AYUNTAMIENTO DE GETAFE

NORMATIVA DE USO DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE:

1. Aprobación y entrada en vigor

La presente Normativa de Uso de los Sistemas de Información (en adelante, la normativa), ha sido informada por el Comité de Seguridad de la Información y Protección de Datos Personales (en adelante, CSIPDP) del Ayuntamiento de Getafe y entrará en vigor al día siguiente de su aprobación por la Alcaldesa.

2. Objeto

Los sistemas de información son elementos básicos para el desarrollo de la actividad del Ayuntamiento de Getafe. Estos medios se ponen a disposición del usuario/a como instrumentos de trabajo para el desempeño de su actividad profesional, motivo por el cual los usuarios/as deben utilizar estos recursos de manera responsable, mediante el cumplimiento de normas, y buenas prácticas que salvaguarden la seguridad y protección de la información, los sistemas de información y los recursos tecnológicos proporcionados.

El Ayuntamiento podrá establecer normas, pautas, instrucciones, procedimientos o buenas prácticas que complementen o regulen aspectos particulares de la presente normativa, o de su aplicación en supuestos específicos, que deberán estar aprobadas por el CSIPDP.

A los efectos de aplicación de esta normativa, la información tratada en el Ayuntamiento, ha sido calificada como:

- **Uso Oficial (información confidencial):** se considerará toda aquella información de acceso restringido y cuya divulgación no autorizada, pérdida o destrucción pueda generar impactos importantes para la entidad local, siendo la siguiente:
  - Categorías especiales de datos: establecidos en el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD): origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos, salud, vida sexual, orientación sexual y en el artículo 10 del RGPD: condenas e infracciones penales.
  - Información que contenga datos personales, que, sin considerarse de categorías especiales, no sean de difusión pública.
  - Documentos en fase de desarrollo, contengan datos personales o no, que sirvan de soporte para la elaboración de los acuerdos municipales.
  - Aquellos documentos que, a criterio del usuario/a que los ha elaborado, se considere que tienen carácter “uso oficial”.
- **Interna:** se considerará toda aquella información que sólo debe ser conocida por los integrantes de la administración (todos o parte), y no por personas externas a la misma, salvo autorización expresa. En este caso, la divulgación no autorizada, pérdida o destrucción de esta información podrá generar impactos limitados para la entidad local.
- **Pública:** se considerará toda aquella información de uso general y público dentro y fuera de la entidad local. La divulgación o pérdida o destrucción de esta información no generará ningún impacto para la entidad local. (Esta información deberá contener los datos de carácter personal anonimizados o pseudoanonimizados conforme a los criterios municipales y normativa vigente.)

3. Ámbito de Aplicación

Mediante la presente normativa, el Ayuntamiento de Getafe regula el uso de los recursos tecnológicos de su sistema de información a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal tanto laboral, como funcionario del Ayuntamiento, así como aquellas personas que mantengan otra relación con la entidad local (cargos políticos, personal de confianza, becarios, personal en prácticas, colaboradores externos, etc.) los cuáles quedan sujetos a la misma, así como a los principios éticos y de buenas prácticas recomendados en la utilización de los recursos puestos a su disposición, considerando las particularidades que se describen en el Anexo I de la presente normativa.

4. Revisión y/o Actualización

El CSIPDP, es el órgano encargado de exigir el cumplimiento de la norma, así como de su revisión y actualización. En concreto, le corresponden las siguientes funciones:

- Dictar criterios generales de aplicación respecto a las dudas que puedan surgir de su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad y cumplimiento.

El CSIPDP revisará la presente normativa con una periodicidad anual, procediendo a su modificación, en caso de ser necesario. La aprobación de las modificaciones que procedan se realizarán siguiendo el procedimiento previsto en el apartado “APROBACIÓN Y ENTRADA EN VIGOR”.

En todo caso, serán objeto de revisión los siguientes puntos:

- Identificación de acciones de mejora en la gestión de la seguridad de la información.
- Adaptación a los posibles cambios normativos, tecnológicos, organizativos, etc.
- Mejoras en la gestión y protección de la seguridad de la información.

Será el CSIPDP, el órgano encargado de la custodia y divulgación de la versión aprobada de este documento. Esta normativa estará disponible en la Intranet al igual que el acceso a la formación online asociada a la misma.

5. Normas de utilización de equipamiento informático y de comunicaciones

El Ayuntamiento de Getafe pondrá a disposición del personal definido en el apartado “ÁMBITO DE APLICACIÓN” de la presente normativa, que así lo precisen, los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles (equipos de sobremesa, portátiles, smartphones, tabletas, dispositivos de almacenamiento, dispositivos de comunicaciones, periféricos, …), necesarios para el desarrollo de las funciones profesionales que tenga atribuidas.

Mediante estos equipos los usuarios/as tendrán acceso a los Sistemas de Información del Ayuntamiento de Getafe, motivo por lo que es necesario adoptar una serie de precauciones y medidas para su adecuada utilización.

Estas normas conciernen específicamente a todos los dispositivos facilitados y configurados por el Ayuntamiento para su utilización por parte de los usuarios/as, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la entidad.

