

III. ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE

137

VILLA DEL PRADO

ORGANIZACIÓN Y FUNCIONAMIENTO

Al no haberse presentado reclamaciones durante el plazo de exposición al público, queda automáticamente elevado a definitivo el acuerdo plenario inicial aprobatorio del Reglamento Municipal de Uso de los Servicios y Bienes Informáticos y de Comunicaciones del Ayuntamiento de Villa del Prado, cuyo texto íntegro se hace público, para su general conocimiento y en cumplimiento de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

REGLAMENTO MUNICIPAL DE USO DE LOS SERVICIOS Y BIENES INFORMÁTICOS Y DE COMUNICACIONES DEL AYUNTAMIENTO DE VILLA DEL PRADO

Capítulo I

Disposiciones generales

Artículo 1. *Objetivo y ámbito de aplicación.*—1.1. Objetivo: el Ayuntamiento de Villa del Prado ofrece a todos sus componentes, empleados públicos, miembros de la Corporación y demás usuarios señalados en el artículo 2.3, el acceso a la Red Informática Municipal de Villa del Prado (RIMVDP) para el mejor desarrollo de su actividad.

Este Reglamento y las normas relacionadas tienen como objetivos:

- Asegurar el correcto despliegue y uso de los servicios y bienes informáticos del Ayuntamiento y para que la información difundida en las comunicaciones, sea utilizada de forma adecuada.
- Garantizar la calidad de los servicios y un uso de los medios informáticos de acuerdo con los fines últimos para lo que fueron creados: mejorar los servicios generando una mejor atención al ciudadano.
- Establecer los requerimientos para la protección y utilización de los recursos informáticos, telefonía fija, móvil y comunicación telemática en el Ayuntamiento de Villa del Prado. Dichos recursos incluyen los sistemas de acceso a la RIMVDP, aplicaciones de programas informáticos (“software”) y “hardware” asociado.

1.2. Ámbito de aplicación: la presente normativa es de aplicación a los usuarios señalados en el artículo 2.3, así como a cualquier otra persona que tenga acceso a la red informática interna del Ayuntamiento. Cualquier equipo que se conecte a dicha red, aunque no sea propiedad del Ayuntamiento, quedará sujeto a las normas y condiciones contenidas en este Reglamento. Asimismo, todo tipo de información, indistintamente del medio en que esté almacenado, así como los medios automatizados que hayan sido utilizados para su almacenamiento, proceso y transmisión de la información, quedan incluidos en el presente Reglamento.

El presente Reglamento será de aplicación sin perjuicio de las disposiciones legales aplicables en la materia.

Art. 2. *Procedimiento y acceso a los servicios y recursos.*—2.1. Procedimiento de actuación: la información es el activo más valioso del Ayuntamiento. La conservación de su integridad y disponibilidad es esencial para obtener un buen resultado con los administrados. Se tomarán medidas para la protección de la información y de los sistemas de procesamiento de la misma contra su uso no autorizado, modificación, divulgación y destrucción accidental o intencionada. Los métodos para la protección de la información variarán, aunque puede que incluyan actividades como auditorías periódicas de los sistemas.

2.2. Concejalías a cargo: las Concejalías responsables (Nuevas Tecnologías y Recursos Humanos) estarán a cargo del servicio de gestión de los activos informáticos, telemáticos, de comunicaciones, telecomunicaciones, y, en general, aquellos que se encuadran en las llamadas Tecnologías de la Información y de las Comunicaciones (TIC).

2.3. Usuarios del servicio. Son usuarios de los servicios y recursos informáticos del Ayuntamiento de Villa del Prado en sus distintas modalidades:

- a) Todos los empleados públicos municipales y miembros de la Corporación.
- b) Toda persona que, en virtud de un convenio o de una autorización emitida por el órgano competente, resulten habilitados para ello.
- c) Cualquier persona que preste servicios para los cuales requiera el uso o acceso a la red informática del Ayuntamiento de Villa del Prado.

