III. ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE

91 MORATA DE TAJUÑA

ORGANIZACIÓN Y FUNCIONAMIENTO

El Ayuntamiento de Morata de Tajuña, en sesión de Pleno celebrada el día 6 de agosto de 2020, aprobó inicialmente el Reglamento Municipal Regulador para el Uso Seguro de Medios Tecnológicos del Ayuntamiento de Morata de Tajuña, sin que durante el período de exposición al público se hayan presentado reclamaciones o sugerencias, haciéndose público el contenido íntegro del mismo mediante la inserción del presente anuncio en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID:

REGLAMENTO MUNICIPAL REGULADOR PARA EL USO SEGURO DE MEDIOS TECNOLÓGICOS DEL AYUNTAMIENTO DE MORATA DE TAJUÑA (MADRID)

Capítulo I

Disposiciones preliminares

Artículo 1. *Objeto*.—La presente normativa tiene por objeto regular la norma de uso seguro de los medios tecnológicos que forman parte de los sistemas de información del Ayuntamiento de Morata de Tajuña, con el fin de minimizar la probabilidad de la materialización de las amenazas que ponen en riesgo la seguridad de los sistemas de información.

Art. 2. *Ámbito de aplicación*.—1. En el ámbito de la presente normativa, se entiende por usuario a cualquier persona que utilice o posea acceso a los medios tecnológicos puestos a su disposición por el Ayuntamiento de Morata de Tajuña.

2. Las normas enunciadas serán de obligado cumplimiento para todos los usuarios definidos en el punto anterior.

3. Sus contenidos desarrollan las directrices de carácter general definidas en la política de seguridad de la información, teniendo en cuenta que se podrán definir normas restrictivas en ciertos ámbitos específicos que lo precisen.

Art. 3. *Principio general de actuación*.—La seguridad de la información depende de todas las personas que participan en su tratamiento y compromete a todas las que integran la organización. Todos los usuarios se comprometen a hacer un uso correcto de todos los activos que requieran para el desarrollo de sus funciones, a respetar las medidas de seguridad que se establezcan y a notificar lo antes posible a los responsables que corresponda de los eventos y puntos débiles de la seguridad de la información que detecten, de manera que puedan emprenderse las acciones oportunas.

Art. 4. *Definiciones*.—A los efectos previstos en esta normativa, las definiciones, palabras, expresiones, y términos han de ser entendidos en el sentido indicado en la normativa de protección de datos de carácter personal, en el esquema nacional de seguridad y en el glosario incluido en el Anexo.

Capítulo II

Normas generales

Art. 5. *Tratamiento de la información*.—1. El Ayuntamiento de Morata de Tajuña será responsable del tratamiento de la información en cualquier medio tecnológico que forme parte de sus sistemas de información y redes de comunicaciones, y adoptará las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos.

2. Quienes por razón del ejercicio de sus funciones accedan a información que no sea de acceso público, deberán observar la necesaria reserva, confidencialidad y sigilo, incluso después de haber cesado en sus funciones o finalizado la relación contractual o laboral.

3. Quienes traten información que no haya sido clasificada de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente imprescindibles para desempeñar su cometido.

BOCM-20210215-91

4. Queda prohibido, asimismo, transmitir o alojar información propia del Ayuntamiento de Morata de Tajuña en sistemas de información externos, salvo autorización expresa del organismo responsable del tratamiento de la información, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre el Ayuntamiento de Morata de Tajuña y la empresa responsable de la prestación del servicio, incluyendo los acuerdos de nivel de servicio que procedan, el correspondiente acuerdo de confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

Art. 6. *Propiedad y uso de los medios tecnológicos*.—1. Todos los medios tecnológicos puestos a disposición de los usuarios: ordenadores personales y portátiles, aplicaciones, programas, sistemas de impresión y escaneo de documentos, dispositivos móviles, el acceso a la red corporativa y a internet, son propiedad del Ayuntamiento de Morata de Tajuña.

2. El Ayuntamiento de Morata de Tajuña le proporcionará a cada usuario un puesto de trabajo con los medios tecnológicos necesarios para el desempeño de las funciones encomendadas.

3. Dichos medios no están destinados al uso personal, y no podrán utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento del Ayuntamiento de Morata de Tajuña o sean contrarias a los intereses de esta.

4. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los medios tecnológicos, salvo autorización expresa del organismo con competencias en tecnologías de la información. En todo caso, estas operaciones solo podrán realizarse por el personal de soporte técnico autorizado.

5. La instalación, utilización o conexión a la red corporativa de cualquier medio tecnológico ajeno, requerirá una autorización previa por parte de la Concejalía competente en materia de tecnologías de la información que corresponda.

