Ayuntamiento de
Las Rozas

PROYECTO DE REGLAMENTO DE NORMATIVA DE USO DEL SISTEMA DE INFORMACIÓN Y DE RECURSOS INFORMÁTICOS Y DE CREACIÓN DEL REGISTRO DE INCIDENCIAS DEL AYUNTAMIENTO DE LAS ROZAS DE MADRID.

Contenido

CAPÍTULO I. OBJETO, ÁMBITO DE APLICACIÓN Y REVISIÓN:

Artículo 1. Objeto

1. Los sistemas de información son elementos básicos para el desarrollo de la actividad del Ayuntamiento de Las Rozas. Estos medios se ponen a disposición de las personas usuarias como instrumentos de trabajo para el desempeño de su actividad profesional, motivo por el cual, éstas deben utilizar estos recursos de manera responsable, mediante el seguimiento de normas y buenas prácticas que salvaguarden la seguridad de la información, los sistemas de información y los recursos tecnológicos proporcionados por la entidad local.

2. El Ayuntamiento podrá establecer, previa aprobación por parte del Comité de Seguridad, normas, pautas, procedimientos o buenas prácticas que complementen o regulen aspectos particulares de la presente Normativa o de su aplicación en supuestos específicos.

3. A los efectos de aplicación de esta Normativa, la información tratada en el Ayuntamiento de Las Rozas ha sido calificada como:

a) Confidencial: se considerará por "Información Confidencial" : (I) toda aquella información de cualquier naturaleza (técnica, financiera, operacional, comercial) y en particular, toda aquella relacionada con la ideación, desarrollo, protección y fabricación, (II) cualquier información técnica o de otra naturaleza, diseño, proceso, innovación, procedimiento o mejora con valor comercial y/o de carácter secreto que sea patentable o no, (III) cualquier material confidencial, documentos, informes, datos, especificaciones, software, códigos, invenciones, know-how, secretos comerciales, programas informáticos, (IV) cualquier información técnica o de otra naturaleza, diseño, proceso, innovación, procedimiento o mejora con valor comercial y cuya divulgación no autorizada, pérdida o destrucción pueda generar impactos importantes para la entidad local siendo la siguiente:

   i. Categorías especiales de datos establecidos en el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, 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 o artículo 10 del RGPD (condenas e infracciones penales).

   ii. Los Datos Personales son cualquier información relativa a una persona física viva identificada o identificable. Todos los datos personales serán confidenciales. En todo caso, los Datos Personales tratados por el Ayuntamiento no son de difusión pública.

   iii. Documentos en fase de desarrollo, contengan datos personales o no, que sirvan de soporte para la elaboración de los acuerdos municipales.

   iv. Aquellos documentos que, a criterio de la persona que los ha elaborado, considera que tienen carácter "confidencial".

b) 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 organización.

c) Pública: se considerará toda aquella información de uso general y público dentro y fuera de la entidad local. La divulgación, pérdida o destrucción de esta información

no generará ningún impacto para la organización. Se atenderá a la Ley 19/2013, de 9 de diciembre, de trasparencia, acceso a la información pública y buen gobierno.

Artículo 2. Ámbito de aplicación

1. Mediante la presente Normativa, el Ayuntamiento de Las Rozas 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 del Ayuntamiento, tanto laboral como funcionario, así como aquellas personas que mantienen otra relación con la entidad local (cargos políticos, personal de confianza, becarios, personal en prácticas, etc.), los cuales quedan sujetos a la misma, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

2. Lo expuesto en el primer párrafo del presente artículo será de aplicación igualmente a aquellos entes dependientes del Ayuntamiento de Las Rozas, así como al conjunto del sector público institucional local (Fundaciones, Entidades Públicas Empresariales, Organismos Autónomos etc.).

3. También será de aplicación al personal de terceros con acceso al sistema (empresas proveedoras, colaboraciones reguladas por convenios), quienes quedan también sujetos a la misma, en la medida que le sean de aplicación tal y como se describe en el Anexo I de la presente Normativa, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el desempeño de sus actividades en el Ayuntamiento.

Artículo 3. Revisión y/o actualización

1. El Comité de Seguridad de la Información del Ayuntamiento de las Rozas, es el órgano encargado de exigir el cumplimiento de la norma, así como de su propuesta de revisión y actualización. En concreto, le corresponden las siguientes funciones:

a) Dictar criterios generales de aplicación respecto a las dudas que puedan surgir de su aplicación.

b) Proponer su actualización, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

c) Verificar su efectividad y cumplimiento.

