

RESOLUCIÓN DE GERENCIA GENERAL N° 15 -2020-EMMSA

Santa Anita, 06 de marzo de 2020.

VISTOS:

El Informe N° 033-SGI-EMMSA-2019, de fecha 11 de setiembre de 2019, emitido por la Subgerencia de Informática; el Informe N° 06-2020-GPPE-SGPL-EMMSA, de fecha 24 de febrero de 2020, emitido por la Subgerencia de Planeamiento, el Memorando N° 045-2020-GPPE-EMMSA, emitido por la Gerencia de Planeamiento, Presupuesto y Estadística y el Informe N° 045-GAL-EMMSA-2020, de fecha 05 de marzo del 2020, emitido por la Gerencia de Asesoría Legal;

CONSIDERANDO:

Que, la Empresa Municipal de Mercados SA – EMMSA, es una empresa municipal de derecho privado, formado bajo la modalidad de Sociedad Anónima, que tiene por objeto administrar, controlar, supervisar y dirigir los mercados mayorista existentes en la provincia de Lima y cuyas acciones y patrimonios son propiedad de la Municipalidad Metropolitana de Lima, gozando de autonomía económica y administrativa;

Que, de conformidad con lo dispuesto por el artículo I, numeral 8, del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, EMMSA es una «entidad de la Administración Pública», en tanto que es una persona jurídica bajo el régimen privado que presta un servicio público por delegación de la Municipalidad Metropolitana de Lima; realizando la actividad de operación de mercado mayorista, calificada como servicio público prioritario, de acuerdo a lo dispuesto por al artículo 4° de la Ley N° 28026, Ley del Sistema de Mercados Mayoristas de Alimentos.

Que, mediante el Decreto Legislativo N° 1412 que aprueba la "Ley de Gobierno Digital" se establece el marco legal que regula la adecuada gestión de la identidad digital, servicios digitales, seguridad digital, arquitectura digital, interoperabilidad y datos, así como el régimen jurídico para el uso de las tecnologías digitales, siendo aplicables de acuerdo a su artículo 2, a todas las entidades que forman parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General;

Que, a través del literal g) del artículo 5 del Decreto Supremo N° 013-2003-PCM, el mismo que fue incluido por el artículo 2 del Decreto Supremo N° 076-201-PCM, se dispuso que las entidades deben elaborar las directivas internas que establezcan el perfil de los tipos de usuarios de acuerdo al uso que estos darán a las herramientas informáticas (sistema operativo y herramienta de ofimática);

Que, por medio de la Resolución Ministerial N° 004-2016-PCM se aprobó el uso obligatorio de las Normas Técnica Peruana "NTP-ISO/IEC 27001:2014 - Tecnología de la Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información. Requisitos 2ª Edición", para todas las entidades integrantes del Sistema Nacional de Informática;



Que, mediante Resolución de Gerencia General N° 028-GG-EMMSA-2017, de fecha 20 de abril de 2017, se aprobó el documento denominado Directiva N° 002-2017-GG-EMMSA sobre el "Uso de Equipos, Software y Servicios Informáticos en la Empresa Municipal de Mercados S.A. – EMMSA", asimismo se aprobó la Directiva N° 003-2017-GG-EMMSA sobre "Guía para la Administración de Software en la Empresa Municipal de Mercados S.A. – EMMSA", dicha normativa interna deberá ser actualizada adecuándose al cuerpo legal antes previsto, los mismos que brindarán el soporte necesario respecto a temas informáticos de la entidad;



Que, en ese sentido la Subgerencia de Informática mediante el documento del visto, propone a la Gerencia de Administración y Finanzas, la actualización de los documentos normativos internos precitados, en cumplimiento a la reformulación realizada al Plan Operativo Institucional – III Trimestre 2019;



Que, la Subgerencia de Planeamiento mediante el documento del visto, en coordinación con la Gerencia de Administración y Finanzas a través de la Subgerencia de Informática, formula los siguientes proyectos de documentos normativos: i) Directiva DI-012-GAF/009 "Uso de Equipos, Software y Servicios Informáticos en EMMSA", primera versión y la ii) Directiva DI-013-GAF/010 "Administración de Software en EMMSA", primera versión, señalando que los mismos cumple con lo estipulado en la Directiva DI-001-GPPE/001- "Formulación de los Documentos Normativos de EMMSA", primera versión.

Que, en virtud de ello la Gerencia de Asesoría Legal, mediante el documento del visto emite opinión legal con relación a los documentos normativos formulados, señalando que los mismos presentan la consistencia legal pertinente y recomienda su aprobación;

Que, de acuerdo a lo expuesto anteriormente resulta pertinente emitir el acto administrativo que corresponde;



Contando con las visaciones de la Gerencia de Administración y Finanzas, la Gerencia de Gerencia de Planeamiento, Presupuesto y Estadística, la Gerencia de Asesoría Legal y la Subgerencia de Informática, en el marco de sus respectivas competencias funcionales; y en uso de las facultades conferidas a la Gerencia General de la Empresa Municipal de Mercados S.A.-EMMSA, en el artículo 15, numeral 14) del Reglamento de Organización y Funciones de EMMSA aprobado mediante acuerdo Directorio N° 039-2015;



SE RESUELVE:

ARTÍCULO PRIMERO.- DEJAR SIN EFECTO la Resolución de Gerencia General N° 028-GG-EMMSA-2017, de fecha 20 de abril de 2017, que aprobó la Directiva N° 002-2017-GG-EMMSA sobre el "Uso de Equipos, Software y Servicios Informáticos en la Empresa Municipal de Mercados S.A. – EMMSA", así como también aprobó la Directiva N° 003-2017-GG-EMMSA sobre "Guía para la Administración de Software en la Empresa Municipal de Mercados S.A. – EMMSA".

ARTÍCULO SEGUNDO.- APROBAR la Directiva DI-012-GAF/009 "USO DE EQUIPOS, SOFTWARE Y SERVICIOS INFORMATICOS DE EMMSA", primera versión; así como también la Directiva DI-013-GAF/010 "ADMINISTRACIÓN DE SOFTWARE EN EMMSA", primera versión, las mismas que forman parte integrante de la presente Resolución.





EMMSA
Empresa Municipal
de Mercados S.A.

ARTÍCULO TERCERO.- ENCARGAR a la Gerencia de Planeamiento, Presupuesto y Estadística, publicar la presente Resolución de Gerencia General en el Portal Institucional de la Empresa Municipal de Mercados S.A: (www.emmsa.com.pe) y la difusión del documento normativo aprobado.

Regístrese, comuníquese y cúmplase.



EMPRESA MUNICIPAL DE MERCADOS S.A.


.....
JAIMÉ ADEMIR GALLEGOS RONDON
GERENTE GENERAL



EMMSA

Av. La Cultura N° 808, Santa Anita, Lima - Perú

Tel. 518-2800

www.emmsa.com.pe



MUNICIPALIDAD DE
LIMA

Directiva

USO DE EQUIPOS, SOFTWARE Y SERVICIOS INFORMÁTICOS DE EMMSA

Resolución de Gerencia General N° 15 -GG-EMMSA-2020



CÓDIGO: DI-012-GAF/009

Fecha de Aprobación:

Páginas: 1/21

Primera Versión

ÍNDICE

- 
- 
- 
- 
- 
- 
- I. OBJETIVO
 - II. ALCANCE
 - III. BASE LEGAL
 - IV. GLOSARIO DE TÉRMINOS
 - V. RESPONSABILIDADES
 - VI. DISPOSICIONES GENERALES
 - VII. DISPOSICIONES ESPECÍFICAS
 - VIII. DISPOSICIONES COMPLEMENTARIAS
 - IX. VIGENCIA
 - X. APROBACIÓN
 - XI. ANEXOS:
 - ANEXO N° 01: ACTA DE COMPROMISO DE CUMPLIMIENTO DE LAS NORMAS PARA EL USO DE RECURSOS Y SISTEMAS INFORMÁTICOS EN LA EMPRESA MUNICIPAL DE MERCADOS S.A.
 - ANEXO N° 02: CONDICIONES DE USO DE LOS SERVICIOS INFORMÁTICOS.
 - ANEXO N° 03: FORMULARIO SOLICITUD DE CUENTA DE USUARIOS Y ACCESOS.
 - ANEXO N° 04: RECOMENDACIONES Y BUENAS PRÁCTICAS SOBRE EL USO DE EQUIPOS, SOFTWARE Y SERVICIOS INFORMÁTICOS.

I. OBJETIVO

Establecer los lineamientos específicos para el adecuado uso de las herramientas informáticas como son equipos de cómputo, uso de software, correo electrónico y acceso al servicio de Internet en EMMSA.

II. ALCANCE

Esta Directiva es administrada por la Gerencia de Administración y Finanzas a través de la Subgerencia de Informática y es de aplicación obligatoria para todos los órganos y unidades orgánicas que conforman EMMSA.



III. BASE LEGAL

3.1 **Ley N° 28716**, aprueba Ley de Control Interno de Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.

3.2 **Ley N° 30171**, aprueba la Ley de Delitos Informáticos, del 17 de febrero del 2014.

3.3 **Decreto Legislativo N° 1412**, aprueba la ley de Gobierno Digital, del 13 de setiembre de 2018

3.4 **Resolución de Contraloría General N° 320-2006-CG**, aprueba las Normas de Control Interno, del 03 de noviembre de 2006.

3.5 **Resolución Ministerial N° 004-2016-PCM**, aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, 08 de enero de 2016.

3.6 **Resolución Jefatural - N° 088-2003-INEI** aprueba las "Normas para el uso del servicio de Correo Electrónico en las entidades de la Administración Pública", del 03 de abril de 2003.

3.7 **Resolución Jefatural N°053-2003-INEI** aprueba la Directiva sobre "Norma Técnica para la implementación del Registro de Recursos Informáticos en las instituciones de la Administración Pública", del 19 de febrero de 2003.