5.1. Normas Generales

La Unidad de Informática, Administración Electrónica y Transparencia (en adelante UIAET), proporcionará a los usuarios/as el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones, respecto a los cuáles se observarán las siguientes normas generales:

- Los equipos deberán utilizarse únicamente para fines institucionales profesionales y como herramienta para el desempeño de las tareas encomendadas.
- Salvo autorización expresa de la UIAET (todas las peticiones dirigidas a esta unidad deberán dirigirse al Centro de Soporte), los usuarios/as no tendrán privilegios de administrador sobre los equipos.
- Únicamente el personal autorizado por la UIAET podrá distribuir, instalar o desinstalar aplicaciones informáticas (software) y equipamiento informático (hardware), o modificar la configuración de cualquiera de los equipos.
- Cuando sea necesario instalar equipos o conectarse a la red corporativa, que no hayan sido provistos por el Ayuntamiento deberá solicitarse autorización a la UIAET (*).
- Los usuarios/as deberán notificar a la UIAET, a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos (va lento, no arranca, no funciona correctamente, etc.), especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Del mismo modo, deberán comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro del mismo (Véase documento que se entrega junto con el equipamiento).
- Cada equipo deberá estar asignado a una persona o grupo de personas concreto. Tales personas son responsables de su correcto uso.
- Una vez finalizada la jornada laboral o cuando no vaya a ser necesario para el desempeño de sus funciones el usuario/a deberá proceder al **cierre de sesión** y al apagado de su equipo (sobremesa o portátil), así como a aplicar otras recomendaciones de seguridad que puedan ser indicadas por parte de la UIAET.
- Una vez finalizada la relación con el Ayuntamiento o la necesidad de utilizar un equipo o dispositivo móvil o fijo (término de una tarea, cese en el cargo, etc.), el usuario/a lo devolverá (incluyendo los accesorios y demás equipamiento facilitado: cargadores, maletines, cables, ratones, adaptadores, etc…) a la UIAET, 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 una nueva persona.
- Con carácter general no está permitido el uso equipos informáticos o dispositivos móviles propios (no corporativos), "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información municipal salvo que se disponga de autorización expresa.

(*) Si se dispone de un equipo configurado de forma excepcional en época de pandemia, es obligatorio ponerse en contacto con la Unidad de Informática, Administración Electrónica y Transparencia para proceder a su revisión.

5.2. Normas específicas para equipos portátiles y móviles

La Unidad de Informática, Administración Electrónica y Transparencia será la encargada de la asignación y distribución de los equipos portátiles, mientras que los dispositivos móviles (smartphones y tabletas) serán asignadas y distribuidas desde la Unidad de Régimen Interior.

Respecto a los equipos portátiles y los dispositivos móviles, serán de aplicación, además de las normas generales, las siguientes:

- Los equipos portátiles y dispositivos móviles estarán, en todo momento bajo la custodia de la persona que los utilice, que será la responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como del acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la UIAET para la adopción de las medidas que correspondan.
- Al igual que el resto del equipamiento proporcionado por el Ayuntamiento, deberán utilizarse únicamente para fines profesionales, especialmente cuando se usen fuera de las instalaciones de la entidad local.
- Cuando en los dispositivos o equipos se trate o almacene información “de uso oficial” o “interna”, estos deberán disponer de mecanismos de cifrado para proteger dicha información, salvo que existan limitaciones verificadas por la UIAET que impidan cumplir con esta obligación.
- Será la UIAET la encargada de implementar las medidas de cifrado en equipos portátiles y dispositivos móviles.

6. Normas para el almacenamiento de información y copias de seguridad

Para garantizar la disponibilidad de la información municipal frente a un incidente de seguridad, se han establecido políticas de copias de seguridad de todos los recursos corporativos (aplicaciones informáticas, unidades de red u otros servicios/herramientas contratados por el Ayuntamiento).

Los usuarios/as quedan obligados a almacenar en los recursos corporativos de red la información generada en el desempeño de sus competencias profesionales.

La información municipal solo deberá ser tratada utilizando soluciones ofimáticas cuando no existan aplicaciones corporativas específicas para su almacenamiento y gestión.

No está permitido el almacenamiento de información privada del usuario ni de terceros ajenos al Ayuntamiento en los recursos corporativos.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información se habrá de dirigir una petición a la UIAET. A este respecto no se realizan copias de seguridad de la información que se encuentre almacenada fuera de las aplicaciones o unidades de red corporativas, como, por ejemplo, en el escritorio, carpeta “Mis Documentos”, unidad local, etc., de los equipos de usuario.

Los recursos corporativos pueden estar sujetos a cuotas de espacio en función de las capacidades de los sistemas municipales o servicios contratados. En aquellos casos en los que el usuario/a precise de más capacidad de almacenamiento, el Responsable del usuario/a aportando la debida justificación deberá

ponerse en contacto con la UIAET que en coordinación con el Responsable del Sistema (atendiendo a las capacidades disponibles en el sistema) podrá incrementar la cuota de espacio asignada.

7. Normas de uso para soportes de almacenamiento extraíbles

Como norma general, no está autorizado en el Ayuntamiento de Getafe, el uso de soportes de almacenamiento extraíbles (memorias USB, discos duros externos, tarjetas de memoria, etc.), encontrándose los puertos USB inhabilitados. Para su utilización deberá contarse con la autorización expresa del CSIPDP o en su defecto de la UIAET.