En cualquier caso el uso de los servicios y recursos informáticos se condiciona a la existencia del vínculo con el Ayuntamiento de Villa del Prado o la autorización expresa de este.

2.4. Las cuentas de usuario: la utilización de estos servicios se realiza a través de cuentas personales e intransferibles creadas para tal fin en los distintos servidores y equipos del Ayuntamiento de Villa del Prado. Las cuentas asignadas a título personal son intransferibles, por lo que está prohibido el uso de cuentas por personas ajenas a su titular (con conocimiento o no de los usuarios oficiales).

2.5. Uso de tarjetas, certificados y DNIE: en los términos previstos en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y su normativa de desarrollo, los empleados podrán ser requeridos a la utilización de tarjetas, llaves USB u otros soportes que incorporen certificados digitales para autenticar los procesos en los que intervengan. La custodia de estos elementos será análoga a la que se realiza con las claves y contraseñas.

2.6. Conexión de equipos a la RIMVDP: queda prohibida la conexión de equipos informáticos a la red informática municipal. El personal responsable habilitará las conexiones previamente autorizadas por escrito observando en todo momento las medidas contempladas en este reglamento y otras adicionales que pudieran establecerse.

Art. 3. *Condiciones en que se prestan los servicios.*—3.1. Retención de información sobre el tráfico generado y el uso de los servicios: el registro de tráfico y uso de los sistemas que se realicen para estadísticas de uso y mantenimiento no podrá ser utilizado con otros fines, excepto en caso de mandato judicial. Cualquier otro archivado de accesos, tráfico de red, conexiones, envíos, etcétera, requerirá estar amparado en una ley, reglamento o petición judicial.

Se respetará en los términos establecidos por las normas la privacidad del contenido de los mensajes de correo electrónico, sin menoscabo de la capacidad del Ayuntamiento de Villa del Prado para la aplicación sistemática de programas de detección y eliminación de virus o “software” malintencionado y programas de filtro de correo no deseado (llamado en inglés “anti-spam”) a los mensajes que llegan al servidor de correo municipal.

Asimismo, el Ayuntamiento de Villa del Prado, en cumplimiento de lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, podrá realizar el seguimiento de todos los accesos que sus usuarios realicen o intenten realizar a los ficheros con datos personales cuya titularidad corresponda al Ayuntamiento de Villa del Prado, para poder determinar en caso de un mal uso de los mismos las posibles responsabilidades de sus usuarios.

3.2. Compromiso de confidencialidad con relación a los servicios de la RIMVP: todos los usuarios incluidos en el ámbito de aplicación de este Reglamento que por su trabajo tengan acceso al contenido almacenado en los recursos que dan soporte a los servicios deben cumplir con la obligación de secreto y confidencialidad.

3.3. Seguridad y funcionamiento de los bienes y servicios informáticos: en virtud de los principios de responsabilidad y autoprotección, los usuarios deberán adoptar todas aquellas medidas que garanticen la seguridad del sistema informático del Ayuntamiento.

Art. 4. *Responsabilidades y normas de acceso a los equipos informáticos.*—4.1. Responsabilidad corporativa: las Concejalías responsables deberán adoptar las medidas oportunas para que todo el personal tenga conocimiento y cumpla las disposiciones contenidas en este Reglamento.

- 4.1.1. Supervisión y evaluación: las Concejalías responsables tienen la autoridad y responsabilidad de supervisar y evaluar el uso de los recursos informáticos corporativos y asegurar el cumplimiento de este Reglamento y sus normas relacionadas.
- 4.1.2. Provisión de códigos de acceso: los administradores del sistema deben facilitar tantos códigos o identificaciones de acceso, y sus correspondientes claves, a cada usuario para acceder a los sistemas informáticos que requiera para su trabajo. La Identificación Personal y las claves de acceso deberán ser confidenciales.