3.8 **Resolución de Gerencia General N° 063-2019-EMMSA/GG**, aprueba la Directiva N° 001-GPPE/001, Formulación de los Documentos Normativos de EMMSA, del 13 de diciembre de 2019.

3.9 **Acuerdo de Directorio N° 039-2015**, aprueba el Reglamento de Organización de Funciones de EMMSA, del 28 de octubre de 2015.



IV. GLOSARIO DE TÉRMINOS

4.1 Ancho de Banda

Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un periodo de tiempo dado, la unidad de medida es Kilobits por segundo (Kbps).



4.2 Contraseña

Es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quienes no se les permite el acceso.

4.3 Correo Electrónico

Es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use.



4.4 Custodio

Es todo personal al cual se le ha asignado un recurso informático formalmente por documento, y que no necesariamente hace uso directo del mismo.

4.5 Dominio de Internet

Es una red de identificación (Ejemplo: @emmsa.com.pe) asociada a un grupo de dispositivos o equipos conectados a la red e Internet.



4.6 Estación de Trabajo

Equipo informático que se destina a una labor profesional, técnica o científica. Por lo general, una estación de trabajo se encuentra vinculada a otras computadoras y a un servidor. De este modo se facilita el hecho de trabajar en equipo, compartiendo recursos y datos.



4.7 Hardware

Son los dispositivos y componentes físicos del ordenador, es de decir, todo lo que se puede ver y tocar. Se clasifican en 2 tipos: la primera la que se encuentra dentro del CPU y la segunda la que se encuentra alrededor del CPU.



4.8 Internet

Es una red de redes que permite la interconexión descentralizada de las computadoras a través de un conjunto de protocolos TCP/IP, es de alcance mundial.



4.9 Licencia de Software:

Es un contrato entre el licenciante (autor de los derechos de distribuidor) y el licenciatario (usuario consumidor de los programa informáticos a ser utilizados).

4.10 Permisos Informáticos

Son los accesos que tiene todo usuario para acceder al sistema operativo o a los sistemas de información de acuerdo a las funciones que realiza o para el cual fue contratado, según sea el caso.



4.11 Programas

Es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora.

4.12 Recursos Informáticos

Incluye todo equipo informático (computadoras, laptops, servidores, impresoras, fotocopiadoras y periféricos) infraestructura de comunicaciones (módems, router, switch, access point, cableado de red), software (oficina, desarrollo, diseño, antivirus, etc.), servicios (Internet, Intranet, correo electrónico, sitio web).

4.13 Red Informática

Es un conjunto de dispositivos y equipos de comunicación conectados de manera que conformen un enlace entre ellos, la red informática está conformada por todos los recursos informáticos.



4.14 Servidor

Es un ordenador o equipo informático que esta al servicio de otros equipos y ordenadores, y que suministran a ellos todo tipo de información.

4.15 Sistema de Información

Viene a ser cualquier sistema informático o aplicación de software que sea administrado por la Subgerencia de Informática.



4.16 Sistema Operativo

Es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos de hardware y usuario.



4.17 Software

Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital, comprende un conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas en las computadoras.



4.18 Unidad Central de Procesos (CPU)

La unidad central de procesos (CPU), es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas, y procesa los datos. Suele estar integrada en un chip denominado microprocesador.

4.19 Usuario

Es todo personal nombrado, funcionarios, contratados o terceros que hacen uso de los recursos informáticos (hardware y software).



4.20 Virus Informático

Son programas que tienen por objeto alterar el funcionamiento de la computadora sin el permiso o el consentimiento del usuario. Los virus habitualmente reemplazan archivos ejecutables por otros infectados en el código de este. Los virus pueden destruir de manera intencionada, los datos almacenados en un ordenador.



V. RESPONSABILIDADES

- 5.1 La Gerencia de Administración y Finanzas a través de la Subgerencia de Informática, es responsable de velar por la correcta utilización de los

equipos y servicios informáticos, para tal efecto brindará charlas a los usuarios para su empleo adecuado.

- 5.2 Los Gerentes y Subgerentes se harán cargo de supervisar el correcto uso de los recursos y sistemas informáticos asignados a su personal.



- 5.3 Es responsabilidad del usuario que tenga asignado un equipo de cómputo, el controlar y verificar que todo hardware y software instalado en la PC a su cargo, sea el autorizado e instalado por la Subgerencia de Informática. Asimismo, las Gerencias y las Subgerencias son las únicas autorizadas a solicitar la instalación o desinstalación de un hardware o software específico a su personal.



- 5.4 Es responsabilidad del usuario contribuir con la protección de su información, evitando dejar abierto su acceso a la computadora mientras tenga una sesión de trabajo. En este caso lo adecuado es bloquear la pantalla mientras dure su ausencia.

VI. DISPOSICIONES GENERALES

- 6.1 Se considera a los equipos de cómputo de la empresa, sistemas operativos, software base y aplicativos, así como también a los servicios de correo electrónico e internet como herramientas informáticas proporcionadas a los diversos usuarios que laboran en EMMSA, a fin de que estos cumplan sus funciones diarias de manera efectiva y eficiente.



- 6.2 El Administrador de los Servicios Informáticos de la Subgerencia de Informática, tiene autoridad para controlar y negar el acceso a servicios WEB que interfiera con los derechos de otros usuarios, garantizando la correcta operatividad de los servicios en custodia.

- 6.3 El equipo de cómputo cuenta de correo electrónico y acceso a Internet, (dependiendo del perfil del usuario) y se hará en relación a la necesidad operativa de cada una de las áreas funcionales de la Empresa.



- 6.4 El servicio de correo electrónico institucional asignado, es una herramienta de intercambio y comunicación de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, con excepción de las que se remitan con fines institucionales. Todos los usuarios tienen derecho a la privacidad del correo electrónico siempre y cuando éste sea usado para fines de trabajo relacionado a las labores de EMMSA.



- 6.5 Las claves de acceso a todo tipo de sistema o servicio deberán ser estrictamente confidenciales y personales y serán de completa responsabilidad del usuario que las tiene asignadas.

- 6.6 El acceso a Internet es una facilidad proporcionada por la empresa a sus trabajadores a fin de obtener una diversidad de información relacionada a las labores que desarrollan o en actividades que benefician a la empresa.



- 6.7 Las autorizaciones sobre el uso de servicios informáticos para algún usuario será previa autorización expresa de su Gerencia o Subgerencia (Anexo N° 03).

- 6.8 Se deberá tomar conocimiento de las "Recomendaciones y Buenas Prácticas sobre el Uso de Equipos, software y servicios informáticos mencionados en el Anexo N° 04 de la presente Directiva.

VII. DISPOSICIONES ESPECÍFICAS

7.1. Sobre el Uso de Estaciones de Trabajo o Computador Personal



- 7.1.1 La asignación de un equipo de cómputo a un usuario se efectuará previo llenado del formato del Anexo N° 02 "Condiciones de Uso de los Servicios Informáticos" de la presente Directiva.

- 7.1.2 Cada usuario es responsable del equipo informático que le ha sido asignado y del software instalado en el mismo. En el caso de detectarse la presencia de software no legal en el computador del usuario, la Subgerencia de Informática procederá a emitir un Informe a la Gerencia de Administración y Finanzas, quién adoptará las medidas correspondientes.



- 7.1.3 El estándar de configuración base para las estaciones de trabajo en lo que respecta a hardware como en software es establecida por la Subgerencia de Informática, de acuerdo a los requerimientos del negocio y de los avances tecnológicos del mercado, tomando como base la definición de perfiles de usuarios señalado en la "Guía para la Administración de Software en la EMMSA".



- 7.1.4 Toda instalación de hardware y software la debe realizar sólo el personal de la Subgerencia de Informática llevando un estricto control del número de licencias adquiridas por producto.

- 7.1.5 Todo hardware y software no estándar debe ser solicitado por los responsables de área solicitante a la Subgerencia de Informática, especificando el motivo de tal requerimiento, para la evaluación de sus características y aprobación para trámite de compra correspondiente.



- 7.1.6 El requerir recursos de red por parte de los usuarios se efectuará mediante Unidades de Red pre instalado y configurado en cada equipo y para cada usuario y cuyo uso está sujeta a las claves de acceso asignadas a los mismos lo cual será solicitado por el responsable del área solicitante mediante el Anexo N° 03 "Formulario Solicitud de Cuenta de Usuario y Accesos" de la presente Directiva



- 7.1.7 Los trabajos de soporte a las estaciones de trabajo se realizarán en forma coordinada y a solicitud del usuario. Las actualizaciones masivas de software son autorizadas por la Subgerencia de Informática.



- 7.1.8 El encargado del computador será el único responsable de la clave de encendido de dicho equipo ya que la privacidad de la misma estará bajo su responsabilidad.

- 7.1.9 El responsable de un equipo de cómputo, evitará el uso de medios magnéticos de dudosa procedencia ya que estos pueden contener virus informáticos que dañen la operatividad del computador.

7.1.10 Se instalarán lectoras de CD a los equipos de cómputo de los trabajadores que por la naturaleza de su trabajo lo requieran, debiéndose evitar su uso indiscriminado para música y/o videos.

7.1.11 El responsable del equipo de cómputo, al finalizar sus labores, deberá apagarlo en forma adecuada: primero el sistema operativo, luego el computador y sus periféricos y por último el estabilizador. Asimismo, la Subgerencia de Informática verificará el funcionamiento de los procesos de ahorro de energía que poseen los equipos de cómputo garantizando así un uso racional del consumo de energía eléctrica en beneficio de la empresa.

7.1.12 Ante la presencia de fallas en los equipos de cómputo o en los programas, el responsable del computador deberá comunicar dicho inconveniente a la Subgerencia de Informática con el propósito de tomar las acciones pertinentes para la pronta solución a las mismas por los medios de comunicación ya conocidos (telefónico, web o correo). Su incumplimiento por parte del usuario y detección durante el proceso de Mantenimiento Preventivo no hará responsable a la Subgerencia de Informática de las fallas que dicho equipo pueda tener y los perjuicios técnicos y económicos en que se pueda incurrir para la reparación del mismo.