6. Está estrictamente prohibida la ejecución de programas informáticos en los medios tecnológicos que forman parte de los sistemas de información del Ayuntamiento de Morata de Tajuña sin la correspondiente licencia de uso y autorización correspondiente del organismo con competencias en tecnologías de la información.

7. Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

Art. 7. *Identificación de acceso*.—1. La identificación de acceso a cualquier medio tecnológico será personal e intransferible, permitiendo una identificación individual.

2. Los usuarios deben custodiar convenientemente su identificación de acceso, son responsables de toda la actividad relacionada con el uso de su acceso personal autorizado, y en ningún caso podrá ser suministrada a terceras personas.

3. Si un usuario tiene sospechas de que su identificación de acceso está siendo utilizada por otra persona, deberá comunicar inmediatamente al organismo con competencias en tecnologías de la información la correspondiente incidencia de seguridad.

4. Los usuarios deben utilizar contraseñas seguras de acuerdo con la política de contraseñas definida por la Concejalía con competencias en materia de tecnologías de la información (Anexo II).

Art. 8. *Notificación de incidencias*.—1. Una incidencia de seguridad en un sistema, la constituye cualquier situación o eventualidad en la que pueda verse amenazada la información, y pueda en consecuencia dar lugar a una pérdida de: confidencialidad, integridad, disponibilidad y autenticidad.

2. Todos los usuarios están obligados a notificar cualquier incidencia de seguridad a través del procedimiento establecido a tal efecto (Anexo III).

Art. 9. *Implantación de medidas técnicas*.—El personal que realiza funciones en materia de tecnologías de la información, adoptará las medidas técnicas adecuadas al nivel de seguridad establecido para cada tratamiento de la información y en la prestación de los servicios, por el responsable designado en la organización de la seguridad.

Art. 10. *Borrado y destrucción de soportes de información*.—1. Se destruirán de forma segura los soportes de información que vayan a ser desechados.

2. Los soportes de información que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.

Art. 11. *Inspección de los medios tecnológicos*.—La Concejalía competente en materia de tecnologías de la información establecerá por razones específicas de seguridad o de evaluación del desempeño, medidas de control y comprobará mediante los mecanismos formales y técnicos que estime oportunos, la correcta utilización por parte de los usuarios de todos los medios tecnológicos puestos a su disposición para el desempeño de sus funcio-

BOCM-20210215-91

nes. Estos controles y revisiones se realizarán respetando los principios de necesidad, idoneidad y proporcionalidad, preservando las garantías del derecho a la intimidad del usuario y la seguridad de las comunicaciones.

Art. 12. *Cese de actividad.*—1. El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al organismo con competencias en tecnologías de la información.

2. Cuando se modifiquen las circunstancias profesionales que originaron la entrega de un medio tecnológico, el usuario lo devolverá al organismo con competencias en tecnologías de la información, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

Art. 13. *Copias de seguridad.*—La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad de la Concejalía competente en materia de tecnologías de la información. Cada usuario será responsable de la integridad y copia de seguridad de la información almacenada en el medio tecnológico que tenga asignado.

Art. 14. *Acceso desde el exterior.*—Solo está permitido acceder desde el exterior de la RCAM (Red Corporativa del Ayuntamiento de Morata de Tajuña) a recursos internos previa autorización de la Alcaldía-Presidencia.

Art. 15. *Incumplimientos.*—El incumplimiento de las normas de uso expresadas podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

Capítulo III

Medios tecnológicos

Art. 16. *Ordenadores personales de sobremesa.*—1. No está permitido alterar la configuración hardware de los equipos ni conectar otros dispositivos a estos a iniciativa del usuario, así como variar su ubicación.

2. No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas distintos a la configuración establecida por el organismo con competencias en tecnologías de la información.

3. Es obligatorio bloquear la sesión del usuario en el supuesto de ausentarse temporalmente del puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Asimismo, es obligatorio apagar el equipo al terminar la jornada laboral.

4. El almacenamiento de ficheros generados en el desempeño de las competencias profesionales del usuario, se efectuará en la carpeta habilitada en la red informática, a fin de facilitar la realización de copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.

5. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos.

6. No está permitido copiar, extraer o transmitir información contenida en el sistema informático para uso privado o para cualquier otro distinto del servicio público al que está destinada.

7. Los ficheros temporales deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática.

Art. 17. *Equipos portátiles.*—1. Todas las responsabilidades aplicables a los ordenadores de sobremesa son de aplicación para los equipos portátiles.