En el caso de que se autorice su uso, habrán de observarse las siguientes normas:

- Como norma general se utilizarán soportes proporcionados por el Ayuntamiento, siendo de uso exclusivo en los puestos de usuario autorizados y destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de archivos, no como herramienta de almacenamiento.
- El uso de medios de almacenamiento extraíbles particulares requiere autorización del CSIPDP.
- Los dispositivos indicados deberán contar con mecanismos de cifrado implementados por la UIAET y su uso no está autorizado para el almacenamiento de datos personales, salvo autorización expresa del Responsable de Información y Servicios de la Unidad del usuario/a.
- Este tipo de dispositivos deberán custodiarse en lugares seguros, al objeto de prevenir robos o el acceso de terceros no autorizados.
- La pérdida o sustracción de estos dispositivos, con indicación de su contenido, deberá ponerse en conocimiento de forma inmediata de la UIAET, unidad encargada de informar al Delegado/a de Protección de Datos en caso de que hubiera almacenados o hubiera posibilidad de acceso a datos de carácter personal. Sin perjuicio de realizar por parte del usuario/a la pertinente denuncia si así fuera necesario.

7.1. Normas para el borrado y eliminación de soportes informáticos

La reutilización de medios de almacenamiento, deberá ser solicitada a la UIAT, para que proceda a su borrado seguro.

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad y, especialmente, aquellos que deban ser eliminados de forma segura para evitar accesos a dicha información, deberán ser remitidos a la UIAET, debiendo asegurarse el usuario/a que el contenido del soporte puede ser eliminado.

8. Normas respecto a la documentación impresa

8.1. Sistemas de copia/impresión

Con carácter general, deberán utilizarse los sistemas de copia/impresión (incluidos escáneres y faxes) en red corporativos. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte de la persona Responsable del usuario/a y la autorización de la UIAET.

En ningún caso el usuario/a podrá hacer uso de los sistemas de copia/impresión que no hayan sido proporcionados por el Ayuntamiento, salvo que exista autorización por parte la UIAET. En relación a los sistemas de copia/impresión y documentación impresa, el usuario/a debe seguir las siguientes directrices:

- Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en el citado formato.
- Cuando se impriman documentos, en sistemas copia/impresión comunes, éstos deberán ser retirados inmediatamente de las bandejas de salida, para evitar accesos de terceras personas.
- La tarjeta, código o PIN que sea facilitado para acceder a los sistemas de copia/impresión, serán personales e intransferibles.
- En la realización de copias de documentos y/o escaneo, así como envío de faxes, no debe olvidarse la retirada de los originales.
- Al recibir un fax, los documentos deben retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización expresa.
- En caso de encontrarse documentación catalogada como “uso oficial” (en especial, cuando se trata de datos personales) en un sistema de copia/impresión, el usuario/a intentará localizar a la persona propietaria para que proceda a su recogida inmediata. En caso de desconocer a la persona propietaria o no estar localizable, lo pondrá inmediatamente en conocimiento del Responsable de su Unidad.
- Para evitar un uso excesivo de los recursos, mejorando el impacto medioambiental en la generación de documentos en papel, y por motivos de seguridad, antes de imprimir documentos, el usuario/a debe asegurarse de que es absolutamente necesario hacerlo.
- Los sistemas de copia/impresión deben ubicarse en lugares no accesibles por el público.

8.2. Cuidado y protección de la documentación impresa

La documentación debe ser protegida, de forma que sólo tenga acceso a ella el personal autorizado. A tal efecto, el usuario/a tendrá en cuenta las siguientes medidas:

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
- Cuando no vaya a ser utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) bajo llave.
- Cuando los documentos no sean necesarios, deberán ser eliminados utilizando para ello los medios puestos a disposición por parte del Ayuntamiento (destructoras de documentos) de forma que no sea recuperable la información que pudieran contener.
- Antes de abandonar las salas de reuniones o permitir que alguien ajeno acceda a las mismas, se limpiarán adecuadamente las pizarras y se recogerán todos los documentos, cuidando de que no quede ninguna información de “uso oficial” o “interna” accesible a personas no autorizadas.

9. Protección de la propiedad intelectual

En infraestructuras municipales, queda prohibida la ejecución de aplicaciones informáticas sin la correspondiente licencia de uso.

Las aplicaciones informáticas propiedad del Ayuntamiento o licenciadas por el mismo, están protegidas por la vigente legislación sobre propiedad intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización de la UIAET.

También está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, salvo que el usuario/a disponga de la correspondiente autorización para el uso de la obra, siendo su responsabilidad tanto la solicitud de la correspondiente autorización, como el evidenciar estar en posesión de la misma.

10. Instalación de Aplicaciones

Únicamente el personal de la UIAET podrá instalar aplicaciones informáticas en los equipos de los usuarios/as, salvo que se disponga de autorización expresa por parte de esta, en cuyo caso se deberán de tener en cuenta las siguientes indicaciones:

- No se podrán instalar o utilizar aplicaciones informáticas que no dispongan de la licencia correspondiente, o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.
- Se prohíbe la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito del Ayuntamiento de las aplicaciones informáticas instaladas en los equipos que pertenecen a la entidad local.
- No se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por la UIAET especialmente aquellas relacionadas con la seguridad.

11. Acceso a los sistemas de información y a los datos tratados

Para acceder a los sistemas/recursos informáticos municipales se debe disponer de una cuenta de usuario y estar dado de alta en los servidores de dominio.