4.2. Del usuario: el usuario es responsable exclusivo del uso que realice de los servicios y recursos ofrecidos por la RIMVDP y de la custodia de sus claves de acceso.

Al usuario se le imputarán todas las acciones llevadas a cabo a través de ellas. Sin embargo, las claves de acceso no implican que el acceso del usuario y las comunicaciones realizadas a través de los sistemas propiedad del Ayuntamiento sean privados.

- 4.2.1. Prohibición de cesión de claves: está prohibido compartir la Identificación Personal y las claves de acceso, a excepción de circunstancias extremas y solo con autorización de las Concejalías responsables.
- 4.2.2. No transmisión de claves: las Identificaciones Personales y las claves de acceso no deben ser enviadas por correo o archivadas en un lugar visible o accesible por otros.
- 4.2.3. Información de problemas de seguridad: el usuario debe notificar inmediatamente a las Concejalías responsables cualquier uso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad. Asimismo, el usuario debe asegurarse de bloquear el equipo al ausentarse del mismo.
- 4.2.4. Uso de los recursos: los equipos no deben presentar configuraciones ni operar con “software” o dispositivos que causen problemas en la red o a otros equipos conectados a ella.
- 4.2.5. Prohibición de transmitir los servicios y recursos: queda prohibida la cesión o transmisión a terceros en cualquier forma de los servicios y recursos informáticos del Ayuntamiento, salvo autorización expresa del órgano competente.

Art. 5. *Autorizaciones y acceso remoto a ordenadores.*—5.1. Autorizaciones de uso a empleados por parte de sus responsables: los empleados o usuarios que requieran la utilización de cualquier elemento o servicio que forme parte de la RIMVDP o cualquiera de los otros sistemas regulados en este Reglamento deberán solicitar autorización a sus responsables directos.

5.2. Acceso remoto a ordenadores: las Concejalías responsables implementarán en los equipos “software” para el acceso remoto a los terminales que permita realizar tareas de soporte o mantenimiento de forma remota a los equipos y usuarios respectivamente, evitando desplazamientos innecesarios de los técnicos municipales y ganar así en eficiencia y optimización de recursos.

El “software” empleado para el acceso remoto deberá permitir en la medida de lo posible acceder a un perfil de usuario diferente y propio para el soporte remoto. En caso de no ser posible o ser necesario acceder dentro del perfil del usuario que está utilizando el equipo se deberá solicitar la autorización del mismo o de su responsable. El programa deberá mostrar un mensaje advirtiendo de la conexión con el objeto de advertir al usuario de que se está produciendo un acceso remoto al equipo y por tanto, el contenido de la pantalla y los documentos podrían ser observados por el usuario del control remoto.

Art. 6. *Usos incorrectos de los recursos.*—1. Queda prohibido cualquier uso contrario al presente Reglamento, así como a cualesquiera otras normas y condiciones de uso de los servicios y recursos informáticos establecidas por el Ayuntamiento de Villa del Prado o demás normativa de aplicación en esta materia.

En todo caso, se considera incumplimiento de las normas de uso de recursos informáticos y servicios de la RIMVDP los supuestos siguientes:

- a) Exceder los servicios para los cuales se autorizó la cuenta.
- b) La búsqueda de claves de acceso de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos del Ayuntamiento de Villa del Prado o de fuera de ella, o hacer uso de aquellos sistemas para atacar cualquier sistema informático.
- c) Intentar acceder a la información de otro usuario que no haya sido puesta explícitamente de acceso público.
- d) La creación, uso o almacenamiento de programas o de información que puedan ser utilizados para atacar los sistemas informáticos del Ayuntamiento de Villa del Prado o de fuera, en especial los programas de escucha del tráfico de red o de escaneo de puertos.
- e) La introducción intencionada de virus, troyanos, gusanos o cualquier otro “software” perjudicial o nocivo para el correcto funcionamiento de los sistemas informáticos del Ayuntamiento de Villa del Prado.
- f) El empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.