7.1.13 Es responsabilidad de quien utilice equipos de cómputo compartidos por varios usuarios, el comunicar a su Jefe inmediato sobre cualquier ausencia, desperfecto o deterioro en los mismos, a fin de determinar responsabilidades, toda vez que estos equipos son entregados a los usuarios como herramientas de trabajo para el cumplimiento de sus labores.

7.1.14 La asignación de estaciones de trabajo portátiles y/o proyectores multimedia está restringida a las usuarios o áreas que lo requieran por la naturaleza de sus funciones, es necesario la conformidad del responsable del área solicitante.

7.1.15 La Subgerencia de Informática mantendrá un registro detallado de los equipos informáticos (computadoras, impresoras, scanner, etc.) asignados a los usuarios que por sus funciones requieran de los mismos para el cumplimiento de sus labores en EMMSA.

7.1.16 Los equipos de cómputo, software y aplicaciones instalados en las diversas áreas, son usados únicamente por el usuario asignado o por el custodio de dichos equipos, respetando las políticas implementadas en este documento.

2.2 Sobre el Uso de Correo Electrónico

7.2.1 La administración del correo electrónico institucional estará a cargo de la Subgerencia de Informática de la EMMSA.

7.2.2 Todo usuario que utilice los servicios de correo electrónico institucional, está obligado a aplicar la presente política, su incumplimiento genera las responsabilidades y sanciones a que hubiera lugar.



- 7.2.3 El correo electrónico institucional es personal e intransferible ya que viene a ser un servicio de comunicación e intercambio de información institucional, mas no debe ser utilizada para otros fines.
- 7.2.4 Los usuarios de las cuentas de correo electrónico proporcionadas por EMMSA son responsables de todas las actividades que se realizan con las mismas.
- 7.2.5 El buen uso de correo electrónico, comprende lo siguiente:

Uso de contraseñas

- 7.2.5.1 La Subgerencia de Informática brindará al usuario, al momento de la creación o reinicio de una cuenta de correo electrónico, una contraseña temporal y el aplicativo de correo solicitará al mismo el ingreso de una nueva contraseña y su confirmación.
- 7.2.5.2 Es responsabilidad del usuario mantener la confidencialidad de su clave de acceso a la cuenta de correo, proporcionada por EMMSA.
- 7.2.5.3 Cuando el usuario deje de usar su computadora deberá cerrar el software de correo electrónico para evitar que otro usuario use su cuenta de correo.
- 7.2.5.4 La contraseña deberá tener como mínimo una longitud de 8 caracteres y se recomienda utilizar números y letras para mayor seguridad de la misma.

Lectura de correo

- 7.2.5.5 Los usuarios de las cuentas de correo electrónico institucional deberán leer frecuentemente sus mensajes, así como depurar permanentemente los mensajes innecesarios para mantener espacio disponible en su cuenta de correo.
- 7.2.5.6 Se recomienda no abrir correos electrónicos sospechosos, especialmente los que tienen archivos adjuntos aunque el remitente sea conocido, asimos tener especial cuidado con los correos electrónicos recibidos en otro idioma.
- 7.2.5.7 Al recibir un mensaje que se considere ofensivo o no deseado a su persona o cualquier otra persona deberá reenviar dicho mensaje al responsable de la Subgerencia de Informática con el fin de que se tomen las acciones respectivas, evitando borrarlo hasta que dichas acciones se haya tomado y evitando remitirlo a otra cuenta diferente.
- 7.2.5.8 Las cuentas de correos electrónicos de EMMSA serán solicitadas a la Subgerencia de Informática para su creación, mantenimiento o baja por el responsable de la Gerencia o Subgerencia solicitante, para ello se utilizará el Anexo N° 03 "Formulario Solicitud de Cuenta de Usuario y Accesos" de la presente Directiva.
- 7.2.5.9 Es responsabilidad del usuario depurar periódicamente su buzón de correo electrónico, con el fin de evitar acumular



información no necesaria. En el caso de los archivos de trabajo, que son enviados por correo electrónico (archivos adjuntos) éstos deberán ser guardados en los equipos del usuario como copia de respaldo permanente.

- 7.2.6 Es responsabilidad del usuario el uso racional de correo electrónico, evitando el envío y recepción de correos masivos, remitiendo y copiando el mensaje sólo a los destinatarios estrictamente necesarios.

7.3 Sobre el Uso del Servicio de Internet

- 7.3.1 El uso de Internet utilizando PC's, computadora portátil o dispositivos móviles en las redes de EMMSA es exclusivamente para fines de trabajo; la Subgerencia de Informática limitará el acceso a determinadas páginas que no tenga relación a los trabajos propios de cada usuario.
- 7.3.2 Los niveles de los usuarios para la navegación por Internet serán coordinados previamente con la Gerencia o Subgerencia respectiva, definiéndose el criterio por las necesidades de trabajo de cada usuario, para ello se utilizará el Anexo N° 03 "Formulario Solicitud de Cuenta de Usuario y Accesos" de la presente Directiva.
- 7.3.3 Se recomienda no descargar archivos de internet o aplicaciones de celulares en equipos móviles autorizados. Para el caso de archivos de páginas web conocidas, el usuario debe asegurarse que no contenga virus, para ello puede analizar los archivos mediante el software antivirus instalado en su equipo.
- 7.3.4 Al igual que los equipos de cómputo, el uso de internet en los equipos móviles es sólo para usuarios autorizado en la empresa, y este será controlado y supervisado por la Subgerencia de Informática, previo requerimiento del jefe del área solicitante.

7.4 Sobre la Prevención, Detección y Eliminación de Virus Informático

- 7.4.1 Cada equipo de cómputo contará con la instalación de una licencia del software antivirus adquirido por EMMSA.
- 7.4.2 El software antivirus se actualizará diariamente, vía un procedimiento automático configurado por la Subgerencia de Informática al momento de la instalación del mismo en la PC, siendo este totalmente transparente para el usuario; de no contar con dicho software el usuario comunicará inmediatamente a la Subgerencia de Informática para su instalación.
- 7.4.3 Se deberá evitar el uso de medios de almacenamiento externo (USB, discos, etc.) provenientes del exterior de EMMSA o que no garanticen su procedencia.
- 7.4.4 Si por razones de trabajo fuera necesario la utilización de un medio magnético u óptico venido del exterior, éste deberá necesariamente pasar por el software Antivirus adquirido por EMMSA e instalado en cada PC.



7.5 Sobre el Desarrollo de Sistemas

- 7.5.1 Todo proyecto de desarrollo de sistemas de información debe ser coordinado entre la Subgerencia de Informática y la Gerencia solicitante previo requerimiento escrito de la misma.
- 7.5.2 De ser necesario la Subgerencia de Informática elaborará las especificaciones técnicas para la adquisición de: software básico y aplicativo de sistemas de información, en coordinación con el área solicitante.
- 7.5.3 Las modificaciones y/o adiciones a los sistemas existentes, serán comunicadas por escrito por el área solicitante a la Subgerencia de Informática, indicando en forma detallada las especificaciones requeridas para su implementación.
- 7.5.4 Esta política se aplicará en concordancia con la Guía de Procedimientos "Requerimiento de Implementación y Mantenimiento de Sistemas Informáticos de EMMSA" la misma que será distribuida para su conocimiento a los diversos usuarios responsables de los sistemas de información y que se encuentra aprobado por la Gerencia General de EMMSA.



7.6 Sobre la Seguridad Informática

Para el Control de Accesos a Aplicativos

- 7.6.1 Los responsables de las Gerencias y/o Subgerencias de la empresa deben comunicar a la Subgerencia de Informática los módulos de los aplicativos a los que requiera tener acceso sus usuarios.
- 7.6.2 Los responsables o funcionarios de la empresa tienen la obligación de verificar los niveles de autorización de uso de los sistemas del personal a su cargo, de igual forma comunicarán a la Subgerencia de Informática los cambios requeridos para las acciones correspondientes.
- 7.6.3 Cuando un usuario deja de laborar para nuestra empresa o es cambiado de área o se le cambia la naturaleza de sus funciones y por lo tanto ya no requiere los accesos otorgados, el responsable del área, bajo responsabilidad funcional, informará este hecho a la Subgerencia de Informática dentro de las 24 horas subsiguientes a la ocurrencia, a fin de que se proceda a la baja del usuario y a la eliminación de sus niveles de acceso mediante el Anexo N° 03 "Formulario Solicitud de Cuenta de Usuario y Accesos" de la presente Directiva.



7.7 Prohibiciones

- 7.7.1 Cada usuario en general que tengan asignada una computadora o servicio informático, no deberá realizar, bajo responsabilidad, las siguientes prohibiciones:
- 7.7.1.1 Acceder a lugares que distribuyan material pornográfico, musical, sexista, político, religioso o discriminatorio de cualquier tipo, subversivo, ofensivo y que riñan contra la moral y las buenas costumbres.