2. El Comité de Seguridad de la Información revisará anualmente la presente Normativa con una periodicidad anual, pudiendo realizar propuestas para su modificación o actualización, en caso de ser necesario. En dicho supuesto, elevará su propuesta a la Junta de Gobierno Local para que esta pueda, en su caso, incluirlo como Proyecto de Reforma del Reglamento.

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

a) Identificación de acciones de mejora en la gestión de la seguridad de la información.

b) Adaptación a los posibles cambios normativos, de infraestructuras tecnológicas, organizativas, etc.

c) Identificación de oportunidades de mejora en la gestión de la seguridad de la información.

d) La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

CAPÍTULO II. NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

Artículo 4. Normas generales

1. El Ayuntamiento de Las Rozas 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, necesarios para el desarrollo de las funciones profesionales que tenga atribuidas.

2. Mediante estos equipos las personas usuarias tendrán acceso a los Sistemas de Información del Ayuntamiento de Las Rozas, motivo por lo que es necesario adoptar una serie de precauciones y medidas para su adecuada utilización.

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

5. La presente normativa de uso de los sistemas de Información será entregada a todo el personal afectado por la misma e indicado en el ámbito de aplicación. Dicho personal firmará además la declaración recogida en el Anexo II. De manera adicional la presente normativa estará a disposición en la intranet municipal.

6. La Dirección General de la Oficina Digital, en adelante D.G. de la Oficina Digital, proporcionará a las personas usuarias el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones, respecto a los cuales se observarán las siguientes normas generales:

a) Los equipos deberán utilizarse únicamente para fines institucionales profesionales y como herramienta para el desempeño de las tareas encomendadas.

b) Salvo autorización expresa del D.G. de la Oficina Digital, las personas usuarias no tendrán privilegios de administrador sobre los equipos.

c) Únicamente el personal autorizado por la D.G. de la Oficina Digital podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos.

d) Cuando sea necesario instalar equipos que no hayan sido provistos por el Ayuntamiento deberá de solicitarse autorización previa a la D.G. de la Oficina Digital, a través del Centro de Atención y Soporte al Usuario (CAU).

e) Las personas usuarias deberán notificar a la D.G. de la Oficina Digital, a través del Centro de Atención y Soporte al Usuario (CAU) 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.

f) Cada equipo deberá de estar asignado a una persona o grupo de personas concreto. Tales personas son responsables de su correcto uso.

g) No podrán conectarse a la red corporativa equipos o dispositivos que no hayan sido previamente autorizados por la D.G. de la Oficina Digital.

h) Una vez finalizada la relación con el Ayuntamiento o la necesidad de utilizar un equipo o dispositivo este tendrá que ser entregado a la D.G. de la Oficina Digital.

Artículo 5. Normas específicas para equipos portátiles y móviles

1. La D.G. de la Oficina Digital será la encargada de la asignación y distribución de los equipos portátiles y móviles. Al igual que el resto de los equipos, estarán debidamente configurados con acceso a los servicios y aplicaciones necesarios para el desempeño de sus funciones.

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

a) 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 el acceso a ellos por parte de personas no autorizadas.

b) La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la D.G. de la Oficina Digital para la adopción de las medidas que correspondan.

c) 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.

d) Cuando en los dispositivos o equipos se trate o almacene información "confidencial", estos deberán disponer de mecanismos de cifrado para proteger dicha información, salvo que existan limitaciones verificadas por la D.G. de la Oficina Digital que impidan cumplir con esta obligación. Será la D.G. de la Oficina Digital la encargada de implementar las medidas de cifrado en dispositivos o equipos.

e) Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, la persona usuaria lo devolverá a la D.G. de la Oficina Digital, 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.

f) Cuando se utilicen estos dispositivos fuera de la red municipal no se podrán realizar conexiones a redes abiertas, es decir redes públicas o privadas sin mecanismos de identificación.

3. Con carácter general no está permitido el uso de dispositivos móviles propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información municipal salvo autorización expresa, que deberá ser solicitada al Comité de Seguridad de la Información del Ayuntamiento de Las Rozas.

CAPÍTULO III. NORMAS PARA EL ALMACENAMIENTO DE INFORMACIÓN Y COPIAS DE SEGURIDAD

Artículo 6. Normas generales

1. Para garantizar la disponibilidad de la información municipal frente a un incidente de seguridad, se han establecido políticas de copias de seguridad tanto de la información de las aplicaciones informáticas, como de los espacios corporativos en la nube contratados por el Ayuntamiento.