- g) Interferir o interrumpir los servicios, servidores, o redes conectadas a los servicios, o desobedecer cualquier requisito, procedimiento, política o regulación de redes conectadas a los servicios.
 - h) Almacenar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir contenido ilegal de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, atentatorio contra los derechos humanos o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
 - i) Difusión de contenidos personales o partidistas o de contenidos que excedan o sean impropios de la actividad que corresponde a cada usuario.
 - j) Cargar, almacenar, publicar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir algún contenido que viole alguna patente, marca, secreto comercial, derecho de autor o cualquier derecho de propiedad.
 - k) Difusión de mensajes de correo electrónico sin identificar plenamente a su remitente. En el caso de que la cuenta de correo sea utilizada por grupos de usuarios, deberá identificarse el autor.
 - l) Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
 - m) Utilización de los servicios para fines comerciales o publicitarios sin autorización expresa; así pues, los contenidos publicados no pueden contener texto, sonido, imágenes o enlaces de esta naturaleza ni tan solo a título informativo.
 - n) El envío masivo de mensajes de correo o información que consuma injustificadamente recursos del Ayuntamiento de Villa del Prado y su red informática.
 - o) Manipular las cabeceras de los mensajes de correo para intentar ocultar o falsear la identidad del usuario remitente del mensaje.
 - p) Instalar o usar servidores o encaminadores de correo que no cuenten con la autorización del Ayuntamiento de Villa del Prado.
 - q) Utilizar agentes, “proxies”, etcétera, externos no autorizados con el fin de ocultar la identidad.
 - r) Utilización de las redes sociales con fines particulares y en horario laboral.
2. No se consideran usos incorrectos las acciones técnicas de mantenimiento realizadas por el personal competente para garantizar la seguridad y operatividad de los sistemas informáticos del Ayuntamiento.

Art. 7. *Supervisión de la Red Informática Municipal de Villa del Prado.*—Las comunicaciones y actividades llevadas a cabo mediante sistemas de la propiedad del Ayuntamiento serán supervisadas periódicamente para garantizar la correcta utilización de dichos sistemas.

Las actividades de supervisión serán llevadas a cabo cuando un responsable tenga sospechas fundadas que pueda requerir la investigación del uso, por parte del usuario, de los sistemas de información del Ayuntamiento, y siempre de acuerdo a los demás artículos del presente documento y leyes relacionadas.

Capítulo II

Utilización de los elementos de la Red Informática Municipal de Villa del Prado

Art. 8. *Los equipos de cliente.*—La inclusión física en la RIMVDP será realizada por las Concejalías responsables, así como cualquier modificación en la misma.

Art. 9. *Utilización de programas informáticos.*—9.1. “Software” autorizado: como norma, solo podrá ser utilizado “software” que esté homologado oficialmente por el Ayuntamiento de Villa del Prado, para asegurar su compatibilidad y para minimizar el tiempo de respuesta de soporte.

Art. 10. *Licencias de “software”.*—10.1. Necesidad de licencia: todos los programas informáticos instalados en los ordenadores del Ayuntamiento deben tener la licencia correcta.

10.2. Eliminación de “software”: las Concejalías responsables retirarán cualquier “software” sin licencia o que incumpla las leyes o normas de seguridad sin previo aviso.

10.3. Propiedad del “software” propio: todos los programas informáticos desarrollados por los empleados o personal subcontratado, en nombre del Ayuntamiento, son de propiedad del Ayuntamiento y están protegidos bajo la ley de los derechos de propiedad intelectual, contra su uso no autorizado o duplicación.

Art. 11. *Modificación de la configuración de los equipos.*—11.1. Autorización para la modificación: los usuarios no podrán cambiar la configuración de los equipos informáticos del Ayuntamiento de Villa del Prado, instalados y configurados.

