

**APRUEBA REGLAMENTO MUNICIPAL SOBRE USO
DE RECURSOS TECNOLÓGICOS DE LA ILUSTRE
MUNICIPALIDAD DE SANTO DOMINGO.**

DECRETO ALCALDICIO N° 0 0141

SANTO DOMINGO, A

29 ENE 2019

VISTO:

1. Lo dispuesto en el artículo 12 del D.F.L. N° 1, de fecha 26 de julio de 2006, del Ministerio del Interior, que Fija el Texto Refundido, Coordinado y Sistematizado de la ley N° 18.695, Orgánica Constitucional de Municipalidades.
2. El REGLAMENTO MUNICIPAL SOBRE USO DE RECURSOS TECNOLÓGICOS DE LA ILUSTRE MUNICIPALIDAD DE SANTO DOMINGO.
3. El decreto alcaldicio N° 1.861, de fecha 28 de diciembre de 2018, que Aprueba Presupuesto del Área Municipal, correspondiente al año 2019, en la I. Municipalidad de Santo Domingo, y sus modificaciones posteriores.

CONSIDERANDO:

1. Que, la Ilustre Municipalidad de Santo Domingo ha detectado la necesidad de avanzar y mejorar en materias relacionadas a tecnologías de información y comunicación (TIC), en beneficio de la gestión municipal y de los ciudadanos y contribuyentes que usan los servicios tecnológicos de la I. Municipalidad de Santo Domingo.

TENIENDO PRESENTE:

1. El numeral 37°) de la Sentencia de Proclamación de Alcaldes de la Quinta Región, de fecha 1 de diciembre de 2016, dictada por el Tribunal Electoral Regional de Valparaíso, Rol N° 2467-2016; y el decreto alcaldicio-SIAPER N° 538, de fecha 6 de diciembre de 2016, por el cual asumen funciones Alcalde y Concejales, en calidad de titular, de la Ilustre Municipalidad de Santo Domingo, por el período 2016-2020.
2. Las facultades previstas en los artículos 56, 63 y 65 del D.F.L. N° 1, de fecha 26 de julio de 2006, del Ministerio del Interior, que Fija el Texto Refundido, Coordinado y Sistematizado de la ley N° 18.695, Orgánica Constitucional de Municipalidades.

DECRETO:

1. APRUÉBASE el siguiente REGLAMENTO MUNICIPAL SOBRE USO DE RECURSOS TECNOLÓGICOS DE LA ILUSTRE MUNICIPALIDAD DE SANTO DOMINGO:

**REGLAMENTO MUNICIPAL SOBRE USO DE RECURSOS
TECNOLÓGICOS DE LA ILUSTRE MUNICIPALIDAD DE SANTO
DOMINGO**

OBJETIVO

El propósito de este reglamento es establecer las directrices e instrucciones respecto al uso responsable de los recursos y servicios tecnológicos que la Ilustre Municipalidad de Santo Domingo entrega y provee a sus usuarios. Su cumplimiento será supervisado por el Departamento de Informática y Gobierno Electrónico (DIGE).

Se entiende por uso responsable el cumplimiento por parte de los usuarios de las normas legales, políticas y reglamentos municipales, procedimientos y buenas prácticas, que permitan a la Municipalidad resguardar su información y utilizar eficientemente sus recursos y servicios tecnológicos.

ALCANCE

El presente reglamento se aplicará a todos los funcionarios de planta y contrata de la Municipalidad y sus departamentos, cualquiera sea su jerarquía, escalafón o estamento, al personal contratado a honorarios y bajo programas, a personal de empresas externas y en general a cualquiera que tenga acceso o utilice los recursos y servicios tecnológicos del municipio. En adelante se utilizará el término "usuario" para identificar a este conjunto de personas.

Además, el reglamento aplicará para todas las dependencias, equipamientos, sistemas informáticos y plataformas tecnológicas municipales, sean éstas propias o provistas por terceros.