2. Las personas usuarias quedan obligadas a almacenar en las aplicaciones y/o espacios corporativos (OneDrive, SharePoint) los datos generados en el desempeño de sus competencias profesionales.

3. La información personal de trabajo (plantillas, borradores, documentación sobre legislación...) deberá almacenarse en OneDrive, teniendo este una retención de 60 días desde el borrado de la información. Toda documentación de trabajo se almacenará en SharePoint, estando este incluido en las políticas de copia de seguridad del Ayuntamiento. Es importante, hacer hincapié en que la documentación definitiva que forme parte de un expediente ya queda almacenada en el propio gestor de expedientes, haciendo copias de seguridad del mismo.

4. No está permitido el almacenamiento de información privada ni de terceros ajenos al Ayuntamiento en las aplicaciones y/o recursos corporativos en la nube.

5. 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 D.G. de la Oficina Digital, a través del Centro de Atención al Usuario (CAU). A este respecto, se informa que no se realizan copias de seguridad, labores de recuperación o traspaso de la información que se encuentre almacenada fuera de las aplicaciones o recursos corporativos en la nube, como, por ejemplo, en el escritorio, carpeta "Mis Documentos", unidad local, etc., de los equipos de usuario.

6. Los recursos corporativos en la nube 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 la persona usuaria precise de más capacidad de almacenamiento deberá ponerse en contacto con la D.G. de la Oficina Digital, que solicitará Informe de necesidad al Responsable del Servicio/Departamento/Unidad y de cuotas de espacio actualizado a fecha de la solicitud al Responsable del Sistema (atendiendo a las capacidades disponibles en el sistema) podrá incrementar la cuota de espacio asignada.

CAPÍTULO IV. NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

Artículo 7. Normas generales

1. Las personas usuarias que deban de intercambiar o trasladar archivos deberán realizarlo utilizando las funcionalidades a través de los recursos en la nube contratados por el Ayuntamiento. Como norma general, no está autorizado en el Ayuntamiento de Las Rozas, el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros externos, tarjetas de memoria, etc.), encontrándose los puertos USB inhabilitados, a

excepción de aquello utilizados para la atención al público, concretamente en la Oficina de Asistencia en Materia de Registro.

2. Si de manera extraordinaria, es necesario el uso de este tipo de soportes en equipos deshabilitados, debe solicitarse de manera expresa a la D.G. de la Oficina Digital y tras autorizarse habrán de observarse las siguientes normas:

- Como norma general se utilizarán los proporcionados por el Ayuntamiento de Las Rozas, siendo de uso exclusivo en los puestos de usuario del Ayuntamiento. Están destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento.
- El uso de medios de almacenamiento extraíbles particulares no está autorizado.
- Estos dispositivos deberán contar con mecanismos de cifrado que serán implementados por la D.G. de la Oficina Digital. Previa evaluación y aprobación el D.G. de la Oficina Digital podrá establecer la excepción de aplicar mecanismos de cifrado en función el uso del soporte y/o de la información que vaya a ser almacenada en el mismo.
- Su uso no está autorizado para el almacenamiento de datos personales, salvo que se disponga de autorización expresa de la persona Responsable de la persona usuaria.
- Este tipo de dispositivos deberá de almacenarse 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 del D.G. de la Oficina Digital, de forma inmediata. Este será el encargado de informar al Delegado/a de Protección de Datos en caso de incluir datos de carácter personal.

Artículo 8. Normas para el borrado y eliminación de soportes informáticos

1. La reutilización de medios de almacenamiento deberá ser solicitada al D.G. de la Oficina Digital, para que proceda a su borrado seguro.

2. 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 al D.G. de la Oficina Digital, debiendo asegurarse la persona usuaria que el contenido del soporte puede ser eliminado.

CAPÍTULO V. NORMAS RESPECTO A LA DOCUMENTACIÓN IMPRESA

Artículo 9. Sistemas de copia/impresión

1. 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 del correspondiente informe de necesidad por parte de la persona Responsable de la persona usuaria para obtener la autorización pertinente por parte de la D.G. de la Oficina Digital.