- 7.7.1.2 La instalación de cualquier tipo de software que no haya sido previamente autorizado o proporcionado por la Subgerencia de Informática.
- 7.7.1.3 Hacer uso de Internet, para fines comerciales ajenos a la Empresa o que perjudiquen sus intereses. Así como de su uso para propósitos fraudulentos y publicitarios.
- 7.7.1.4 Ejecutar programas de origen desconocido (desde internet o de archivos adjuntos a correos electrónicos), bajo responsabilidad del usuario final.
- 7.7.1.5 El uso de software no licenciado, bajo responsabilidad del usuario final.
- 7.7.1.6 Utilizar en el computador personal, archivos o programas relacionados a actividades de hackeo como escaneadores de puertos de comunicación, lenguaje assembler, entre otros, salvo los utilizados por la Subgerencia de Informática para la supervisión de la red. Caso contrario, el usuario podrá ser sancionado de conformidad con el Reglamento Interno de Trabajo - RIT, así como de la Directiva sobre Administración de Personal de EMMSA.
- 7.7.1.7 No deberá usar los recursos informáticos para acceso, descarga, transmisión, distribución o almacenamiento de material obsceno, o desfavorable.
- 7.7.2 Las siguientes acciones no están permitidas en cuanto al uso del correo electrónico:
- Iniciar o responder cadenas de cualquier tipo.
 - Envío y recepción de archivos con material ajeno a las labores propias como son: pornográfico, musicales, sexista, político, religioso o discriminatorio de cualquier tipo.
 - Enviar cualquier tipo de información hacia los medios de comunicación (televisión, radio, diarios y revistas) que no cuente con la debida autorización de EMMSA.
 - Está prohibido el envío de información interna de EMMSA hacia destinatarios que no pertenecen a la misma, sin la debida justificación.
- 7.7.3 Trasladar las computadoras a otras áreas, sin la autorización escrita del área del usuario y la Subgerencia de Logística - Control Patrimonial.
- 7.7.4 Utilizar fondos de pantalla y/o protectores de pantalla para los monitores de computadoras con fotos de artistas, modelos, deportistas, dibujos animados o cualquier otra imagen poco seria u ofensiva.
- 7.7.5 Que los usuarios efectúen la instalación de software libre (freeware, shareware) en sus equipos de cómputo, sin la debida autorización de la Subgerencia de Informática.



VIII. DISPOSICIONES COMPLEMENTARIAS

Los aspectos no previstos en la presente Directiva serán resueltos por la Gerencia de Administración y Finanzas, de acuerdo a las disposiciones emitidas por la Secretaría del Gobierno Digital y otras en la materia.

IX. VIGENCIA

La presente Directiva entra en vigencia a partir del día siguiente de su publicación.

X. APROBACIÓN

Será aprobada mediante Resolución de Gerencia General.

XI. ANEXOS



EMPRESA MUNICIPAL DE MERCADOS S.A.


JAIME ADMIMIR GALLEGOS RONDÓN
GERENTE GENERAL



ANEXO N° 01

**ACTA DE COMPROMISO DE CUMPLIMIENTO DE LAS NORMAS PARA EL
USO DE RECURSOS Y SISTEMAS INFORMATICOS EN LA EMPRESA
MUNICIPAL DE MERCADOS S.A. – EMMSA,**

Por el presente, yo
identificado con DNI N°..... con el cargo de (de
ser el caso)..... en la Empresa Municipal de Mercados S.A.,
manifiesto que he leído y tengo pleno conocimiento de las disposiciones
establecidas en la presente Directiva "USO DE EQUIPOS, SOFTWARE Y
SERVICIOS INFORMATICOS EN LA EMPRESA MUNICIPAL DE MERCADOS
S.A. EMMSA", por esta razón yo me comprometo a cumplir con ellas. Del mismo
modo reconozco que mi incumplimiento podría originar responsabilidad personal e
institucional y derivar en sanciones internas y/o legales. Por lo tanto acepto que
puedo ser sancionado como corresponda a las normas legales vigentes, el
reglamento interno de personal y cualquier otra sanción de tipo legal civil o penal.

Asimismo, declaro tener pleno conocimiento que este documento, debidamente
firmado, formara parte de mi información personal.

Santa Anita, de del 20.....

.....
FIRMA

ANEXO N° 02

CONDICIONES DE USO DE LOS SERVICIOS INFORMÁTICOS



Mediante el presente, Yo,
identificado con DNI N° , declaro y manifiesto lo siguiente:

Que he recibido lo siguiente:

- Equipo de cómputo identificado con el(los) código(s) patrimonial(es) N°y ubicado en la Gerencia/Subgerencia Propiedad de EMMSA.
- Cuenta de correo electrónico:
- Acceso a Internet: SI () NO ()
- Uso de equipo Móvil: SI () NO ()

Teniendo en cuenta que, el uso del correo electrónico de la empresa es para fines laborales exclusivamente, me comprometo a no utilizarlo para asuntos personales, en caso de requerirlo, tendré que contar con la autorización expresa y previa de mi jefe inmediato.

Por intermedio del presente documento, autorizo expresamente la fiscalización del uso del correo electrónico asignado a mi persona, sometiéndome por ende a las sanciones establecidas en el Reglamento Interno de Trabajo vigente, de ser el caso, y la directiva de administración de Personal, Legislación Laboral y demás normas vigentes en caso de comprobarse el uso inadecuado del mismo.

Santa Anita, de del 20.....



USUARIO

EMMSA

ANEXO N° 03

FORMULARIO SOLICITUD DE CUENTA DE USUARIO Y ACCESOS



Tipo de Solicitud (marque con una "x")

Creación Renovación Bloqueo Anulación

Datos Generales del Usuario

Nombre del Usuario:

Cargo:

Unidad Orgánica:

Condición de Contrato:

Nombrado Plazo Fijo Otros

Del Servicio solicitado (marque con una "x")

Vigencia:

3 meses 6 meses 9 meses 12 meses Permanente

Tipo de Acceso:

Sistema Nombre del Sistema: _____

Acceso a Red Correo Electrónico Acceso a Internet

Descripción de opciones de los módulos del sistema a brindar acceso:

Observaciones:

Fecha: / /

.....
Usuario

.....
Gerente/Subgerente

.....
Subgerencia de Informática

ANEXO N° 04

RECOMENDACIONES Y BUENAS PRÁCTICAS SOBRE EL USO DE EQUIPOS, SOFTWARE Y SERVICIOS INFORMÁTICOS

1. EQUIPOS DE CÓMPUTO

- a) Se recomienda que para el encendido de los equipos de cómputo primero verificar las tomas de corriente que alimenta al computador; segundo, encender el estabilizador y esperar unos segundos a que nivele la carga eléctrica para posteriormente encender el monitor, luego el CPU y al final los demás periféricos conectados a la computadora (impresora, escáner, etc.)
- b) Apagar adecuadamente los equipos de cómputo, ayuda a conservarlos en óptimas condiciones, por tal motivo se recomienda desde el sistema Operativo (Windows 98 o XP, 7, 8,10 o posteriores), ir al Botón INICIO / APAGAR; una vez apagado el CPU, proceder con el apagado del Monitor y posteriormente los demás periféricos conectados al computador. Para finalizar ésta secuencia, apagar el Estabilizador.

Recomendaciones adicionales:

- a) Evitar apagar el estabilizador con los pies, ya que esto podría causar daños al botón de encendido/apagado o causar descargas eléctricas perjudiciales al usuario
- b) Jalar el cable que conecta el estabilizador a la toma de corriente o el cable que conecta los equipos al estabilizador, ya que esto podría causar rotura interna o externa del mismo, causando daños al equipo y el usuario.
- c) Se recomienda tener especial cuidado en el uso de las impresoras evitando colocar papel con grapas, clips u otro elemento sujetador ya que podrían causar daños internos al equipo, inclusive ocasionando la inoperatividad del mismo.
- d) Para el caso de las impresoras matriciales, verificar constantemente el nivel de desgaste de las cintas de impresión, ya que un uso excesivo produciría fallas en su cabezal y desgaste en los componentes internos.
- e) Para las impresoras de inyección de tinta y laser, verificar el nivel de carga de las mismas y el papel a utilizar, evitando colocar papel que no sea el adecuado para la impresión.
- f) El proceso de Mantenimiento preventivo y correctivo de los equipos de cómputo se encuentra a cargo del Coordinador de Mantenimiento de Equipos, previo cronograma publicado, lo realizará en coordinación con la Subgerencia de Informática.
- g) Mantener limpio el ambiente de trabajo, facilitando de ésta manera la durabilidad de las herramientas proporcionadas para el cumplimiento de sus funciones.
- h) Ingerir alimentos o tomar bebidas cerca de los equipos de cómputo puede perjudicar su operatividad y funcionamiento, por tal motivo se debe evitar este tipo de conducta.
- i) Solo el personal autorizado de la Subgerencia de Informática puede desarmar, configurar e instalar componentes de hardware en la computadora.
- j) Todo requerimiento de configuración especial debe ser coordinado con la Subgerencia de Informática, mediante un documento de requerimiento informático.
- k) Los teclados, mouses, cables y demás componentes o equipos periféricos no deben cambiar de ubicación original de una computadora a otra realizada por los mismos usuarios, caso contrario coordinarlo con la Subgerencia de Informática para dicha labor.
- l) De requerirse un cambio de ubicación física de los equipos, éstos deben ser coordinados con la Subgerencia de Informática y de ser el caso el área de Control Patrimonial de la Subgerencia de Logística.

2. CORREO ELECTRÓNICO

- a) Por motivos de confidencialidad y evitar el uso innecesario de papel, en lo posible los correos "NO" deben ser impresos; es recomendable mantenerlos guardados en los propios buzones del software de correos, salvo que sea necesaria su impresión como sustento de algún trámite administrativo.
- b) Verificar en forma periódica la bandeja de correos a fin de brindar atención oportuna a los correos recibidos.
- c) Para el reenvío de un mensaje, incluir el mensaje original para que el destinatario conozca el contexto en que se está dando el mensaje que recibe, debiendo contener cada correo enviado los datos del remitente original.

3. INTERNET

- a) En lo posible evitar el uso de correo web no institucional (Yahoo, Hotmail, GMail, etc.), la descarga y envío de archivos y software (ftp, http, etc.), salvo necesidad justificada para los temas de trabajo.
- b) Tener especial cuidado en el acceso a páginas que tengan que ver con operaciones bancarias, entre otras, ya que existen actualmente páginas falsas que podrían inducir al usuario al ingreso de información confidencial, causando la pérdida de claves de acceso a cuentas, tarjetas de crédito, etc.
- c) Asimismo, evitar el ingreso a páginas desconocidas que podrían instalar programas ocultos que deriven en instalaciones de virus informáticos.

