cualquier otro medio de la Institución, será notificada de inmediato al Alcalde Municipal y a la Jefatura del Departamento del usuario involucrado. Esta acción dará lugar al inicio del procedimiento disciplinario correspondiente para determinar las responsabilidades del caso. Así mismo, la Institución se reserva el derecho de acudir a las instancias judiciales que correspondan para denunciar la intrusión, manipulación o destrucción de información institucional por parte de funcionarios o terceros.

CAPÍTULO X

Del control de cumplimiento

Artículo 33° — Todos los usuarios de la Municipalidad de Zarceró tienen la obligación de conocer el presente Reglamento para el Uso de los Recursos Tecnológicos de Información y Comunicación de la Municipalidad de Zarceró, y regir su actuar por los principios y disposiciones consignados en él. El DTIC deberá asegurar la divulgación y la disponibilidad de este documento para consulta.

Artículo 34° — Toda Jefatura o Dirección es responsable de supervisar y controlar el uso adecuado de los recursos tecnológicos dentro de sus departamentos, e implementar los controles operativos necesarios para garantizar el cumplimiento de este reglamento por parte de su personal a cargo, así como el cuidado de los equipos de cómputo y dispositivos asignados a sus dependencias.

Artículo 35° — Cualquier infracción a este Reglamento o el uso inadecuado de los recursos tecnológicos a los que se refiere, autoriza al jefe inmediato del funcionario a llamarle la atención de forma verbal o escrita y conminarle a corregir el comportamiento. Si la infracción se repitiere o si la gravedad del hecho lo amerita desde el primer momento, el jefe inmediato deberá informar por escrito a la Dirección respectiva y a la Asesoría Legal (si aplica), con copia al Departamento de Tecnologías de Información y Comunicación, a fin de que se inicie el respectivo procedimiento disciplinario contra el funcionario responsable, conforme a la normativa vigente.

Artículo 36° — El Departamento de Tecnologías de Información y Comunicación será el ente técnico contralor y supervisor de la administración y el uso de los recursos informáticos y de

comunicación en la Municipalidad de Zarcero, y brindará el soporte técnico necesario para la aplicación de este reglamento.

Artículo 37°— Las faltas cometidas al tenor de lo dispuesto en el presente reglamento serán sancionadas de conformidad con las disposiciones establecidas en el Código de Trabajo y el Reglamento Interno de Trabajo de la Municipalidad de Zarcero, así como las demás disposiciones legales y reglamentarias vigentes y aplicables, sin perjuicio de las responsabilidades civiles, administrativas o penales que deba asumir el infractor.

Artículo 38° — Rige a partir de su publicación.