2. En ningún caso la persona usuaria podrá hacer uso de los sistemas de copia/impresión que no hayan sido proporcionados por el Ayuntamiento. En relación a los sistemas de copia/impresión y documentación impresa, la persona usuaria debe seguir las siguientes directrices:

a) Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en el citado formato.

b) Cuando se impriman documentos, en sistemas copia/impresión comunes, éstos deberán permanecer el menor tiempo posible en las bandejas de salida, para evitar que terceras personas puedan acceder a la misma.

c) Los códigos o claves que sean facilitados para acceder a los sistemas de copia, impresión o escaneo serán personales e intransferibles.

d) En caso de encontrase documentación catalogada como "confidencial" en un sistema de copia/impresión, la persona usuaria intentará localizar a la persona propietaria para que proceda a su recogida inmediata. En caso de desconocer a la persona propietaria o estar localizable, lo pondrá inmediatamente en conocimiento de la persona responsable de su Área/Departamento/Servicio.

e) 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, la persona usuaria debe asegurarse de que es absolutamente necesario hacerlo.

Artículo 10. Cuidado y protección de la documentación impresa

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

a) 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.

b) Cuando no vaya a ser utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) preferentemente bajo llave.

c) 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.

d) Se pondrá a disposición en la intranet municipal la información de gestión documental relativa a documentación susceptible de eliminación y el protocolo de actuación para la destrucción segura de la misma.

e) 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 ningún tipo de información "confidencial" o interna accesible a personas no autorizadas.

2. La documentación impresa debe respetar el calendario de transferencias establecido para cada una de las áreas, no debiendo obrar en poder de la oficina documentación de más de dos años de antigüedad.

3. Los protocolos de transferencia y eliminación de la documentación impresa establecidos desde la Política de Gestión Documental del Ayuntamiento de Las Rozas estarán a disposición de todo el personal en la intranet.

CAPÍTULO VI. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

Artículo 11.

1. Está estrictamente prohibida en los Sistemas de Información del Ayuntamiento de Las Rozas la ejecución de aplicaciones informáticas sin la correspondiente licencia de uso.

2. 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 previa del D.G. de la Oficina Digital.

3. 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 la persona usuaria 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 esta.

CAPÍTULO VII. INSTALACIÓN DE APLICACIONES

Artículo 12.

1. Únicamente el personal del D.G. de la Oficina Digital podrá instalar aplicaciones informáticas en los equipos de las personas usuarias, salvo que se disponga de autorización expresa, en cuyo caso se deberán de tener en cuenta las siguientes indicaciones:

a) 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.
b) 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.
c) No se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el D.G. de la Oficina Digital especialmente aquellas relacionadas con la seguridad.

CAPÍTULO VIII. ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

Artículo 13.

1. Para acceder a los sistemas/recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de dominio. El alta de las personas usuarias será comunicada a la D.G. de la Oficina Digital, a través del Centro de Atención y Soporte al Usuario (CAU) por el Departamento de Recursos Humanos, siendo la persona Responsable de la persona usuaria la encargada de indicar el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada persona usuaria, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

2. El Departamento de Recursos Humanos comunicará la baja de los usuarios a la D.G. de la Oficina Digital a través del Centro de Atención y Soporte al Usuario (CAU) para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

3. Los cambios o modificaciones en el acceso a los sistemas de información a los sistemas de información municipales dentro de un mismo Área/Departamento/Servicio serán comunicados al D.G. de la Oficina Digital a través del CAU por la persona Responsable de la persona usuaria. En aquellos casos en los que la persona usuaria cambie de Área/Departamento/Servicio deberá ser comunicada por el Departamento de Recursos Humanos esta circunstancia, siendo la persona responsable del Área/Departamento/Servicio al que será trasladada la persona usuaria la encargada de indicar los requisitos de acceso.

4. Cuando la persona usuaria esté vinculada a un contrato de servicios será la persona Responsable del Área/Departamento/Servicio responsable del expediente la encargada de comunicar tanto el alta, modificaciones o baja de la persona usuaria a la D.G. de la Oficina Digital.

5. Con el fin de garantizar que la relación de personas usuarias con accesos a los sistemas de información se encuentra actualizada y que disponen de los correspondientes permisos de acceso en cada caso, se llevarán a cabo revisiones por parte del D.G. de la Oficina Digital con la colaboración del Departamento de Recursos Humanos y de las personas Responsables de las Áreas/Departamentos/Unidades municipales.

6. Es responsabilidad de la persona usuaria hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por la D.G. de la Oficina Digital en caso de mala utilización. Las personas usuarias tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

7. Cuando la persona usuaria deje de atender su equipo durante un cierto tiempo o se ausente de su puesto de trabajo, se procederá al bloqueo de la sesión de usuario 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 5 minutos, salvo que el puesto de usuario precise establecer otra configuración que será previamente analizada y aprobada por el Comité de Seguridad.