4. ANTIVIRUS

- a) Se recomienda llevar un registro de los medios magnéticos u ópticos de almacenamiento que sean entregados a EMMSA desde fuera de ella, su origen y el usuario que lo portó, a fin de contar con elementos de control en caso de detectar alguna posible infección de equipos de cómputo.
- b) Cuando un equipo de cómputo se encuentra infectado se presenta cualquiera de los síntomas siguientes:
 - La carga de los programas toma más tiempo de lo normal
 - Demora excesiva en los accesos al disco, cuando se efectúan operaciones sencillas de escritura.
 - Se producen inusuales mensajes de errores.
 - Encendido de las luces de acceso a dispositivos, cuando no son requeridos en ese momento.
 - Disposición de menos memoria de lo normal.
 - Desaparecen programas o archivos misteriosamente.
 - Se reduce repentinamente el espacio del disco.
 - Los archivos ejecutables cambian de tamaño.
 - Aparecen inexplicablemente algunos archivos escondidos.
 - Aparecen en la pantalla una serie de caracteres especiales sin ninguna explicación lógica.
- c) Al detectar virus en un equipo de cómputo, se recomienda seguir los pasos siguientes:
 - El software Antivirus está instalado en las PC de los usuarios, este detectará la presencia de algún virus y procederá a eliminarlo por los procedimientos automáticos de dicho programa.
 - De no poder eliminarlo el software anunciará vía mensajes en pantalla de los procedimientos alternativos, para lo cual el usuario deberá notificar del hecho a la Subgerencia de Informática, quien indicará el procedimiento a seguir.



- Si se detectan indicios continuos de presencia de virus en la PC, proceder a apagar el equipo y todos los dispositivos conectados a él y se avisará a la Subgerencia de Informática quien procederá a su verificación.

- d) Dependiendo de la gravedad del daño ocasionado por el virus, si es necesario, se reconstruirá el sistema. Este proceso lo debe realizar personal de la Subgerencia de Informática.

5. BUENAS PRÁCTICAS PARA EL DESARROLLO DE SOFTWARE

Las pautas a considerar para el desarrollo de sistemas son las siguientes:

- a) Realizar el levantamiento de información para el análisis y desarrollo del proyecto
- b) Los datos serán almacenados en un servidor de Base de Datos respectivo
- c) Utilizar como lenguaje de programación aquel que EMMSA haya adquirido para tal fin.
- d) El Modelo de datos a utilizar será Entidad – Relación
- e) Realizar las pruebas del prototipo del sistema en un esquema de prueba con participación del área solicitante.
- f) Se instalará el sistema requerido en los equipos designados para tal fin y se levantará un acta de entrega y operación.
- g) Todo esto en concordancia con el "PROCEDIMIENTO PARA REQUERIMIENTO DE IMPLEMENTACION/MANTENIMIENTO DE SISTEMAS DE INFORMACION" aprobado por la Gerencia General.

6. BUENAS PRÁCTICAS PARA LA SEGURIDAD INFORMÁTICA

- a) Toda Identificación de un usuario debe ser autenticada, antes de permitirse el acceso a los aplicativos, sistemas y equipos.
- b) El password o clave de acceso debe ser confidencial, personal y no trivial.
 - Confidencial, que sólo es de conocimiento del usuario responsable
 - Personal, al establecerse bajo la responsabilidad de una persona.
 - No trivial, es decir complejo, difícil de adivinar por terceros.
- c) Es recomendable que todo usuario cambie periódicamente de password. Debe memorizarlo y no guardarlo escrito en un medio físico susceptible de ser leído por alguna otra persona ó en un archivo de computadora y es responsable de la calidad del mismo.
- d) Todos los sistemas y aplicativos deben cumplir las siguientes condiciones en cuanto a la administración de los password:
 - Confidencial, que sólo es de conocimiento del usuario responsable
 - Revisar la longitud del password, el cual debe ser mínimo de 6 caracteres
 - Revisar la calidad del password, el cual debe contener al menos un número y al menos una letra.
 - Permitir la utilización de caracteres especiales.
 - Bloquear los códigos de usuario luego de 3 intentos errados de autenticación (password errado).
 - Los password "NO" deben ser almacenados en forma legible en archivos batch, scripts de logon-in automáticos, macros de software, computadoras sin control de acceso, ó en otro medio físico ó electrónico que posibilite que personas no autorizadas puedan descubrirlos.
 - Los password no deben ser mostrados ni impresos en el momento en que son solicitados.
 - Los sistemas de comunicación y de computación deberán ser diseñados, probados y controlados de modo que los password guardados no puedan ser recuperados ya sea en forma encriptada o no.



7. BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESOS

- Los responsables del área son los autorizados a evaluar y solicitar el acceso a los sistemas y aplicativos para sus usuarios, de acuerdo a las funciones asignadas y a los perfiles previamente establecidos.
- La autorización y privilegios para acceder a información, recursos y sistemas de comunicación se otorgarán teniendo en cuenta las necesidades reales de los usuarios para la realización de las labores encomendadas.



8. BUENAS PRÁCTICAS PARA LOS PROCESOS DE BACKUP

a) Consideraciones Previas

- Con el propósito de realizar de una manera rápida y efectiva las copias de seguridad, los usuarios deberán estructurar carpetas especiales donde podrán grabar su información de importancia sobre los trabajos realizados considerando para ello la estructura interna del mismo con nombres que identifiquen el tipo de información a grabar, facilitando de esta manera una ubicación rápida y oportuna.
- Adicionalmente, la Subgerencia de Informática ha instalado en cada uno de los computadores de los usuarios, unas unidades de red que servirán para la replicación de los datos considerados de importancia y que han sido creados conforme a lo señalado en el punto anterior. Dichas unidades de red almacenan la información en el Servidor de Archivos instalado en la Subgerencia de Informática.
- Cada uno de los programas ofimáticos que utilicen los usuarios de los equipos de cómputo para el desarrollo de sus labores se deberán configurar para que registren y obtengan de forma pre definida la información generada en las carpetas creadas con el procedimiento mencionado en el punto anterior, lo que se deberá coordinar con la Subgerencia de Informática para su cometido.
- Se deberán tomar en consideración que para la determinación del nombre de los archivos estos deben considerar hacer referencia al tipo de documento generado y de ser posible un número correlativo para su identificación sin tomar en cuenta caracteres especiales (% & \$ #, etc.). En cuanto a las extensiones de los mismos deben considerarse solamente las correspondientes al software utilizado por ejemplo word = *.doc, excel = *.xls, power point = *.ppt, etc.; ya que el colocar alguno que no corresponda puede ocasionar una mala identificación o no reconocimiento por el software origen.
- En caso de recibir información en medios magnéticos, se deberán revisar previamente con el software antivirus proporcionado por EMMSA en los equipos de cómputo a fin de evitar la infección y/o pérdida de información.



b) Procedimiento de Copiado

Para la Subgerencia de Informática

- "Copias en caliente" para las bases de datos: Como oficina encargada de salvaguardar la integridad de la información de EMMSA en cuanto a Bases de Datos en ORACLE, el procedimiento de Backups de la información generada por los diversos Sistemas, se almacenarán en archivos con extensión *.dmp (generados por utilitarios del propio administrador de base de datos ORACLE), mediante la ejecución automática y en forma diaria de un proceso en lotes en una consola del sistema operativo, para ser comprimidos y luego trasladados a dispositivos de almacenamientos magnéticos.
- "Copias en frío" para las bases de datos: Este proceso de copia de seguridad requiere desconectar a la totalidad de usuarios, es decir, no tener cargado en el servidor principal ningún enlace con la base de datos ORACLE y luego del cual se procederá a realizar la compresión de los archivos que conforman la base de datos para luego ser copiado en medios magnéticos.
- Se realizará Backups de la información generada por los diversos sistemas de información con que cuente la entidad y se generaran en archivos comprimidos y luego son copiados en dispositivos de almacenamientos magnéticos.
- Los Archivos de programas fuentes se almacenan en medios magnéticos y en formato comprimido.



- Cualquier otro tipo de información generada por la Subgerencia de Informática será alojada en carpetas especiales para su posterior copia de respaldo en medios magnéticos.
- Conforme a los requerimientos de las diversas áreas, la Subgerencia de Informática procederá a realizar copias de seguridad de la información alojada en los equipos de cómputo de los usuarios de dichas áreas en medios magnéticos.
- Se capacitará a los usuarios que cuenten con dispositivos de almacenamiento masivo de información en sus equipos de cómputo a fin de que puedan desarrollar esta labor de respaldo para la seguridad de los datos contenidos en los equipos ubicados en su área.
- Se evaluará la conveniencia de contratar los servicios de un tercero para la custodia de los medios de resguardo al menos una (1) vez por semana.

Para los usuarios diversos

- Los usuarios deberán registrar su información en las carpetas creadas para tal fin, conforme a lo mencionado en el primer punto de las consideraciones previas, lo que facilitará el proceso de copia de seguridad.
- Tal como se mencionó en el segundo punto de las consideraciones previas, será responsabilidad de los usuarios de equipos de cómputo la generación de sus copias de seguridad de réplica en las unidades de red, creadas para tal fin.
- Aquellos usuarios que cuentan en sus equipos de cómputo con dispositivos de almacenamiento masivo podrán realizar copias de seguridad de los datos contenidos en los equipos de cómputo de su respectiva área como un respaldo adicional a los antes mencionados.
- Para las áreas que no cuentan con dispositivos de almacenamiento masivo de información se cuenta con lo alojado en la unidad de red de las computadoras con que cuenta dicha área. Establecer los lineamientos para la formulación, aprobación, suscripción, seguimiento y evaluación de los Convenios suscritos con la Empresa Municipal de Mercados S.A. – EMMSA y la entidad.



EMPRESA MUNICIPAL DE MERCADOS S.A.