Art. 12. *Copias de seguridad de equipos.*—El servicio encargado de las copias de seguridad y su custodia no realizará ninguna tarea en equipos de usuario.

En caso de pérdida de información en los equipos de los usuarios, estos serán los únicos responsables de esta pérdida de datos. Es de obligado cumplimiento que los datos referentes al trabajo diario se guarden en los servidores destinados para ello, especialmente los que requieran seguridad o copia de respaldo.

Capítulo III

Uso del correo electrónico del Ayuntamiento de Villa del Prado

Art. 13. *Normas generales.*—Los sistemas de correo electrónico facilitados o utilizados en el Ayuntamiento de Villa del Prado solo podrán ser usados para los fines relacionados con el puesto de trabajo o tareas propias del usuario, tal y como recoge el artículo 6 del presente Reglamento.

13.1. Control de las cuentas de correo: los correos entrantes no serán tenidos en cuenta y el Ayuntamiento habilitará todas las medidas necesarias en la medida de sus posibilidades para que estos no contengan contenido inapropiado.

13.2. Contenido de los mensajes: el uso de los sistemas de correo electrónico del Ayuntamiento es una herramienta de trabajo. La mala utilización de dichos sistemas podrá ser la causa de la pérdida de tal instrumento y/o acciones disciplinarias. Son supuestos de abusos, entre otros, cuya realización puede ser objeto de sanción disciplinaria:

- a) Utilización del correo electrónico para información no relacionada con el trabajo (envío de cartas en cadena, publicidad personal de artículos para vender y envío de dibujos de humor inoportunos).
- b) Utilización del correo electrónico para la transmisión de material incompatible con cualquier procedimiento del Ayuntamiento (ejemplo: acoso sexual, discriminación, etcétera).
- c) Utilización o acceso a la cuenta de correo de otro usuario y/o material, sin la previa autorización del Área de Nuevas Tecnologías.
- d) Distribuir información que pueda ser confidencial del Ayuntamiento. El uso del correo electrónico para el envío de información técnica no exime al remitente ni al receptor del cumplimiento de la normativa aplicable.

Art. 14. *Prohibición de abuso en el correo electrónico (ACE).*—14.1. Prohibición del abuso. Está prohibido cualquier uso del correo electrónico, cuando sea:

- a) Abusivo por el contenido: enviar, almacenar o distribuir mensajes cuyo contenido atente contra los derechos reconocidos en las Leyes españolas y Tratados Internacionales suscritos por España o promueva actuaciones contrarias a la Ley.
- b) Abusivo por el medio: envío de correo utilizando un servidor de correo ajeno sin el consentimiento del titular del mismo.
- c) Abusivo por no solicitado: envío de comunicaciones electrónicas a una pluralidad de receptores que no las hayan solicitado (“spam”) a excepción del expresamente autorizado por el Ayuntamiento de Villa del Prado.
- d) Abusivo por su finalidad: envío de mensajes de correo electrónico cuyo único propósito sea el de sobrecargar, paralizar o, de cualquier otro modo, perjudicar el normal uso de este servicio o los equipos informáticos de otros usuarios de Internet.

El envío de correo masivo o difusión masiva de mensajes y el envío continuo de un número elevado de mensajes quedan asimismo limitados. Desde el momento en el que se detecte que dichas actividades perjudican el correcto funcionamiento de los servicios y/o provoquen retrasos en las entregas de correo de los demás usuarios de los sistemas, adoptará las medidas que considere necesarias, ya sea bloqueando direcciones IP, dominios, usuarios u otras medidas, pudiendo incluso procederse a la suspensión del servicio.

Art. 15. *Protección de los sistemas de correo electrónico.*—15.1. Cuentas autorizadas: las únicas cuentas de correo que pueden utilizar los usuarios comprendidos en el ámbito de aplicación de este Reglamento para las labores derivadas de su puesto son las proporcionadas por las Concejalías responsables.