DISPOSICIONES GENERALES

El presente reglamento utiliza como marco de referencia las siguientes normas técnicas y estándares:

- La Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, dispuestas en el Decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia.
- La Norma Técnica para la adopción de medidas destinadas a minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos del Estado y en las asignadas a sus funcionarios, dispuestas en el Decreto N° 93, de 2006, del Ministerio Secretaría General de la Presidencia.
- La Norma Técnica descrita en el Decreto 14, de 2014, del Ministerio de Economía, Fomento y Turismo, en lo relativo sitios electrónicos y plataformas web abiertas.
- La Norma Chilena NCh-ISO 27002 Of 2009 basada en el estándar ISO/IEC 27002 sobre Sistemas de Gestión de Seguridad de la Información.

La supervisión de este reglamento estará a cargo del Departamento de Informática y Gobierno Electrónico.

Los usuarios son los responsables finales por el cuidado de los recursos que les hayan sido asignados y de la información municipal que manejen. El no cumplimiento de este reglamento o la detección de conductas negligentes o malintencionadas que deriven en un deterioro, daño o pérdida de los bienes y recursos asignados por el municipio o de la información municipal que contienen dará origen a una investigación sumaria o sumario administrativo, acciones disciplinarias o legales según corresponda.

Los casos no previstos en el presente reglamento serán analizados por el Departamento de Informática y Gobierno Electrónico y el Administrador Municipal para decidir las acciones a seguir.

El reglamento deberá ser conocido por todos los funcionarios y el personal que haga uso de los recursos y servicios tecnológicos provistos por la Ilustre Municipalidad de Santo Domingo. La

aprobación del presente reglamento mediante decreto alcaldicio y su debida comunicación, hará que se presuma conocido por todos, no pudiendo alegarse desconocimiento del mismo.

1. ACERCA DE LA ASIGNACIÓN DE ESTACIONES DE TRABAJO Y CUENTAS DE USUARIO

La institución, a través del Departamento de Informática y Gobierno Electrónico, cumplirá con:

1.1. Asignación de estaciones de trabajo y cuentas de usuario

Se asignará a cada funcionario el equipamiento necesario para el cumplimiento de sus labores, de acuerdo a su función efectiva, comunicada por el Departamento de Personal al momento de su incorporación, teniendo en consideración la factibilidad técnica. Así mismo, se asignará una cuenta de correo institucional y cuentas de acceso a los sistemas de información municipales según corresponda.

De acuerdo a la disponibilidad presupuestaria, se definirá el equipamiento estándar para cada función efectiva. En caso de circunstancias excepcionales, como problemas médicos debidamente justificados o por necesidades adicionales a las labores propias de la función, la jefatura podrá solicitar requerimientos especiales al DIGE, el que analizará la factibilidad de dicha solicitud.

1.2. Devolución de estaciones de trabajo

Cuando un funcionario por cualquier motivo deje de pertenecer a la institución, deberá entregar el equipamiento a su cargo directamente al DIGE que le entregará un comprobante de dicha devolución. Además, se suspenderán sus cuentas de usuario al momento del cese correspondiente. Por razones de seguridad, la suspensión de los servicios podrá ser previa a la total tramitación del cese.

Respecto de funcionarios que realicen labores directivas y/o críticas el DIGE podrá realizar un respaldo de su información.

1.3. Renovación de Equipos

Los equipos computacionales serán renovados de acuerdo a los siguientes criterios:

- Obsolescencia tecnológica o cumplimiento de la vida útil del equipo.
- Costos de reparación superior al 40% del valor del equipo.
- Requerimientos adicionales sea por labores críticas realizadas por el funcionario o por situaciones de fuerza mayor, pérdida, hurto o robo.

2. ACERCA DEL CUIDADO DE LOS RECURSOS COMPUTACIONALES

2.1. SEGURIDAD FISICA

Los recursos físicos computacionales son elementos delicados y de alto costo que deben ser tratados con el cuidado necesario por parte de los funcionarios.

2.1.1. Cuidado de equipos institucionales

El cuidado básico de los equipos computacionales y dispositivos asignados a un funcionario es de su responsabilidad. Se debe resguardar en todo momento para que estos no sean dañados, evitando golpes, caídas, temperaturas extremas y derrames de líquidos.