JAIME ADHEMIR GALLEGOS RONDON
GERENTE GENERAL



Directiva

ADMINISTRACIÓN DE SOFTWARE EN EMMSA

Resolución de Gerencia General N° 15 -GG-EMMSA-2020



CÓDIGO: DI-013-GAF/010

Fecha de Aprobación:

Páginas: 1/16

Primera Versión

ÍNDICE



I. OBJETIVO

II. ALCANCE

III. BASE LEGAL



IV. GLOSARIO DE TÉRMINOS

V. RESPONSABILIDADES

VI. DISPOSICIONES GENERALES

VII. DISPOSICIONES ESPECÍFICAS

VIII. DISPOSICIONES COMPLEMENTARIAS



IX. VIGENCIA

X. APROBACIÓN

XI. ANEXOS:

ANEXO N° 01: POLÍTICAS DE REGISTRO REFERENTES AL USO LEGAL DE SOFTWARE PARA LAS COMPUTADORAS PERSONALES.

ANEXO N° 02: FORMATO DE REQUERIMIENTO DE INSTALACIÓN DE SOFTWARE.

ANEXO N° 03: REGISTRO DE SOFTWARE INSTITUCIONAL.

ANEXO N° 04: ESTÁNDAR DE SOFTWARE LEGAL A UTILIZARSE EN EMMSA.



I. OBJETIVO

Establecer lineamientos para la administración y uso del software en la Empresa Municipal de Mercados S.A. - EMMSA, con el propósito de asegurar la legalidad del software, así como también el uso en cumplimiento de los términos de la licencia correspondiente.

II. ALCANCE

Esta directiva es administrada por la Gerencia de Administración y Finanzas a través de la Subgerencia de Informática y es de aplicación obligatoria para todos los órganos y unidades orgánicas que conforman EMMSA.

III. BASE LEGAL

- 
- 
- 
- 
- 
- 
- 3.1 **Ley N° 28612**, aprueba Ley que Norma el Uso, Adquisición y Adecuación del Software en la Administración Pública, del 18 de octubre de 2005.
 - 3.2 **Ley N° 28716**, aprueba Ley de Control Interno de Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.
 - 3.3 **Decreto Legislativo N° 822**, aprueba Ley Sobre el Derecho de Autor, del 24 de abril de 1996.
 - 3.4 **Decreto Supremo N° 013-2003-PCM**, aprueba medidas para Garantizar la Legalidad de la Adquisición de Programas de Software en Entidades y Dependencias del Sector Público, de 13 de febrero de 2003.
 - 3.5 **Decreto Supremo N° 043-2003-PCM**, aprueba Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 24 de abril de 2003.
 - 3.6 **Decreto Supremo N° 024-2006-PCM**, aprueba Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública, del 24 de mayo de 2006.
 - 3.7 **Decreto Supremo N° 350-2015-EF**, aprueba el Reglamento de la Ley N° 30225, Ley de contrataciones del estado, del 10 de diciembre de 2015 y sus modificatorias.
 - 3.8 **Decreto Supremo N° 082-2019-EF**, aprueba el Texto Único Ordenado de la Ley N° 30225, Ley de contrataciones del estado, del 13 de marzo de 2019.
 - 3.9 **Resolución Ministerial N° 073-2004-PCM**, aprueba Guía para la Administración Eficiente del Software Legal en la Administración Pública, del 17 de marzo de 2004.
 - 3.10 **Resolución Ministerial N° 139-2004-PCM**, aprueba documento "Guía Técnica sobre Evaluación de Software para la Administración Pública", del 28 mayo de 2004.
 - 3.11 **Resolución Ministerial N° 246-2007-PCM**, aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad

de la Información. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática del 25 de agosto de 2007.

- 3.12 **Resolución de Contraloría N° 320-2006-CG**, aprueba las Normas de Control Interno, del 03 de noviembre de 2006.
- 3.13 **Resolución de Gerencia General N° 063-2019-EMMSA/GG**, aprueba la Directiva N° 001-GPPE/001, Formulación de los Documentos Normativos de EMMSA, del 13 de diciembre de 2019.
- 3.14 **Acuerdo de Directorio N° 039-2015**, aprueba el Reglamento de Organización y Funciones de EMMSA, del 28 de octubre de 2015.



IV. GLOSARIO DE TÉRMINOS

4.1 Antivirus

Programa cuya función es detectar y eliminar virus informáticos y otros programas maliciosos que afectan el normal funcionamiento de las computadoras y/o red de cómputo.



4.2 Adquisición de Software

Para la presente directiva la adquisición de un software incluye los discos, la documentación técnica, los manuales y la licencia de uso del producto. El propietario del software es el autor o productor y la propiedad nunca se transfiere. El proveedor del producto, es licenciataria del software y goza de potestad adquirida bajo un contrato de distribución, de ceder al usuario el derecho de uso otorgado por el autor. El distribuidor, en cambio, no transfiere la propiedad intelectual del software, actuando solamente como intermediario entre el titular y el consumidor, sin perjuicio de las normas aplicables de protección al consumidor.



4.3 Declaración de Software

Documento por el cual la institución declara los programas de computadoras o software y licencias de uso con las que cuenta; la misma que debe estar acompañada de las copias de licencias de uso de software y las facturas consignadas en la declaración.



4.4 Freeware

Programas gratuitos que los desarrolladores ponen a disposición de otros usuarios sin ningún costo.



4.5 Licencia

Documento obtenido por la compra, cuya posesión faculta la instalación y uso de software o programa de computadora y establece las reglas básicas para su utilización y sus limitaciones.



4.6 P2P (Peer to Peer)

Programas o conexiones de red empleados para prestar servicios, a través de Internet, de intercambio de archivos de software, música (mp3), videos (películas) y juegos por lo general; entre la lista de principales aplicaciones P2P podemos mencionar a los siguientes:

- 4.6.1 BitTorrent (Azureus, BitComet, DirectConnect).
- 4.6.2 Gnutella (Shareaza, NeoModus, DirectConnect, DC).
- 4.6.3 EnDonkey (Overnet, Cliente eDonkey).
- 4.6.4 Emule (clienteemule, aMule, mIDonkey, Iphant).
- 4.6.5 KaZaa; Freenet; Limewire; Napster; WinMX; Soulseek; Audiogalaxy; Bearshare; Imesh Morpheus; Grokster; Xolox; OneMX; Freewire; Gnucleus; Blubster1.2.3; Soulseek. Blubster2.x (o Piolet).
- 4.6.6 Skype.

4.7 Reproducción o Copia

Cualquier forma de fijación u obtención de copias de obra de forma permanente o temporal sea por imprenta, registro electrónico, fonográfico, digital, etc.

4.8 Servidor

En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otros denominados clientes. Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios (clientes) se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

4.9 Shareware

Software distribuido en forma gratuita para ser probado. Si el usuario decide quedarse con el programa y seguir usándolo, debe pagar al desarrollador o fabricante.

4.10 Sistema Informático

Es el conjunto de partes interrelacionada que comprenden hardware, software y recursos humanos que permiten almacenar y procesar información.

4.11 Software o Programa para Computadora

Conjunto de instrucciones mediante palabras, códigos, planes o cualquier otra forma, que al ser incorporados en un dispositivo de lectura automatizada, es capaz de hacer que una computadora ejecute una determinada tarea u obtenga un resultado. El software o programa de computadora comprende también la documentación técnica y los manuales de uso.

4.12 Software desarrollado por EMMSA

Se refiere a los aplicativos desarrollados por el personal de la Subgerencia de Informática de la Gerencia de Administración de Finanzas de EMMSA o por terceros para brindar soporte a nuestra empresa, de los que EMMSA, es propietario del aplicativo y de los programas fuentes.



V. RESPONSABILIDADES

- 5.1 La Subgerencia de Informática, supervisa el cumplimiento de la presente Directiva a nivel de todas las áreas de la Empresa Municipal de Mercados S.A. – EMMSA.
- 5.2 Los Gerentes y Subgerentes son responsables de velar por el estricto cumplimiento de la presente Directiva.
- 5.3 Todo el personal de la Empresa Municipal de Mercados S.A. - EMMSA, en calidad de usuarios de los sistemas informáticos, son responsables de cumplir con lo dispuesto en la presente Directiva.



VI. DISPOSICIONES GENERALES

- 6.1 La Subgerencia de Informática formula y comunica mediante el Anexo N° 01 a las áreas de EMMSA, sobre la "Política de la Empresa Municipal de Mercados S.A. - EMMSA referente al uso legal de software para computadoras personales", la que permite establecer el compromiso de EMMSA, en concordancia con los siguientes objetivos:

- 6.1.1 Respeto a los derechos de autor.
- 6.1.2 Administración de las necesidades de software.
- 6.1.3 Adquisición o regularización del software y su licencia mediante el proceso de compra aprobada.

- 6.2 La Empresa Municipal de Mercados SA. - EMMSA, establece como política institucional el uso legal del software en los servidores de la red y las estaciones de trabajo, cumpliendo con lo establecido en los términos de la licencia de uso de software.

- 6.3 Esta Directiva es de carácter general y de cumplimiento obligatorio para todo el personal de EMMSA, para tal efecto, todos los usuarios de EMMSA, tendrán acceso a ésta, a través de la web institucional: <http://www.emmsa.com.pe>.

- 6.4 La Subgerencia de Informática debe comunicar cualquier actualización de la presente Directiva e informar sobre información adicional de la misma.