15.2. Acceso no autorizado: está prohibido el uso de claves de acceso no autorizadas y la utilización de códigos para obtener el acceso al correo electrónico de otros usuarios, salvo en aquellos casos que las Concejalías responsables.

15.3. Correo electrónico por Internet: está prohibida la utilización de los servicios particulares y personales de correo electrónico para la correspondencia del Ayuntamiento, salvo en los casos que las Concejalías responsables lo autoricen. El correo electrónico de Internet u otros sistemas públicos de correo electrónico, no deben ser usados para transmitir información, o datos, que sean considerados confidenciales, de propiedad industrial o que no puedan ser divulgados públicamente. El correo electrónico no debe ser utilizado como método seguro de comunicación para información confidencial.

15.4. Uso indebido del correo electrónico. Se consideran “uso indebido del correo electrónico” las siguientes prácticas:

- a) Derivar el correo electrónico del Ayuntamiento a una cuenta pública de correo electrónico.
- b) Utilizar el correo electrónico como una utilidad de transmisión de ficheros.
- c) Derivar mensajes para permitir a otros la lectura de los mensajes personales.
- d) Permitir a otros empleados el uso de la propia cuenta del correo electrónico.
- e) Utilizar la cuenta para enviar texto y archivos adjuntos que no se correspondan con la labor a desarrollar por el usuario.

Capítulo IV

Acceso a Internet

Art. 16. *Uso de los accesos a Internet.*—16.1. Responsabilidad del empleado: el acceso a Internet debe ser utilizado con responsabilidad y siempre para usos relacionados con las tareas propias del trabajo del usuario. El incumplimiento será constitutivo de infracción o falta en los términos recogidos en el presente Reglamento.

16.2. Supervisión: el Ayuntamiento podrá revisar todos los accesos a Internet que pertenezcan a su sistema, ejerciendo así el derecho reconocido de control sobre los equipos y el uso que se les da.

La supervisión general del tráfico con el fin de controlar los sistemas en su seguridad y calidad no se considerará personalizada y podrá ser ejercida por los técnicos de las Concejalías responsables sin previo aviso.

16.3. Filtrado de contenidos: para evitar el acceso a páginas no necesarias para el trabajo habitual y protección de los sistemas del Ayuntamiento de “software” malicioso se proveerán sistemas de filtrado de contenidos, gestores de ancho, cortafuegos y tanto sistemas de seguridad como se consideren necesarios para interceptar el tráfico no deseado ni autorizado.

Art. 17. *Uso indebido de los accesos a Internet.*—El uso del sistema de acceso a Internet es una herramienta de trabajo. La mala utilización de dicho sistema podrá dar lugar a la adopción de las medidas previstas en este Reglamento.

Son supuestos de abusos, o usos indebidos:

- a) Utilización de los servicios de Internet para fines ilegales.
- b) La utilización del nombre de otra persona, clave de acceso, teclas de seguridad, archivos, datos o falsificar la identidad de otros usuarios, compañías o administraciones.
- c) Utilizar programas de ordenador o instrumentos para desviar, destruir o impedir cualquier medida de seguridad en todo el sistema de la red.
- d) Tomar parte, intencionalmente, en cualquier actividad que pudiera causar daños a los sistemas informáticos de la red o a los archivos almacenados. Incluyendo, pero no limitándose a la propagación de virus, ya sea destruyendo archivos, interrumpiendo o denegando el acceso al sobrecargar intencionalmente los sistemas principales de la red informática.
- e) Utilizar los sistemas del Ayuntamiento para fines comerciales.
- f) La descarga de paquetes informáticos sin licencia para realizar pruebas o su utilización en el Ayuntamiento. Todos los programas informáticos deben ser evaluados y homologados por las Concejalías responsables.
- g) La utilización de equipos del Ayuntamiento para instalar programas lúdicos o juegos a través de Internet.
- h) Cargar o descargar gráficos, imágenes u otros materiales que sean inapropiados y no estén relacionados con las tareas en el Ayuntamiento.