Las nuevas incorporaciones de personal serán comunicadas a la UIAET por parte de la Unidad de Recursos Humanos, siendo el Responsable del usuario/a el encargado de solicitar y autorizar el perfil necesario con el que se configuren las funcionalidades y privilegios en función de las competencias de cada usuario/a, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

La Unidad de Recursos Humanos comunicará la baja de los usuarios/as a la UIAET para proceder a la eliminación efectiva de los derechos de acceso y a los recursos informáticos asignados al mismo.

Los cambios o modificaciones en el acceso a los sistemas de información municipales dentro de una misma Unidad serán comunicados a la UIAET por parte del Responsable o Jefe de Servicio del usuario/a.

En aquellos casos en los que el usuario/a cambie de Unidad, serán retirados los privilegios actuales al usuario/a y asignados los nuevos privilegios o requisitos de acceso por la UIAET en función de la solicitud formulada por parte del Responsable de la Unidad a la que será trasladado el usuario/a.

Cuando el usuario/a esté vinculado a un contrato de servicios o prácticas, será el Responsable de la Unidad responsable del expediente, el encargado de comunicar tanto el alta, como las modificaciones o baja del usuario/a la UIAET.

Es responsabilidad del usuario/a hacer buen uso de su cuenta de usuario. En favor de la seguridad, la cuenta se podrá desactivar por la UIAET, en caso de detectar comportamientos anómalos. Las personas usuarias tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones.

Cuando el usuario/a deje de utilizar su equipo durante un cierto tiempo, deberá bloquear la sesión para evitar el acceso por parte de personas no autorizadas (suplantación de identidad). Por razones de seguridad, el equipo se bloqueará automáticamente tras un periodo de inactividad de 20 minutos, salvo que el puesto de usuario precise establecer otra configuración analizada y aprobada por el CSIPDP.

El usuario/a deberá informar a la UIAET sobre aquellas aplicaciones que haya dejado de usar para proceder a retirar los permisos de acceso a las mismas.

11.1. Identificación y Autenticación

Los usuarios/as dispondrán de credenciales nominales (código de usuario y una contraseña) para el acceso a los sistemas de información del Ayuntamiento, siendo responsables de su custodia y de toda actividad relacionada con el uso de su acceso autorizado, respecto de los que deberá observar las siguientes medidas:

- El código de usuario es único para cada persona, intransferible e independiente del equipo de usuario o terminal desde el que se realiza el acceso.
- Los usuarios/as no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. De igual modo, no deben utilizar ningún acceso autorizado de otra persona, aunque dispongan de la autorización de su titular.
- Si una persona tiene sospechas de que sus credenciales han sido vulnerados o están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar a la Unidad de Informática, Administración Electrónica y Transparencia la correspondiente incidencia de seguridad.
- No podrán establecerse en los sistemas municipales las mismas contraseñas que los usuarios/as utilizan para el acceso a servicios o herramientas en el ámbito personal.
- Los usuarios/as deben utilizar contraseñas seguras, por lo que las mismas tienen que tener una longitud mínima de 12 caracteres que incluyan letras mayúsculas y minúsculas, caracteres especiales (del tipo @, #, +, etc.) y número. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables al usuario/a (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).
- En aquellos sistemas que dispongan de doble factor de autenticación (2FA) se habilitará el mismo siempre y cuando el usuario/a disponga de los medios necesarios para validarse utilizando 2FA.
- El sistema fuerza al cambio de contraseñas periódico, al menos cada 90 días. Los sistemas que así lo permitan, forzarán el cambio de la contraseña, previo aviso con los suficientes días de antelación.

En los casos en los que no sea posible, será responsabilidad del usuario/a su cambio dentro del plazo anteriormente indicado.

- En aquellos casos en los que se proceda a suspensión temporal de la relación laboral que no implique el mantenimiento de derechos y obligaciones frente a la entidad local, se limitarán los accesos a los sistemas de información municipales según los criterios que sean establecidos por el CSIPDP.
- Por motivos de seguridad se podrá proceder a la desactivación de los accesos a los sistemas de información municipales que hayan tenido un periodo de inactividad superior al plazo establecido para el cambio de las contraseñas.

11.2. Certificados electrónicos y firma electrónica

En el uso de certificados de administración pública, los usuarios/as deberán tener en cuenta las siguientes consideraciones:

- Las herramientas de firma deben ser las corporativas y hacer uso de las mismas siguiendo las recomendaciones indicadas desde la UIAET.
- Es preciso cumplir con los términos y condiciones de uso asociados al certificado de administración pública (certificado de AP) que haya sido facilitado al usuario/a.
- Únicamente emplear el certificado de AP para la realización de gestiones relacionadas con el desempeño de las funciones y competencias profesionales, quedando prohibido su uso en el ámbito personal.
- Comunicar cualquier incidencia (uso indebido, sospecha de uso indebido, etc.), a la UIAET para gestionar su revocación, así como la posible incidencia de seguridad. (Véase documento que se entrega junto con el equipamiento).
- Los certificados deberán estar protegidos mediante contraseña salvo en aquellos casos en los que se hayan adoptado otras medidas de protección equivalentes y validadas por la UIAET.

Los certificados electrónicos personales sólo podrán ser utilizados en casos excepcionales con autorización previa del Responsable del usuario/a.