2. Responsabilidades adicionales específicas de los equipos portátiles:

a) Con carácter general, no se almacenará información sensible o confidencial en este tipo de equipos, y en caso de ser necesario, deberá ser protegida mediante herramientas de cifrado.
b) Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. No se dejará el equipo portátil desatendido o abandonado en lugares donde pueda ser sustraído con facilidad.
c) Los usuarios de estos equipos se responsabilizarán de que no serán usados por usuarios no autorizados.
d) La pérdida o robo de cualquier dispositivo o equipo portátil deberá notificarse de inmediato al organismo con competencias en tecnologías de la información.
e) No deberán conectarse directamente a redes ajenas.

BOCM-20210215-91

f) Deberá estar desactivada la búsqueda de redes inalámbricas.

3. Los usuarios de equipos portátiles deberán realizar conexiones periódicas al menos mensuales a la red corporativa, según las instrucciones proporcionadas por el organismo con competencias en tecnologías de la información, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.

4. Sobre los ordenadores portátiles se adoptarán las medidas técnicas adecuadas al nivel de seguridad establecido atendiendo al tratamiento de la información que vaya a efectuar.

Art. 18. *Impresoras, fotocopiadoras, escáneres, faxes y equipos multifunción.*—1. Es obligatorio el uso de buzones de impresión con clave de acceso, en los dispositivos multifunción compartidos que lo permitan.

2. Cuando se imprima documentación, esta deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

3. Se deberán recoger los originales de la fotocopiadora, impresora, escáner o equipos multifunción una vez finalizado el proceso de copia o digitalización.

Art. 19. *Dispositivos móviles.*—1. Todas las responsabilidades de uso específicas de los equipos portátiles, también lo son para los dispositivos móviles.

2. Es obligatorio configurar el dispositivo móvil para que pasado un tiempo de inactividad pase automáticamente a modo de suspensión y se active el bloqueo de la pantalla.

Art. 20. *Dispositivos de almacenamiento removibles autorizados.*—1. Los dispositivos de almacenamiento removibles autorizados serán los proporcionados por el Ayuntamiento de Morata de Tajuña, serán conformes a las normas de seguridad de la organización, y serán destinados a un uso exclusivamente profesional, como herramienta de transporte de ficheros, y no como herramienta de almacenamiento.

2. En caso de ser necesario almacenar información sensible o confidencial en este tipo de dispositivo, deberá ser protegida mediante herramientas de cifrado.

3. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. No se dejará el dispositivo desatendido o abandonado en lugares donde pueda ser sustraído con facilidad.

4. La pérdida o robo de cualquier dispositivo de almacenamiento removible deberá notificarse de inmediato al organismo con competencias en tecnologías de la información.

Art. 21. *Correo electrónico corporativo.*—1. Las cuentas creadas en los servidores del Ayuntamiento de Morata de Tajuña tienen como objetivo el intercambio de mensajes propios del desempeño profesional. Queda prohibido su uso con fines comerciales, financieros o personales.

2. No están permitidos los envíos masivos, siendo rechazados los mensajes si el número máximo de destinatarios es superior al límite establecido por la Concejalía con competencias en materia de tecnologías de la información.

3. Queda totalmente prohibido suplantar la identidad de una persona a través del correo electrónico.

4. No se permite el uso de cuentas de correo distintas a las proporcionadas por el Ayuntamiento de Morata de Tajuña dentro de la RCAM, salvo autorización expresa de la Concejalía con competencias en materia de tecnologías de la Información.

5. Los usuarios no deben enviar mensajes con información sensible tanto en el cuerpo del mensaje como en los archivos adjuntos. Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información sea inteligible o manipulada por terceros (cifrado y firma electrónica).

6. El correo electrónico es una de las fuentes más importantes de difusión de virus, por lo que se recomienda no abrir mensajes recibidos de remitentes desconocidos.

7. Para garantizar la identidad del remitente los correos se firmarán digitalmente.

8. Debido al incremento y a la continua aparición de nuevos virus, son eliminados automáticamente los mensajes con anexos susceptibles de ejecución.

9. Se limitará el tamaño máximo de los ficheros adjuntos y se asignará a los usuarios un tamaño máximo de buzón, dentro de unos límites razonables.

Art. 22. *Acceso a Internet desde la RCAM.*—1. Condiciones de acceso a Internet:

a) El acceso a internet se realizará únicamente a través de la salida a internet establecida por la Concejalía con competencias en materia de tecnologías de la información utilizando los medios tecnológicos que se dispongan a tal fin.
b) El acceso a internet por otros medios, está expresamente prohibido.

BOCM-20210215-91

c) Los recursos de internet serán filtrados según su contenido a través de sistemas automatizados y cada usuario tendrá asignado un perfil de acceso en función de su puesto de trabajo, que determinará a qué tipo de contenidos podrá acceder y en qué horarios.

d) Los perfiles de acceso serán creados por la Concejalía con competencias en materia de tecnologías de la información.