En caso de ocurrir un incidente que afecte a dichos equipos debe reportar formalmente a su jefatura directa y al DIGE de manera inmediata.

En el caso de los equipos portátiles, dispositivos móviles, o bien equipos aquellos estacionarios asignados para su uso dentro o fuera de las dependencias municipales, este cuidado debe extenderse consecuentemente.

2.1.2. Seguridad de acceso físico a las dependencias municipales

Será responsabilidad de la IMSD establecer las medidas de control del acceso a las dependencias de la institución. En todo caso y sin perjuicio de estos controles regulares dispuestos para el control de acceso los funcionarios deben procurar mantener sus equipos con el resguardo adecuado para evitar accesos no autorizados.

2.1.3. Seguridad para evitar hurto o robo

Se deben mantener las medidas prácticas de seguridad para evitar hurtos o robos de los recursos computacionales municipales, especialmente en los casos de equipos portátiles y de telefonía, como por ejemplo notebooks, impresoras, celulares, memorias externas, dispositivos de comunicaciones y otros.

En caso de hurto o robo el funcionario debe reportar inmediatamente a su jefatura directa y al DIGE, adjuntando la constancia en Carabineros para establecer las acciones pertinentes.

2.1.4. Uso Cable candado o similar

En los casos en que los notebooks estén provistos de cables de seguridad, es responsabilidad del funcionario instalar el cable y candado para evitar hurtos o robos. En caso de traslado, no debe dejarlo al interior de vehículos, incluyendo la maleta u otros compartimentos del mismo, ya que puede ser hurtado, robado o dañado por exceso de temperatura.

2.1.5. Otros medios de Seguridad Física

El DIGE será responsable de poner a disposición de los funcionarios cualquier otro medio de seguridad física que la institución incorpore, informando acerca de su uso correcto.

2.2. SEGURIDAD DE LA INFORMACIÓN

Los equipos computacionales, las aplicaciones y sistemas municipales manejan información, que en algunos casos es reservada y/o sensible, por lo que es responsabilidad del funcionario que tiene autorización para accederla, mantener un nivel de seguridad adecuado para su resguardo.

2.2.1. Cuentas de Usuario

Tanto los computadores como los sistemas de información municipales disponen de sistemas de seguridad y control de acceso basado en la asignación de una "Cuenta de Usuario", la que tiene asociada una "Contraseña" de uso individual e intransferible.

La cuenta de usuario corresponde al nombre que identifica de manera única a un usuario en un sistema y es asignado exclusivamente por el DIGE.

La contraseña corresponde a un conjunto de caracteres, compuesto por números, letras o símbolos que tiene por objeto impedir el acceso no autorizado al computador o al sistema.

La cuenta de usuario y su contraseña son de uso individual e intransferible y no deben entregarse a ninguna persona. La contraseña es secreta.

Para el manejo de contraseñas se deben considerar a lo menos las siguientes medidas de seguridad y buenas prácticas:

- No crear contraseñas fáciles de adivinar, tales como nombres, fechas, lugares, el número directo de su anexo, número de Rut, etc.
- Cada cierto tiempo cambiar las contraseñas.
- No compartir las contraseñas.
- No registrar las contraseñas o claves en papel.
- Evitar configurar el navegador de internet para que recuerde su usuario y contraseña.
- Cambiar las contraseñas o claves cuando haya indicios de un posible compromiso de estas.
- Elegir contraseñas que tengan una longitud mínima de ocho caracteres.
- Evitar reutilizar contraseñas antiguas.
- Cambiar la contraseña temporal al iniciar la primera sesión.
- Configurar el tiempo de cierre de la sesión automática cuando sea posible.

Los funcionarios no deben intentar acceder a sistemas o estaciones de trabajo a los que no han sido expresamente autorizados. Esta acción puede suponer intento de accesos maliciosos o suplantación de identidad.

En caso que un funcionario presuma que la contraseña de su cuenta de usuario esté comprometida, deberá informar inmediatamente al DIGE para coordinar su restauración.

El DIGE podrá gestionar cambios periódicos de contraseñas obligatorios y será responsable de la implementación y administración de cualquier otro medio de autenticación que la institución incorpore.