VII. DISPOSICIONES ESPECÍFICAS

7.1 DE LA ADMINISTRACIÓN DE SOFTWARE

- 7.1.1 Con el propósito de desarrollar una eficiente administración del software, así como poder establecer las necesidades de software de las áreas de EMMSA y estandarizar el uso de los distintos programas, la Subgerencia de Informática, realiza las siguientes acciones:



- a) Efectuar semestralmente el inventario físico, de todas las computadoras (servidores, estaciones de trabajo, computadoras portátiles) con que cuenta en EMMSA.
- b) Efectuar semestralmente el inventario de software, instalado en las computadoras de EMMSA, apoyado de las herramientas informáticas de administración de recursos informáticos, con que cuenta la institución para tales fines.
- c) Evaluar e identificar el software instalado en las computadoras de EMMSA, a fin de detectar software no licenciado o malicioso, procediendo a la desinstalación inmediata, de ser el caso.
- d) Realizar el inventario físico de la documentación del software adquirido e instalado en las computadoras de EMMSA, el mismo que incluirá los medios (discos compactos, direcciones URL, DVD, u otros), que son utilizados para la instalación del producto, de las licencias originales de uso, así como también el registro de los números de las órdenes de compra que acrediten la compra del software.
- e) Emitir semestralmente un reporte del análisis comparativo entre la cantidad de licencias adquiridas por EMMSA y las que están en uso, a fin de determinar la cantidad de licencias necesarias para adquisición, habiendo efectuado previamente, la depuración del software en las computadoras de EMMSA, teniendo en cuenta la labor funcional de los usuarios. La Subgerencia de Informática debe informar los resultados semestralmente a la Gerencia de Administración y Finanzas, para la gestión correspondiente.

7.1.2 La Subgerencia de Informática elabora y actualiza el registro de software institucional, utilizando para ello el Anexo N° 03 "Registro de Software Institucional". El registro consiste en un inventario actualizado de las licencias de software en uso: sistema operativo, software de oficina, software antivirus y demás programas especializados que se utilicen.

7.1.3 Para las aplicaciones de software desarrolladas por la Subgerencia de Informática, o por terceros de los que se tengan los programas fuentes, se debe remitir el listado de dichos programas a la Gerencia General de EMMSA, para su registro ante la Oficina de Derechos de Autor del INDECOPI.

7.1.4 La Subgerencia de Informática debe incluir dentro de su Plan de Trabajo Anual, la ejecución semestral del inventario de software de todas las computadoras y/o servidores de EMMSA.

7.1.5 La Subgerencia de Informática debe mantener identificadas las computadoras que intervienen directamente en la captura, procesamiento, registro, reporte, almacenamiento o recuperación de datos, asegurándose que el software utilizado en estos cuenta con su respectiva licencia, además de estar documentado y validado para su uso.



- 7.1.6 La Subgerencia de Informática, debe tomar las acciones necesarias para el mantenimiento de las licencias de software, liberando licencias asignadas teniendo en consideración los reportes de personal cesante provistos por la Subgerencia de Recursos Humanos.

7.2 ESTANDARIZACIÓN Y ADQUISICIÓN

- 7.2.1 La Subgerencia de Informática, debe definir el estándar inicial de software a utilizarse en las computadoras de EMMSA a fin de cumplir con lo dispuesto en la Ley de Contrataciones del Estado, aprobado mediante Decreto Legislativo N° 1017 y su Reglamento; usando para tal efecto el Anexo N° 4 "Estándar de Software Legal a Utilizarse en la Empresa Municipal de Mercados S.A. -EMMSA", el mismo que será validado anualmente.

- 7.2.2 El software es considerado un activo intangible de la institución por lo que corresponde a la Subgerencia de Informática, en coordinación con la Subgerencia de Contabilidad, de la Gerencia de Administración y Finanzas, tener un inventario actualizado de las licencias originales de todos los programas que haya adquirido o adquiriera EMMSA, con el propósito de contar con un documento consolidado, que será avalado por el acervo documentario del software adquirido en la institución (como copias fotostáticas de órdenes de compra y/o facturas de compra). Así mismo, en caso existiese un activo tangible (disco duro externo, computadora, etc.) que constituya parte del activo intangible (software), este debe ser informado a la Subgerencia de Logística - Control Patrimonial y consecuentemente la remisión de los documentos fuentes que sustenten su adquisición, para su registro, control y asignación, con el respectivo código patrimonial y usuario que corresponda.

- 7.2.3 En concordancia con lo dispuesto por el Art. 3° del Decreto Supremo N° 013-2003-PCM, la Subgerencia de Informática deberá solicitar ante el área pertinente de EMMSA, la previsión presupuestal para el financiamiento de la adquisición de las licencias necesarias. Así mismo, cada vez que se formule un requerimiento de compra de un equipo de cómputo, éste deberá considerar en su presupuesto el costo del software y licencias del sistema operativo, software de oficina y software antivirus.

- 7.2.4 En concordancia con el Art. 6° del Reglamento de la Ley N° 28612, toda adquisición y uso de licencias de software en la institución requerirá de un Informe Técnico Previo de Evaluación de Software, que deberá ser emitido por la Subgerencia de Informática. De ser necesario, se requerirá el apoyo del (as) área(s) usuaria(s) involucrada(s) en dicho requerimiento de software.

- 7.2.5 Para la elaboración del Informe Técnico Previo de Software, las áreas solicitantes del o los productos de software, debe proporcionar a la Subgerencia de Informática, a través de la documentación correspondiente, la siguiente información:

- 7.2.5.1 Nombre del Órgano o Unidad Orgánica.



- 7.2.5.2 Nombre de la persona que efectuó la evaluación de los productos de software.
- 7.2.5.3 Justificación para la adquisición del producto de software.
- 7.2.5.4 Alternativas de productos de software, con una breve explicación.
- 7.2.5.5 Análisis técnico Comparativo de los productos de software evaluados.

7.2.6 En concordancia de los Arts. 8° y 9° del Reglamento de la Ley N° 28612, Subgerencia de Informática, debe gestionar la publicación en la página Web Institucional, de los Informes Técnicos Previo que sirvan de sustento para los procesos de selección que involucren la adquisición de software, salvo que cuando por razones de seguridad nacional, el contenido del mencionado Informe Técnico Previo haya sido calificado como información secreta, reservada o confidencial, de acuerdo a lo establecido en los artículos 15°, 16° y 17° del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo N° 043-2003-PCM y sus modificatorias.

7.2.7 La Subgerencia de Informática, a través de sus dependencias, evalúa permanentemente los programas y/o actualizaciones existentes en el mercado tecnológico para su posible incorporación dentro de la lista de programas estandarizados.

7.3 DE LA INSTALACIÓN DE SOFTWARE

7.3.1 El personal de la Subgerencia de Informática, es responsable de revisar, instalar o desinstalar el software; así mismo debe eliminar el software que no esté incluido en el perfil de usuario, aun cuando sean estos legales y de propiedad del usuario; estando prohibido, bajo responsabilidad, de instalar software que no sea proporcionado por la Subgerencia de Informática con las respectivas licencias de uso.

7.3.2 Para el caso de los programas de distribución gratuita (freeware) o de prueba (shareware), los usuarios del sistema, pueden utilizarlos siempre y cuando demuestren que son utilizados por un periodo corto, y para el desarrollo de las labores asignadas dentro de la entidad. Dentro de los programas que pueden ser instalados, se encuentran los llamados "parches" o "actualizaciones" que los fabricantes distribuyen en forma gratuita para optimizar sus productos; así como también, el software gratuito para leer documentos en formato PDF (Adobe Acrobat Reader).

7.4 DE LOS PERFILES DE USUARIO

7.4.1 El perfil de usuario de software debe ser elaborado y administrado por la Subgerencia de Informática para la estandarización, control y optimización del uso de los programas, según las necesidades de la institución.

7.4.2 Para solicitar la instalación de software se utiliza el Formato de Requerimiento de Instalación de Software (Anexo N° 02), el cual se remite mediante Memorando dirigido a la Subgerencia de



Informática, a través del Sistema de Tramite Documentario, teniendo en consideración los siguientes perfiles:

7.4.2.1 **Usuario Nivel 1:** Aquel que utiliza el sistema operativo windows, antivirus, utilitario para lectura de archivos PDF, aplicativos institucionales.

7.4.2.2 **Usuario Nivel 2:** Aquel que utiliza el sistema operativo, windows, software de oficina, antivirus, utilitario para lectura de archivos PDF y aplicativos institucionales.

7.4.2.3 **Usuario Nivel 3:** Aquel que utiliza el sistema operativo windows, software de oficina, antivirus, utilitario para lectura de archivos PDF, aplicativos institucionales y software específico para funciones establecidas y formalizadas por pedido expreso por escrito del Gerente del área correspondiente.

Una vez aceptada la solicitud, el personal de la Subgerencia de Informática procederá a ejecutar la instalación de contarse con la disponibilidad de licencias de ser el caso.

7.4.3 La Subgerencia de Informática instala los programas en los equipos asignados, según el perfil de usuario, eliminando aquellos que no correspondan con el perfil establecido.

7.4.4 Toda solicitud de instalación de software, debe estar debidamente justificada por el rol y responsabilidades establecidas al usuario y la solicitud, utilizando para ello el Anexo N° 02 "Formato de Requerimiento de Instalación de Software".

7.4.5 De acuerdo a lo solicitado, la Subgerencia de Informática, evalúa si las características técnicas del equipo a instalar satisfacen los requerimientos mínimos para su adecuado funcionamiento, además de las licencias de uso disponibles del software. Si la solicitud es aceptada, la Subgerencia de Informática procede a coordinar la ejecución de la instalación.

7.4.6 Al finalizar la instalación, se debe obtener la conformidad y registro del usuario a través de la Subgerencia de Informática.

7.4.7 La Subgerencia de Informática debe efectuar el seguimiento y control sobre el uso de las licencias asignadas a los usuarios, mediante el uso de herramientas de administración de recursos o visitas inopinadas, según el perfil de usuario de software establecido y los formatos de requerimientos de su Gerencia.

7.4.8 Para el caso de los aplicativos institucionales que requieren acceso por código de usuario, las áreas efectúan la respectiva solicitud de creación o modificación de usuarios.

7.4.9 Los programas instalados que no sean de utilidad para el usuario, deben ser eliminados inmediatamente. Si el usuario no utiliza los programas, inicialmente instalados en su equipo, se recomienda que soliciten a la Subgerencia de Informática, la desinstalación de aquellos, permitiendo de esa forma el uso racional de la licencia correspondiente.