2. Responsabilidad del usuario final:

a) La utilización de internet debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse toda utilización que no tenga una mínima relación con las funciones encomendadas al usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado.

b) No está permitido el acceso a páginas de contenido ofensivo, inapropiado, pornográfico, o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social.

c) No se permite la descarga desde internet de cualquier clase de programas, aplicaciones, documentos o archivos que no provengan de páginas oficiales relacionadas con el trabajo, todo ello con la finalidad de que la descarga no pueda poner en peligro los sistemas informáticos y la información que el Ayuntamiento de Morata de Tajuña custodia.

ANEXO I

GLOSARIO DE TÉRMINOS

Amenaza: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Contraseña o clave de acceso: información secreta, en general compuesta por un grupo de caracteres, utilizada para la autenticación.

Copia de seguridad o respaldo: es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Dispositivos móviles: un dispositivo móvil se puede definir como un equipo de un tamaño pequeño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

Cifrado: transformación criptográfica de datos para producir un criptograma o texto cifrado.

Equipo portátil: es aquel ordenador personal que es capaz de realizar la mayor parte de las tareas que realizan los ordenadores de sobremesa, con similar capacidad, con la ventaja de su peso y tamaño reducidos, así como su movilidad.

Identificación de acceso: proceso que limita y controla el acceso a los recursos de un sistema de información.

Información sensible: aquella, así definida por su propietario, que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o a algo.

Hardware: se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Ordenadores personales: son los equipos informáticos básicos de los puestos de trabajo, donde estarán instaladas las aplicaciones necesarias para el desempeño de las funciones y desde los que accederá el usuario a la red corporativa y a los sistemas de información.

Perfil de Acceso: limitación del acceso a los recursos exclusivamente a personas, entidades o procesos con la debida autorización.

Telefonía fija: es aquella que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales telefónicos no portables, y generalmente enlazados entre ellos o con la central por medio de conductores metálicos.

Red Corporativa del Ayuntamiento de Morata de Tajuña (RCAM): es la infraestructura común para la interconexión de las sedes del Ayto. de Morata de Tajuña, tanto a nivel de los servicios de datos como de voz, con distribución geográfica que abarca todo el municipio de Morata de Tajuña.

Red informática: sistema de comunicación que conecta ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos.

BOCM-20210215-91

Red inalámbrica: la conexión de equipos por medio de ondas electromagnéticas y sin necesidad de una conexión física mediante cables. Las redes más usuales suelen ser WIFI, Bluetooth, o infrarrojos.

ANEXO II

POLÍTICA DE CONTRASEÑAS

1. Equipos de sobremesa y portátiles:

La contraseña debe cumplir los siguientes requisitos:

— Longitud mínima de 8 caracteres.
— Debe contener mínimo una letra mayúscula, una letra minúscula y un número.
— Debe contener mínimo un carácter especial: @ (arroba),. (punto), - (guión), _ (guión bajo).

Recomendaciones:

Para que su contraseña sea segura, no utilice información personal, como su fecha de nacimiento, nombre, apellidos, etc, y no utilice palabras comunes que se encuentran en diccionarios.

Asegúrese de que su nombre de usuario y contraseña sean diferentes.

Haga combinaciones:

— Reemplace letras por números. Por ejemplo, utilice el número 3 en lugar de e, un 1 en lugar de una i o un cero en lugar de una o. Por ejemplo: S3gur1d@d (seguridad) o B13nv3n1d0 (Bienvenido).
— Cree una frase en lugar de solo una palabra, por ejemplo: MiGr@do100.
— Utilice una ortografía alternativa, como aquella de los mensajes de texto, por ejemplo: bus en lugar de autobús.

2. Telefonía móvil:

Cualquier dispositivo móvil (que lo permita) debe contener un código de desbloqueo de mínimo 4 números. También se permite el uso de patrones. Estos dispositivos deben tener activado el bloqueo automático, no siendo superior a 30 segundos.

ANEXO III

PROCEDIMIENTO DE NOTIFICACIÓN DE INCIDENCIAS

Toda incidencia o consulta debe ser reportada mediante correo electrónico al buzón cau@ayuntamientodemorata.com especificando/aportando en dicho correo la siguiente información:

— Asunto: Breve descripción del problema o consulta.
— Cuerpo del mensaje con este formato:
— Usuario: Nombre y Apellidos.
— Fecha de detección: DD/MM/AAAA.
— Hora de detección: HH:MM en formato 24 horas.
— Descripción: Descripción de la incidencia / consulta.

Se recomienda adjuntar si es posible un pantallazo para facilitar la resolución.

El presente Reglamento entrará en vigor a partir del día siguiente de su publicación definitiva en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

Morata de Tajuña, a 3 de febrero de 2021.—El alcalde, Ángel M. Sánchez Sacristán.

(03/3.783/21)

BOCM-20210215-91