Los usuarios/as deberán utilizar únicamente las herramientas corporativas establecidas en el Ayuntamiento para la firma electrónica de documentos.

11.3. Acceso a una cuenta de un usuario/a en su ausencia o baja

Cuando sea necesario acceder a información concreta (un archivo, información, etc.) ubicada en una carpeta personal o cuenta de correo corporativa de un usuario/a, será necesario contar con la autorización expresa del mismo.

En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser autorizado por el Responsable del usuario/a. En estos casos el acceso se realizará por la UIAET conforme al procedimiento concreto de auditoría establecido.

En todos estos casos se deberá motivar la necesidad de acceso y ser comunicada a la UIAET, que procederá a la elaboración de un acta en la que se recojan todas las acciones llevadas a cabo.

12. Confidencialidad y protección de datos de carácter personal

La información contenida en los sistemas de información del Ayuntamiento es responsabilidad de la entidad local, por lo que los usuarios/as deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia entidad (persona que disponga de capacidad para autorizar). Además, deberán tener en cuenta las siguientes premisas:

- Todas las personas del Ayuntamiento, que por razón de su actividad profesional hubieran tenido acceso a información gestionada por la entidad local (documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta confidencialidad.
- Los usuarios/as sólo podrán acceder a la información necesaria para el desempeño de las funciones que tengan asignadas con las debidas autorizaciones/permisos.
- Toda información contenida en los sistemas de información del Ayuntamiento o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones que tiene encomendadas el usuario/a.
- Los derechos de acceso de los usuarios/as a la información y a los sistemas de información que la tratan, deberán siempre otorgarse en base a los principios de “mínimo privilegio posible y necesidad de conocer”.
- La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos, estando obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con el Ayuntamiento.
- Como empleado o colaborador externo deberá adecuar sus actuaciones, con la debida diligencia, a las instrucciones que reciba del Ayuntamiento, respetando el derecho a la intimidad y la protección de los datos personales de las personas con las que se relaciona, y ayudando al municipio al adecuado cumplimiento de la normativa de protección de datos personales.
- Para la comunicación o publicación de datos personales deberán tenerse en cuenta las recomendaciones y los procedimientos de anonimización o pseudoanonimización establecidos en procedimientos e instrucciones municipales.
- El tratamiento de datos personales deberá realizarse bajo alguna de las actividades de tratamiento identificadas, aprobadas y publicadas por la entidad. Si precisa tratar u operar con datos personales no recogidos en el Registro de Actividades de Tratamiento municipales, deberá ponerlo en conocimiento del/la Delegado/a de Protección de Datos para tramitar su definición, aprobación y publicación.
- Los tratamientos de datos personales dentro del ámbito de actuación municipal deben ser realizados conforme a la normativa vigente en materia de protección de datos, teniendo en cuenta lo establecido en la Política de Seguridad y Protección de Datos municipal, así como la Guía de Buenas prácticas del Pacto Digital para la Protección de las Personas de la Agencia Española de Protección de Datos.
- En el caso de los datos personales de los que sea responsable el Ayuntamiento de Getafe deban de ser operados por un tercero consecuencia de una relación contractual, convenio o relación jurídica similar, será preciso que las relaciones entre el responsable (Ayuntamiento de Getafe) y el

encargado (entidad contratada o colaboradora) se formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable, donde se regule de forma minuciosa el modelo de operar con dichos datos.

- Los usos y operaciones en los tratamientos de datos personales cuyo responsable sea el Ayuntamiento de Getafe deberán ser realizados conforme a las políticas, procedimientos, instrucciones o notas técnicas que en materia de protección de datos hayan sido aprobadas, comunicadas y publicadas por parte del CSIPDP.
- El Ayuntamiento de Getafe podrá exigir las responsabilidades derivadas de un incumplimiento de la normativa de protección de datos atendiendo a la propuesta de la autoridad de control (Agencia Española de Protección de Datos).
- En el caso de personal de terceros, el incumplimiento de las instrucciones en materia de protección de datos puede ser objeto de sanción, y el tercero responsable del personal ajeno al Ayuntamiento podrá ocupar la posición de responsable del tratamiento cuando los datos se utilicen con otra finalidad, o sin cumplir las exigencias en esta normativa referidas, debiendo responder de las infracciones que pueda cometer su personal.

13. Metadatos y datos ocultos de los documentos electrónicos

Se define metadato como toda información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan. Los metadatos son comúnmente llamados “datos sobre los datos” o “información sobre la información”.

Se define información o datos ocultos como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos programas, para su visualización. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc…) tienen integrados en sus propiedades una serie de metadatos o datos ocultos en el contenido del archivo, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, notas, etc.

Los metadatos y/o datos ocultos contenidos en los archivos pueden llegar a afectar tanto a la seguridad de la información como a la imagen del Ayuntamiento. Por ello, todo archivo que vaya a ser publicado (página web, sede electrónica, etc…), o remitido electrónicamente a un tercero, deberá ser revisado para determinar los metadatos y datos ocultos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento municipal establecido, pudiendo solicitar en caso necesario la asistencia a la UIAET.

14. Salida de información

La salida de información del Ayuntamiento de Getafe (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado, autorización que contemplará igualmente a la propia información que sale. En este caso se deberá enviar una solicitud, al Responsable de

Información y Servicios del usuario/a y una vez autorizada, realizar la salida conforme a las medidas de seguridad y procedimiento establecido para la salida de información.