2.2.2. Información de Trabajo de los Usuarios

La información es uno de los activos de valor estratégico en la institución. Los funcionarios deben adoptar medidas de seguridad para resguardar la información que esté almacenada en sus computadores y sistemas de información, para lo cual:

- a) Para el trabajo diario se deben utilizar los sistemas de información designados por la institución, de acuerdo a los roles y/o perfiles asignados al funcionario.
- b) El funcionario debe priorizar el almacenamiento de la información en su computador y su ingreso en los sistemas municipales, evitando en la medida de lo posible mantener la información o archivos en medios distintos, como pendrives y discos duros externos.
- c) Para el trabajo diario se debe utilizar sólo el software provisto y autorizado por la institución a través del DIGE.
- d) Los usuarios deberán abstenerse de ingresar, almacenar y/o manipular archivos que pudieran tratar contenido ilegal, pornográfico, insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista y en general todos aquellos que sean ajenos a las funciones que les correspondan.
- e) Es responsabilidad del funcionario que tiene la autorización correspondiente mantener a buen recaudo las aplicaciones y sistemas municipales que manejan información reservada y/o sensible.
- f) Es responsabilidad del funcionario respaldar la información de trabajo residente en los computadores a su cargo. Así mismo el funcionario podrá solicitar al DIGE realizar un respaldo de esta información en caso que lo requiera.

- g) Para aquellos funcionarios que determine la administración, el DIGE implementará un disco virtual donde podrán almacenar los archivos institucionales que no se encuentran en los sistemas de información y sean considerados como críticos.
- h) El funcionario debe conectar su computador a la red municipal en forma periódica, a lo menos cada 15 días, para los efectos de actualizar el software y servicios de uso general tales como antivirus, sistema operativo y políticas de dominio.

2.2.3. Información de los Sistemas de Gestión y Bases de Datos Municipales

La información que se almacena en las bases de datos, producto de la utilización de los sistemas de información, servicios digitales y plataformas municipales, es uno de los activos de valor estratégico en la institución, por lo tanto la IMSD deberá velar por el correcto uso y precauciones de seguridad de ésta.

El DIGE será responsable del respaldo de los datos de los sistemas de información, servicios digitales y plataformas municipales. El mecanismo y periodicidad de estos respaldos serán establecidos a través de los procedimientos correspondientes.

El DIGE implementará mecanismos de control de acceso y monitoreo de los sistemas de información, servicios digitales y plataformas municipales que corresponda.

3. USO DE LOS SERVICIOS TECNOLÓGICOS MUNICIPALES

La plataforma tecnológica de la IMSD está compuesta de los elementos de hardware, software y comunicaciones necesarias para la prestación de los servicios de tecnologías de información a la institución.

3.1. RED INSTITUCIONAL

La red de datos y la infraestructura de comunicaciones municipales son recursos compartidos y limitados. Los usuarios contarán con un acceso controlado a la red de datos municipal que les permitirá trabajar con recursos compartidos, tales como carpetas, aplicativos e impresoras, así como también navegar por Internet.

Preferentemente, la conexión a la red de datos municipal será a través de la red cableada cuando el computador del usuario sea fijo, o a través de la red inalámbrica cuando el computador sea portátil.

La conexión de teléfonos celulares a la red de datos municipal no está permitida.

Según sea el caso, los usuarios contarán con una cuenta de usuario para acceder al Dominio Windows en sus computadores. El Dominio Windows es un mecanismo para organizar a los usuarios de la red, que permite administrar la seguridad en forma centralizada.

La creación de cuentas de usuario de dominio y configuración del acceso a la red de datos municipal en los equipos de los usuarios será realizada solamente por personal técnico del DIGE. Esto también incluye a los usuarios que accedan a la red a través de conexión inalámbrica.

Una vez ingresado a la red de datos municipal el usuario es responsable por su uso, el cual debe enmarcarse dentro de sus funciones. Así mismo es responsable por el uso de los servicios y sistemas disponibles a través de la red y del contenido de las comunicaciones realizadas.