7.4.10 Queda terminantemente prohibida la instalación y uso de software para operar sistemas en redes de tipo Peer to Peer (P2P) utilizados para prestar servicios a través de Internet de intercambio de archivos de software, música (mp3), videos (películas) y juegos en general.

7.5 DE LA CUSTODIA DE SOFTWARE

7.5.1 La Subgerencia de Informática, debe preservar en un lugar seguro centralizado, todas las licencias de software originales, medios de instalación (discos compactos, DVD, etc.) y documentación.

7.5.2 Periódicamente la Subgerencia de Informática, debe comunicar a la Gerencia de Administración y Finanzas, la relación de software en desuso u obsoleto, para que esta disponga al área competente la baja correspondiente, entregando, los discos compactos, DVD, otros medios de instalación y documentación, que ya no se utilicen por estar en desuso u obsolescencia.

7.6 DE LAS SANCIONES

7.6.1 De conformidad con lo establecido en el Art. 69° del Capítulo II del Título VI: De los Programas de Ordenador del Decreto Legislativo N° 822, Ley de Derechos de Autor, los programas de ordenador (computadora), se protegen en los mismos términos que las obras literarias. Dicha protección se extiende a todas sus formas de expresión, tanto a los programas operativos como a los aplicativos, ya sea en forma de código fuente o código objeto. Dicha protección se considera extendida a cualquier de las versiones sucesivas del programa, así como a los programas derivados.

7.6.2 Asimismo, la indicada norma dispone que la reproducción de un programa de ordenador, inclusive para uso personal, exigirá la autorización del titular de los derechos, con la excepción de la copia de seguridad.

7.6.3 Además de los acuerdos de licencias, la ley de derechos de autor protege a los autores del software, de la reproducción y distribución no autorizados de software. La misma ley prohíbe también que los usuarios carguen, descarguen o transmitan copias no autorizadas de software por Internet u otros medios electrónicos. Las violaciones de estas restricciones pueden constituir delitos, los cuales exponen al infractor a sanciones.

7.6.4 La Subgerencia de Informática no permitirá que el personal de EMMSA, instale o realice copias no autorizadas de software. El personal que labore en EMMSA que instale o copie software ilegalmente cometerá falta y estará sujeto a las acciones disciplinarias correspondientes.

7.7 DE LA DIFUSIÓN

7.7.1 La Empresa Municipal de Mercados SA. - EMMSA, a través de la Subgerencia de Informática, se compromete a comunicar y difundir la presente Directiva al personal de EMMSA que labora bajo cualquier modalidad de contrato de servicios.



VIII. DISPOSICIONES COMPLEMENTARIAS

Los aspectos no previstos en la presente Directiva serán resueltos por la Gerencia de Administración y Finanzas, a través de la Subgerencia de Informática, de acuerdo a las disposiciones emitidas por la Secretaría del Gobierno Digital y otras en la materia.

IX. VIGENCIA

La presente Directiva entra en vigencia a partir del día siguiente de su publicación.

X. APROBACIÓN

Será aprobada mediante Resolución de Gerencia General.

XI. ANEXOS



EMPRESA MUNICIPAL DE MERCADOS S.A.


JAIME ADHEMIR GALLEGOS RONDÓN
GERENTE GENERAL

ANEXO N° 01

POLÍTICA DEL REGISTRO REFERENTES AL USO LEGAL DE SOFTWARE PARA COMPUTADORAS PERSONALES



1. EMMSA, adquiere las licencias de software de diversos fabricantes, para sus computadoras (estaciones de trabajo y servidores de red) y son de uso del personal de la empresa. La Empresa Municipal de Mercados S.A. - EMMSA no es propietario de este software, ni de su documentación y, a menos que cuente con autorización del desarrollador del software, no tiene derecho para reproducirlo, excepto para crear una copia de respaldo (backup).
2. Con respecto a aplicaciones cliente / servidor y para redes, el personal de EMMSA, utilizará el software respetando las disposiciones de los contratos de licencia correspondientes.
3. Queda terminantemente prohibido descargar e instalar software no autorizado de la Internet; asimismo la instalación y uso de software para operar sistemas de tipo Peer to Peer (P2P) empleados para prestar servicios a través de Internet de intercambio de archivos de software, música (mp3), videos (películas) y juegos en general.
4. El personal de EMMSA que tenga conocimiento de uso incorrecto de software o documentación relacionada dentro de la institución, deberá informarlo al responsable del área donde labora, para que este haga lo propio a la Subgerencia de Informática, a fin de adoptar las medidas correctivas correspondientes.
5. Está prohibido el préstamo o el otorgamiento del software con licencia de la institución a persona alguna.
6. El personal que labore en EMMSA, que instale o reproduzca software ilegalmente cometerá falta al exponer a la institución a demandas civiles, penales y administrativas y estará sujeto a las acciones disciplinarias correspondientes. La Ley de Derechos de Autor (Decreto Legislativo N° 822), establece que las personas involucradas en la reproducción ilegal de software pueden sufrir sanciones por daños civiles y penales, incluyendo multas y pena privativa de libertad.
7. Todas las dudas que tenga el personal de EMMSA sobre la autorización para copiar o utilizar un programa de software específico, deberán ser aclaradas por la Subgerencia de Informática, antes de proceder a realizar la copia o utilizar el software.
8. Todo requerimiento de software deberá ser solicitado mediante "Formato de Requerimiento de Instalación de Software" (Anexo N° 02). No se deberá instalar ningún programa en la computadora sin la autorización respectiva, a efectos de que la Subgerencia de Informática, verifique que cuente con la licencia de uso correspondiente.
9. La Empresa Municipal de Mercados S.A. - EMMSA se reserva el derecho de proteger su reputación e inversión en software para computadoras al imponer controles internos para evitar que se hagan o usen copias no autorizadas de software. El personal de la Subgerencia de Informática efectuara estos controles que pueden incluir verificaciones frecuentes y periódicas del uso de software, revisiones programadas y no programadas de las computadoras de la institución para asegurar el cumplimiento, y la remoción de cualquier software que se encuentre instalado en equipos de los que no pueda determinarse la disponibilidad legal.
10. Todo proyecto de software desarrollado a iniciativa propia de las áreas deberá contar con la aprobación de la Subgerencia de Informática quien evaluará su factibilidad técnica-operativa y autorizará su ejecución.
11. Cualquier programa de software adquirido y/o desarrollado por las áreas a nombre de la Empresa Municipal de Mercados S.A. - EMMSA, deberá ser declarado a la Subgerencia de Informática para su registro y custodia.

ANEXO N° 02
FORMATO DE REQUERIMIENTO DE INSTALACIÓN DE SOFTWARE

Nombre y Apellidos: _____ N° DNI: _____

Área donde labora: _____

Nivel de Usuario: _____

Gerencia que autoriza: _____

Fecha: _____

Número de Serie y/o código Patrimonial del CPU: _____

El (los) producto (s) de software especializado (s) que requiero, aún no se encuentra instalado en la computadora que se me asigno para el desempeño de mis labores, pero me ayudará en el desarrollo de mis tareas y funciones. El software que requiero sea instalado en la computadora que tengo asignada es el siguiente:

Programa de Software	Versión	Utilización (1, 2)	Sustento o Justificación de Uso

Utilización: 1=Permanente; 2=Temporal (Si elige la opción 2, declarar el tiempo de uso. Al cumplirse el tiempo declarado, la Subgerencia de Informática desinstalará el software sin que, necesariamente se consulte al usuario)

 Usuario Solicitante

 Firma y Sello del Gerente que Autoriza

ANEXO Nº 03

REGISTRO DE SOFTWARE INSTITUCIONAL

1.- Nombre :

2.- Sumilla :

3.- Tipo de Licencia : OEM Full Pack Por Volumen Otras

4.- Versión :

5.- Fabricante :

6.- N° Serie :

7.- Código de Licencia :

8.- Licencias Adquiridas : 9.- Licencias instaladas :

10.- Estado Actual : Operativa en uso Operativa en Desuso De baja

11.- Fecha de Adquisición : / /

12.- Régimen de Tenencia : Propia Alquilado Prestado Donado

13.- Tipo de Software : Sistema Operativo Lenguaje de Programación
 Base de Datos Red de Datos
 GIS Diseño Gráfico
 Software de Oficina Software de Seguridad
 Aplicativo Institucional Otros

14.- Manuales : De diseño Si No
 De usuario Si No

15.- Saldo de Nro Licencias : Exceso Defecto

.....
 Firma del Encargado de Licenciamiento

Fecha:



ANEXO N° 04

ESTANDAR DE SOFTWARE LEGAL A UTILIZARSE EN EMMSA



1. SERVIDORES DE RED

- 
- a. Sistema Operativo: Windows Server, HP UX y Linux RED HAT.
 - b. Sistema de Base de Datos: Oracle y SQL Server.
 - c. Antivirus Corporativo: ESET File Security.
 - d. Plataforma de Servicio /Dominio/Correo Electrónico: MS Exchange.
 - e. Sistema de Seguridad Web.



2. ESTACIONES DE TRABAJO

- 
- 
- 
- a. Sistema Operativo: MS Windows Professional.
 - b. Software de Oficina: MS Office Professional.
 - c. Software Antivirus: ESET Endpoint Security.
 - d. Utilitario: Adobe Acrobat Reader.
 - e. Software Especializado:
 - Firma Digital: Adobe Acrobat Professional.
 - Estadístico: IBM SPSS Statistics.
 - Diseño: Adobe Creative Suite, Corel Draw GS, QuarkXpress.
 - Proyectos: MS Project Professional y CA Change Manager.
 - Modelamiento de Base de Datos: IBM RSA, PL/SQL Developer.
 - Diagramación: MS Visio Estándar, Bizagi Modeler, Archi.
 - Otros a necesidad de servicio.