Los usuarios/as no podrán sacar al exterior información del Ayuntamiento de Getafe en dispositivos de almacenamiento externo tales como (discos ópticos (CDs, DVDs), memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

15. Uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de las personas usuarias del Ayuntamiento, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Se trata de un recurso compartido por todas las personas del Ayuntamiento, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todas las personas.

Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades, motivo por el cual, se establecen las siguientes directrices con el objetivo de reducir el riesgo en el uso del correo electrónico:

- **Firma del correo:** Todos los correos salientes deberán incluir pie de firma establecido en el Ayuntamiento de Getafe y suministrado por la Unidad de Comunicación.
- **Necesidad:** Sólo se facilitará una cuenta de correo electrónico corporativa a aquellas personas que la precisen para el desarrollo de su trabajo en el Ayuntamiento.
- **Uso responsable:** Empleo del correo electrónico en base al “sentido común” y teniendo en cuenta la responsabilidad y funciones desempeñadas por el usuario/a, tratando en cualquier caso de no poner en compromiso ni los sistemas, ni la imagen del Ayuntamiento.
- **Servicios de detección de correo no deseado:** El Ayuntamiento quedará facultado para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada a las personas usuarias para el desarrollo de sus funciones laborales, al objeto de prevenir aplicaciones maliciosas (virus, ransonware, etc.) o en el supuesto de que existan razones fundamentadas en una firme sospecha por parte del Ayuntamiento sobre la existencia de actividades delictivas o dolosas del personal.

  Así mismo, el sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente normativa.
- **Cuentas de correo departamentales:** Los responsables de las Unidades establecerán en que ocasiones deben ser utilizadas las cuentas de correo electrónico departamentales tanto para la recepción como para el envío de información o documentos necesarios para el correcto desarrollo de las funciones y competencias de la Unidad.
- **No ceder el uso de la cuenta de correo a terceras personas**. La cesión del uso de la cuenta de correo electrónico a una tercera persona provocaría una suplantación de identidad y el acceso a información “uso oficial” o “interna”.
- **Difusión de las direcciones de correo electrónico**: Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y

cuando el fin último sea el cumplimiento de las funciones municipales (por ejemplo, cuando nos subscribimos a un foro).

Siempre que se suscriba a un servicio, relación con otra entidad, intercambio de información, etc. deberá realizarse mediante un buzón de correo corporativo y compartido, indicando como dirección de aviso a notificaciones@ayto-getafe.org.

- **Revisar los campos de direcciones antes de enviar un mensaje**. El envío de información a destinatarios erróneos puede suponer una brecha en la privacidad o confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo Con Copia (CC). Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.
- **No enviar o reenviar correos de forma masiva**. Si, previa autorización del Responsable de Unidad, se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Con Copia Oculta (CCO), evitando así la comunicación de las direcciones a todos los receptores del mensaje. La revelación de direcciones de correo electrónico en la remisión de correos electrónicos masivos al no utilizar listas de distribución o la opción CCO, puede suponer un incumplimiento de la vigente normativa de Protección de Datos.
- **No enviar mensajes en cadena**. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe proceder a su borrado inmediatamente, comunicando la incidencia a la UIAET.
- **No responder a mensajes de Spam**. La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envía a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la entidad local. En cualquier caso, nunca debe responderse.
- **Asegurarse de la identidad del remitente antes de abrir un mensaje**. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Al tratarse de un incidente que puede afectar gravemente a los sistemas municipales debe ponerse en conocimiento de la UIAET. (Véase documento que se entrega junto con el equipamiento).
- **No remitir información "uso oficial" o "interna".** Cuando un remitente desconocido o un contacto habitual siempre que dude de su procedencia las solicite, se debe verificar siempre con carácter previo la identidad del solicitante a través de un medio que permita verificar la identidad (por ejemplo, firma electrónica, llamando al solicitante para verificar la petición).
- **No ejecutar archivos adjuntos sospechosos**. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso. Gran parte del código malicioso suele insertarse en archivos adjuntos, ya sea en forma de

ejecutables (.exe o una macro, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

- **Informar de correos con virus, phishing, malware, etc**. Si el usuario/a detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente a la UIAET y no reenviarlo, para evitar su posible propagación.
- **Acceso/utilización de cuentas de correo electrónico no corporativas (Gmail, Yahoo!, Hotmail, etc.):** Desde los equipos (fijos o móviles) puestos a disposición del personal, el uso de cuentas de correo no corporativas supone una amenaza a la seguridad, por lo que su uso no está permitido, salvo autorización de la UIAET, en cuyo caso deberán aplicarse las mismas recomendaciones que para el correo corporativo.
- **Medidas a aplicar en el navegador usado para acceder al correo electrónico:** Desactivar las características de recordar contraseñas para el navegador en los accesos al correo electrónico y activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.