- i) Vender o distribuir programas informáticos a través de Internet para el beneficio personal.
- j) Remitir o cargar información confidencial del Ayuntamiento a algún servicio de Internet que pueda ser interceptado.
- k) Almacenar, remitir, mostrar, transmitir intencionalmente o intercambiar programas informáticos ilegales o claves de acceso de las que no se disponga la licencia pertinente en propiedad.
- l) Almacenar, remitir, mostrar, transmitir intencionalmente o intercambiar material indecente u obsceno.
- m) Almacenar, remitir, mostrar, transmitir intencionalmente o intercambiar material protegido por derechos de autor, “copyrights” o cualquier otra protección legal.
- n) Cualquier otro supuesto de uso de los servicios de Internet que sean contrarios a las disposiciones de este Reglamento.

Capítulo V

Servidores informáticos del Ayuntamiento de Villa del Prado e incorporación de nuevas aplicaciones

Art. 18. *Copias de seguridad de servidores.*—18.1. Ubicación de los archivos con copia de seguridad requerida: se realizarán copias de seguridad de los datos que residan en los servidores municipales. La copia se hará de los datos almacenados en los servidores, de forma que toda información referente al trabajo diario de los usuarios deberá estar almacenada en dichos servidores y no en los equipos locales. Por ello, todo dato que por cualquier motivo tenga obligación de mantener una copia de seguridad será alojado en una carpeta autorizada del servidor que corresponda.

Art. 19. *Carpetas y archivos en servidores.*—19.1. Usos de las carpetas departamentales: las carpetas departamentales no podrán ser usadas para otras funciones que no sean las ya indicadas. Nunca deben dedicarse o usarse como:

- a) Copia de seguridad de los datos del disco duro propio.
- b) Copia de seguridad del correo electrónico.
- c) Lugar de intercambio de archivos.
- d) Copia de seguridad de las propias carpetas departamentales o de las de otros departamentos.
- e) Alojamiento de “software” para instalar.
- f) Alojamiento de archivos bajados de Internet, a no ser que sean necesarios para el trabajo.
- g) Alojamiento de grandes archivos de vídeo, música, etcétera.
- h) En general, no se alojarán archivos que no cumplan, al menos, una de estas tres características: requieran ser compartidos, deban disponer de copia de seguridad o deban ser protegidos con permisos específicos.

19.2. Medios extraíbles de almacenamiento: debido a que suponen una gran amenaza como dispositivos de propagación de virus y son además un medio que facilita la extracción masiva de información, queda prohibida la utilización de medios de almacenamiento extraíbles tales como “pendrives”, discos duros externos, etcétera.

Cualquier utilización de estos dispositivos, deberá ser solicitada por escrito especificando el tipo de medio a conectar, el objeto de su utilización y el período de utilización.

Si la importancia de la información lo requiere, deberá proporcionarse sistemas de encriptado que impidan el acceso a los datos a personas no autorizadas en los supuestos por ejemplo de robo o extravío del medio.

Capítulo VI

Telefonía fija y móvil

Art. 20. *Uso telefonía fija y móvil.*—20.1. Uso adecuado: el teléfono es una herramienta para una mejor comunicación y desempeño de la labor profesional, no un medio de comunicación privado o personal, por lo que se deberá utilizar exclusivamente con una finalidad laboral.

20.2. Responsabilidad: cada usuario es responsable del terminal que se le asigne.

20.3. Imputación de las llamadas realizadas: comprobado el uso inadecuado de un terminal podrán imputarse las llamadas realizadas al usuario responsable de dicho uso.

En caso de disponer de conexión a Internet, envío de MMS, SMS, etcétera, serán considerados como llamadas a todos los efectos de responsabilidad.

20.4. Reparación de averías: cualquier avería del terminal será comunicada a las Concejalías responsables, por lo que en ningún caso se intentará arreglar dicha avería por el usuario.