Los usuarios tienen prohibido manipular la configuración de la red, excepto bajo la supervisión del personal técnico autorizado.

El DIGE se encargará de administrar la seguridad en la red de datos municipal a través de la implementación de un Firewall y de otros dispositivos para enrutamiento y filtrado de tráfico. El DIGE se encargará de implementar los sistemas para monitorear la disponibilidad de los enlaces de comunicación, los accesos y la navegación en Internet.

Está prohibido interrumpir o interceptar las comunicaciones de la red, acceder a recursos e información a los cuales no han sido autorizados y ejecutar programas o herramientas que vulneren o comprometan la seguridad de la red municipal, de los sistemas o de la información. Se suspenderá el acceso a la red al usuario que sea sorprendido realizando cualquiera de estas actividades, acto seguido se notificará a su jefatura directa y se realizarán los procedimientos administrativos que correspondan.

3.2. NAVEGACION EN INTERNET

La navegación en Internet es un servicio que la IMSD pone a disposición de sus usuarios para el desarrollo de sus funciones y en consecuencia debe ser usada solo para estos fines.

El DIGE, por iniciativa propia o a requerimiento fundado de los directivos o del Alcalde, podrá suspender el acceso a sitios que considere que afectan al desempeño de los usuarios, al buen funcionamiento de la red o si se considere son ajenos a las funciones institucionales.

Los usuarios deben informar al DIGE cuando consideren que algún sitio de internet deba ser bloqueado, quien evaluará la solicitud e implementará la medida si la estima procedente.

Así mismo, los usuarios deben informar al DIGE cuando no puedan acceder a algún sitio de Internet que esté bloqueado y que requieran para el desempeño de sus labores.

Los usuarios podrán tener distintos niveles de restricción sobre la navegación en Internet. Estos niveles se establecerán de acuerdo a su función, perfil de usuario o según solicitud fundada.

Los usuarios deberán abstenerse de visitar sitios o descargar archivos que pudieran tratar contenido ilegal, pornográfico, insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista o participar en sitios relacionados con las materias señaladas y en general aquellos que sean ajenos a las funciones que les correspondan.

EL DIGE podrá suspender el acceso a la red al usuario que sea sorprendido realizando cualquiera de las actividades señaladas en el párrafo anterior, acto seguido se notificará a su jefatura directa y se realizarán los procedimientos administrativos que correspondan.

3.3. CORREO ELECTRÓNICO

La plataforma de correo electrónico institucional es un servicio que funciona a través de internet, puede ser accedida por medio de un navegador o de un teléfono inteligente. Permite a los usuarios enviar y recibir mensajes por medio de una "casilla de correo", que está asociada a una dirección única compuesta por un identificador del usuario seguido de "@santodomingo.cl". Cada casilla posee un espacio de almacenamiento limitado y funciones que permiten su utilización y mantenimiento. El conjunto de estos elementos se denomina "cuenta de correo electrónico".

La creación, entrega y eliminación de cuentas de correo será responsabilidad del DIGE, según el procedimiento establecido para estos fines. La asignación de cuentas de correo será bajo los criterios indicados en el mismo procedimiento. La solicitud de cuenta de correo para un usuario será iniciada por el Departamento de Personal al momento de su incorporación a la institución.

Los usuarios deben hacer una adecuada y responsable utilización de su cuenta de correo para el cumplimiento de sus funciones. El DIGE deberá monitorear e informar sobre el funcionamiento general de la plataforma de correo electrónico institucional.

El usuario es responsable de los contenidos y mantenimiento del espacio de su cuenta de correo. El DIGE será responsable de advertir al usuario cuando su espacio de datos esté próximo a agotarse, prestando la ayuda técnica para que el usuario pueda respaldar y vaciar su cuenta de correo.

El DIGE podrá realizar respaldos del correo electrónico a petición de un usuario, o realizar respaldos programados para usuarios definidos como críticos por parte de la Dirección.

El usuario deberá usar un lenguaje adecuado y respetuoso en sus mensajes, evitando contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.