Respecto al uso del correo electrónico en el Ayuntamiento, **queda terminantemente prohibido**:

- Falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.
- Leer o acceder a correos electrónicos ajenos, sin autorización previa.
- Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos tipificados como “uso oficial”, salvo que se adopten medidas de cifrado o similares. Se deberán de aplicar las medidas de seguridad de cifrado según los procedimientos específicos establecidos por el Ayuntamiento.
- Utilizar el correo electrónico como medio de comunicación con el ciudadano salvo que se cuente con su consentimiento.
- Utilizar el correo como sistema de almacenamiento o gestión de la información.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, o bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

16. Acceso a Internet y otras herramientas de colaboración

El acceso corporativo a Internet es un recurso centralizado que el Ayuntamiento pone a disposición de las personas usuarias, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional. El Ayuntamiento velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso. Respecto al acceso a Internet se establecen las siguientes normas de utilización:

- **Acceso a Internet para fines profesionales:** Las conexiones que se realicen a Internet deben obedecer a fines profesionales. El acceso a Internet para fines personales debe limitarse y, de ser

absolutamente necesario, sólo debe realizarse por un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

- **Uso de navegador suministrado:** Sólo se podrá acceder a Internet mediante los navegadores recomendados para la realización de las gestiones propias del Ayuntamiento y configurados por la Unidad de Informática, Administración Electrónica y Transparencia en los puestos de usuario, no pudiendo alterarse la configuración de los sistemas ni utilizar un navegador alternativo.
- **Filtrado y bloqueo de accesos:** El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.
- **Conexiones autorizadas:** Las conexiones a Internet solo podrán ser realizadas utilizando los medios facilitados por la UIAET. La conexión de los sistemas a redes inalámbricas o de otro tipo deberán contar con la autorización expresa de la UIAETa.
- **Comunicación de anomalías:** Deberá notificarse a la UIAET cualquier anomalía (redirección a páginas solicitadas, aviso de sitio no seguro, en páginas habitualmente utilizadas, etc.) detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso. (Véase documento que se entrega junto con el equipamiento**).**

Se consideran **usos prohibidos** los siguientes:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.
- La descarga de aplicaciones informáticas, sin la autorización previa de la UIAET, o archivos con contenido dañino que supongan una fuente de riesgos para la entidad. En todo caso debe asegurarse que el sitio web visitado es confiable.
- El acceso a recursos y sitios web, o la descarga de aplicaciones informáticas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de aplicaciones informáticas de intercambio de información, P2P o similares) para la descarga masiva de archivos, aplicaciones informáticas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por la UIAET.
- La visualización de contenidos multimedia (videos, música, etc.) que no estén relacionados con los fines profesionales.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

17. Trabajo fuera de las dependencias municipales (Teletrabajo)

Se considerará trabajo desde fuera de las dependencias municipales, el acceso desde el exterior a recursos internos del Ayuntamiento con el objeto de realización de tareas propias del puesto de trabajo.

La UIAET podrá habilitar el acceso remoto para el uso de recursos informáticos fuera de las dependencias municipales previa solicitud por parte del Responsable del usuario/a. Además de las normas específicas para el trabajo fuera de las instalaciones que puedan ser establecidas por el Comité de Seguridad de la Información y Protección de Datos Personales, los usuarios/as deberán tener en consideración:

- **Equipos y dispositivos:** Para el acceso a los servicios del Ayuntamiento, se deberán utilizar exclusivamente los medios ofrecidos por la entidad local, salvo autorización de la UIAET (uso de dispositivos no corporativos para el trabajo fuera de las dependencias municipales).
- **Medidas de seguridad:** El acceso a los sistemas de información municipales se realizará mediante una VPN con doble factor de autenticación (2FA) y todas las recomendaciones de uso entregadas con el dispositivo y publicadas en los medios de información internos.
- **Seguridad durante la conexión:** Cada usuario/a deberá evaluar la seguridad de la ubicación desde la que accede a los servicios para evitar factores de riesgo como robos, accesos no autorizados e interceptación de la comunicación y/o de la información.
- **Desconexión:** Una vez finalizada la sesión, el usuario/a deberá realizar la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.

18. Incidencias de Seguridad

Nunca se debe proporcionar información sensible de facturación, cuentas bancarias, datos de identificación, usuarios y contraseñas, o similar, vía telefónica, correo electrónico e incluso personalmente a un tercero, ya que las tareas de soporte técnico informático municipal nunca lo requerirán.

Tampoco es preciso que sin previa planificación o autorización expresa de la UIAET o del Responsable de Información y Servicios, se acceda a un equipo o dispositivo para su actualización de software, sistema operativo, conexión remota, o se realice aviso acerca de que éste se encuentra en riesgo, o pueda existir alguna información comprometida. Podría el usuario estar siendo objeto de un fraude de Ingeniería Social.

Cuando un usuario/a detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arrancan o que se cierran de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los sistemas de información del Ayuntamiento de Getafe o su imagen, deberá informar inmediatamente a la UIAET, que lo registrará debidamente y elevará al Comité de Seguridad de la Información y Protección de Datos Personales, en caso de que sea necesario (Véase documento que se entrega junto con el equipamiento).

Será la UIAETa encargada de comunicar el incidente al Delegado/a de Protección de Datos en caso de que el mismo afecte a datos de carácter personal.

19. Acceso y permanencia de terceros en los edificios, instalaciones y dependencias

Los terceros, deberán cumplir las siguientes normas, además del resto de normativas de seguridad del Ayuntamiento:

- Acceso y permanencia en los edificios, instalaciones y dependencias:

Los terceros que temporalmente deban acceder a los edificios, instalaciones o dependencias del Ayuntamiento, deberán hacerlo siempre bajo la supervisión de algún miembro de la misma y previa autorización del Responsable de la Unidad afectada.