Capítulo VII

Videovigilancia

Art. 21. *Videovigilancia*.—La utilización de sistemas de videovigilancia en las dependencias del Ayuntamiento de Villa del Prado persigue garantizar la seguridad de los bienes y las personas.

En este ámbito el Ayuntamiento de Villa del Prado respeta y aplica los principios contenidos en la legislación vigente y en particular la Ley 15/1999, de 13 de diciembre, Orgánica de Protección de Datos, y su Reglamento de Desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RDLOPD), y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

El uso de los sistemas de videovigilancia será respetuoso con los derechos de las personas, se notificará a la Agencia de Protección de Datos de la Comunidad de Madrid la existencia de un fichero referente a la grabación de imágenes, se informará en todo momento mediante carteles indicativos de la grabación de imágenes y no se grabarán imágenes en zonas ajenas a las instalaciones del Ayuntamiento.

Capítulo VIII

Régimen sancionador

Art. 22. *Infracciones*.—Conforme a lo previsto en el artículo 139 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, se establecen las siguientes infracciones para la adecuada ordenación del uso de los servicios y equipamientos informáticos:

1. Son infracciones muy graves:

- a) Cualquier acto de deterioro grave y relevante de equipos, instalaciones o sistemas informáticos.
- b) El impedimento o la grave y relevante obstrucción al normal funcionamiento de los sistemas informáticos, comunicación y videovigilancia del Ayuntamiento.
- c) Cualquier otra conducta que suponga el incumplimiento de las normas de este Reglamento y en la que concurra alguna de las circunstancias establecidas en el artículo 140.1 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local.

2. Son infracciones graves o leves cualquier otra conducta que infrinja las disposiciones de este Reglamento, graduándose la gravedad o levedad conforme a los criterios establecidos en el artículo 140.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local.

Art. 23. *Medidas sancionadoras*.—El incumplimiento de la presente normativa podrá dar lugar a la suspensión temporal o privación definitiva del uso de la Red Informática Municipal y los medios que esta pone a disposición de los usuarios a que se refiere este Reglamento, sin perjuicio de las sanciones establecidas en el apartado siguiente y de las responsabilidades disciplinarias y de cualquier otro tipo en que se hubiere incurrido.

El órgano competente del Ayuntamiento podrá imponer multas por infracción de este Reglamento en las cuantías siguientes:

- Infracciones muy graves: hasta 3.000 euros.
- Infracciones graves: hasta 1.500 euros.
- Infracciones leves: hasta 750 euros.

Las sanciones a aplicar a los empleados municipales por medio del procedimiento disciplinario apropiado, que traigan como causa el incumplimiento de lo previsto en el presen-

te Reglamento, se regirán por la normativa de régimen disciplinario aplicable al personal municipal.

DISPOSICIÓN ADICIONAL

Primera. *Comisión Especial*.—Se creará una comisión que se reunirá en casos especiales para velar por el cumplimiento y la aplicación del presente Reglamento, compuesta por:

- a) El concejal de Recursos Humanos.
- b) El concejal de Nuevas Tecnologías.
- c) Un técnico informático, perteneciente a la Concejalía de Nuevas Tecnologías.
- d) El secretario general de la Corporación.
- e) Un representante de los trabajadores.
- f) Un representante de cada grupo político.

DISPOSICIÓN FINAL

Primera. *Entrada en vigor*.—Este Reglamento entrará en vigor al día siguiente de su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

Contra el presente acuerdo se interpondrá recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid en el plazo de dos meses, a contar desde el día siguiente a la publicación del presente anuncio, de conformidad con el artículo 46 de la Ley 29/1998, de 13 de julio, de la Jurisdicción Contencioso-Administrativa.

En Villa del Prado, a 8 de mayo de 2012.—La alcaldesa, Belén Rodríguez Palomino.

(03/16.712/12)