Está prohibido enviar o reproducir cadenas de mensajes, promociones comerciales o mensajes de uso comercial.

El usuario deberá abstenerse de enviar mensajes masivos ya sea al interior de la IMSD o hacia el exterior. En caso de ser requerido, se deberá contar con la autorización de la jefatura y siempre con fines institucionales.

El usuario deberá tener especial precaución de abrir correos electrónicos cuya procedencia sea desconocida o sospechosa, que pueda contener adjuntos programas o documentos con contenido ejecutable, dado que pueden ser archivos que contienen virus. Cuando el usuario se encuentre con un correo de estas características deberá informar inmediatamente al DIGE.

En caso de pérdida de contraseña o ante la sospecha de que su cuenta de correo se encuentra comprometida, el usuario deberá comunicar inmediatamente al DIGE, que realizará una revisión y luego procederá a restaurar la contraseña.

En caso de cese de funciones de un usuario, el DIGE suspenderá la cuenta de correo electrónico asociada. Por razones de seguridad, la suspensión de la cuenta de correo podrá ser previa a la total tramitación del cese.

Previa orden judicial o requerimiento del Ministerio Público, la IMSD podrá entregar información acerca del contenido de los correos electrónicos.

4. LICENCIAS DE SOFTWARE Y PROPIEDAD INTELECTUAL

En la Ilustre Municipalidad de Santo Domingo está prohibido utilizar software que infrinja la normativa vigente o la ley de propiedad intelectual. La instalación de software sin la correspondiente licencia que autoriza su uso, compromete la responsabilidad del usuario.

El DIGE podrá suspender el acceso a la red al usuario que sea sorprendido utilizando software ilegal, acto seguido se notificará a su jefatura directa y se realizarán los procedimientos administrativos que correspondan.

Para mayor comprensión, deben considerarse los siguientes alcances:

a) Software no autorizado

Para prevenir infracciones a la normativa vigente y la potencial introducción de programas maliciosos que propicien riesgos o amenaza para la red de datos o la información municipal, los usuarios no están autorizados a instalar software por cuenta propia. Toda solicitud de instalación deberá ser autorizada por el DIGE.

b) Programas P2P o de intercambio de archivos

Este tipo de programas está prohibido ya que representan un riesgo de seguridad, proveen de copias ilegales de material protegido y consumen gran ancho de banda de la red de datos municipal, ralentizando o interrumpiendo el servicio de navegación en Internet y perjudicando el desempeño de los servicios y de las funciones de otros usuarios.

c) Otros materiales protegidos por propiedad intelectual o derechos de autor.

Cualquier otro material protegido, como e-books, fotografías, música, videos o similares, no puede copiarse ilegalmente ni mantenerse en los recursos tecnológicos de la IMSD.

d) Software autorizado

En el caso de software libre, "open source", en demo temporal, o de propiedad del usuario, de carácter legal, su instalación deberá ser informada y autorizada por el DIGE, el que podrá denegar su instalación atendiendo a las prevenciones de riesgos indicadas. Lo mismo regirá para la



instalación de drivers y software asociado a dispositivos externos, como grabadores de CD/DVD, escáneres, cámaras digitales y otros.



ENTRADA EN VIGENCIA

El presente Reglamento en entrará en vigencia a partir de su aprobación, mediante decreto alcaldicio.

2. **COMUNÍQUESE**, el presente decreto alcaldicio, todos los funcionarios y servidores públicos de la Ilustre Municipalidad de Santo Domingo.

Anótese, comuníquese, publíquese y archívese.



RENZZO ROJAS TRONCOSO
Secretario Municipal
I. Municipalidad de Santo Domingo



FERNANDO RODRÍGUEZ LARRAÍN
Alcalde
I. Municipalidad de Santo Domingo

FRL / RRT / DRC / KBV / JJA / 

DISTRIBUCIÓN:

- Secretaría Municipal / Unidad de Archivo Municipal (1).
- Dirección de Administración y Finanzas (DAF) / Departamento de Informática y Gobierno Electrónico (1).
- Todos los funcionarios y servidores públicos de la Ilustre Municipalidad de Santo Domingo (1), (copia digital).