Una vez en el interior, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aseos, comedor, zona de máquinas de cafetería, etc.). En el resto de dependencias deberán estar acompañados.

- Acceso lógico a los sistemas de información del Ayuntamiento de Getafe:

Para los accesos (incluido el acceso remoto) al sistema de información municipal, por parte de terceros, se crearán credenciales de usuario asociados a la duración del servicio o trabajo relacionado. Si, de manera excepcional, para resolver problemas urgentes, se tuvieran que utilizar identificadores de personas usuarias ya existentes, los trabajos se realizarán siempre en presencia de la persona a la que corresponden las credenciales. Una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas utilizadas, solicitando, en caso de ser necesario, su cambio a la Unidad de Informática, Administración Electrónica y Transparencia.

Cualquier incidencia que pudiera afectar o comprometer la seguridad de los sistemas de información del Ayuntamiento, durante el acceso de terceros, deberá ponerse en conocimiento de la Unidad de Informática, Administración Electrónica y Transparencia, a la mayor brevedad posible.

20. Supervisión y aplicación de esta normativa

El Ayuntamiento, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

Con este fin, se registrará la actividad de los usuarios/as, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Dicha información, cuando sea considerada dato de carácter personal, formará parte de un tratamiento responsabilidad del Ayuntamiento de Getafe con la finalidad de gestionar los sistemas de seguridad municipales. La legitimación para el tratamiento se encuentra en el artículo 6.1 c) del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD): cumplimiento de una obligación legal y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público [Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica].

Los datos serán conservados durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

Solo se procederá a la cesión de los datos personales a terceros cuando se cumplan las exigencias establecidas en la legislación vigente de Protección de Datos, pudiendo realizarse cesiones a organismos

públicos encargados de la seguridad como Centro Criptológico Nacional (CCN), Agencia Española de Protección de Datos, Fuerzas y Cuerpos de Seguridad del Estado o Juzgados y Tribunales.

El Registro de Actividades de Tratamiento (RAT) del Ayuntamiento podrá ser consultado en la sede municipal.

Esta supervisión se realizará sin previo aviso, en todo caso, garantizando el respeto a los derechos fundamentales reconocidos en el artículo 18 de la Constitución Española: derecho al honor, a la intimidad personal y familiar y a la propia imagen; al secreto en las comunicaciones, salvo resolución judicial; y a la limitación del uso de la informática, así como, de conformidad con lo establecido en la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

21. Incumplimiento de la Normativa

Todos los usuarios/as del Ayuntamiento de Getafe están obligadas a cumplir lo prescrito en la presente Normativa de Uso de los Sistemas de Información.

La UIAET en colaboración con todas las Unidades del Ayuntamiento de Getafe, velará por el cumplimiento de la presente normativa e informará al Comité de Seguridad de la Información y Protección de Datos Personales sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

En el supuesto de que un usuario/a no observe alguno de los preceptos señalados en la presente normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tenga asignados, previa instrucción del procedimiento legal que corresponda.

En el caso de personal de terceros, el incumplimiento de esta normativa podría derivar en la resolución del contrato, siguiendo el procedimiento establecido al efecto en la normativa sobre contratación administrativa.

ANEXO I – PERSONAL DE TERCEROS

En el acceso a los sistemas de información del Ayuntamiento por parte de personal de terceros, se tendrán las siguientes consideraciones en relación a la presente normativa:

a) Con carácter general, el Ayuntamiento no facilitará al personal de terceros equipamiento informático (fijo o móvil) o de comunicaciones para el desarrollo de los servicios contratados. Sin embargo, los equipos informáticos o de comunicaciones que sean utilizados por el personal externo deberán ser configurados según las directrices de la Unidad de Informática, Administración Electrónica y Transparencia.

b) Todas las peticiones o actuaciones que en la presente normativa precisen de autorización previa y se haga referencia a "el Responsable del usuario/a", deberá ser tramitada por el Responsable del expediente del que dependa del usuario/a externo/a.

c) El usuario/a externo/a deberá acceder a los sistemas municipales exclusivamente para realizar las tareas encomendadas teniendo en cuenta las directrices indicadas por el Responsable del expediente del que dependa, así como aquellas indicadas por el personal a la Unidad de Informática, Administración Electrónica y Transparencia.

d) Será responsabilidad de la entidad de la que depende el usuario/a externo/a, el poder evidenciar ante el Ayuntamiento que le ha dado traslado de lo indicado en la presente normativa en la medida que sean de aplicación, por lo que le recepción y entrega de la misma debe ser firmada.

e) El usuario/a externo/a, no dispondrá en ningún caso cuenta nominativa de correo electrónico institucional (@ayto-getafe.org). En caso de que el usuario/a precise de una cuenta de correo se le asignará una cuenta genérica que deberá ser solicitada por el Responsable del expediente del que dependa el usuario/a externo/a, debiéndose notificar una persona responsable de la misma (un empleado público del Ayuntamiento). Así mismo, en la cuenta de correo-e genérica asignada, no podrán configurarse firmas de correo electrónico con nombre y apellidos. Las firmas sólo podrán hacer referencia a la Unidad.

22. Modificaciones

EDICIÓN	FECHA	MODIFICACIONES RESPECTO A LA EDICIÓN ANTERIOR
01	9/2/23	Decreto de Aprobación por la Alcaldesa.