Artículo 14. Identificación y Autenticación en el sistema de información

1. Las personas usuarias dispondrán de credenciales nominales (código de usuario y una contraseña) y en determinados sistemas de un doble factor de autenticación 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 de observar las siguientes medidas:

a) 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. Excepcionalmente se podrá acceder a los sistemas con credenciales compartidas previa autorización del D.G. de la Oficina Digital y siempre que exista un control e identificación de las personas que acceden en cada momento.

b) Las personas usuarias 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.

c) Si una persona tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al D.G. de la Oficina Digital a través del CAU la correspondiente incidencia de seguridad.

d) No podrán establecerse en los sistemas municipales las mismas contraseñas que las personas usuarias utilizan para el acceso a servicios o herramientas en el ámbito personal.

e) Las personas usuarias deben utilizar contraseñas seguras, por lo que las mismas tienen que tener una longitud mínima de 12 caracteres y que incluyan al menos una letra mayúscula una letra minúscula, un carácter especial (del tipo @, #, +, etc.) y un número. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables a la persona usuaria (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.).

f) En aquellos sistemas que dispongan de doble factor de autenticación (2FA) se habilitará el mismo siempre y cuando la persona usuaria disponga de los medios necesarios para validarse utilizando 2FA.

g) El sistema fuerza al cambio de contraseñas periódico, al menos cada 60 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 de la persona usuaria su cambio dentro del plazo anteriormente indicado.

h) 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 Comité de Seguridad.

i) Por motivos de seguridad se podrá proceder a la desactivación de los accesos a los sistemas de información municipales que no hayan tenido un periodo de inactividad

superior al plazo establecido para el cambio de las contraseñas establecido en la presente Normativa.

Artículo 15. Comunicaciones internas de información

1. No se podrá extraer información de los sistemas de información municipales para su remisión a través de un sistema diferente al de origen (correo electrónico, documento ofimático, etc.). En caso de que una persona usuaria precise de cierta información para el correcto desarrollo de sus funciones, se deberá solicitar por la persona responsable de la persona usuarias al D.G. de la Oficina Digital a través del CAU, los accesos necesarios en cada caso.

Artículo 16. Certificados electrónicos

1. En el uso de certificados de la administración pública las personas usuarias deberán tener en cuenta las siguientes consideraciones:

a) Cumplir con los términos y condiciones de uso asociados al certificado de la administración pública que han sido facilitados en la asignación por parte de un Prestador de Servicios de Confianza (TSL).

b) Utilizar el certificado únicamente para la realización de gestiones relacionadas con el desempeño de las funciones y competencias, quedando prohibido su uso en el ámbito personal.

c) Comunicar cualquier incidencia, uso indebido o sospecha de uso indebido al Departamento de TIC a través del Centro de Atención y Soporte al Usuario (CAU) para proceder a su revocación, así como para la gestión de la posible incidencia de seguridad.

d) 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 el D.G. de la Oficina Digital.

2. El uso de certificados personales en los sistemas de información municipales solo podrá realizarse en casos excepcionales y con la autorización previa del Comité de Seguridad.

Artículo 17. Acceso a una cuenta de una persona usuaria en su ausencia o baja.

1. Cuando sea necesario acceder a información concreta (un archivo, un correo electrónico, etc…) ubicada en una carpeta personal, recursos en la nube o cuenta de correo corporativa de una persona usuaria, será necesario contar con la autorización expresa de aquella.

2. En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser autorizado por el Responsable de la persona usuaria. En estos casos el acceso se realizará por el D.G. de la Oficina Digital con la presencia del Responsable de la persona usuaria y una persona que actúe como representante sindical.

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

CAPÍTULO IX. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Artículo 18.

1. La información contenida en los Sistemas de Información del Ayuntamiento es responsabilidad de la entidad local, por lo que las personas usuarias 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 Institución. Además, deberá de tener en cuenta las siguientes premisas:

a) 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 reserva.

b) Las personas usuarias solo podrán acceder a la información necesaria para el desempeño de sus labores con las debidas autorizaciones.

c) 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 la persona usuaria.

d) Los derechos de acceso de las personas usuarias 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".

e) La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos Personales, 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.

f) Solo se podrá transmitir o alojar información con datos de carácter personal de los cuales el Ayuntamiento es responsable en servidores externos cuando exista autorización expresa. Podrá ser consultado para su análisis al Delegado/a de Protección de Datos (DPD) con el objetivo de comprobar todos los posibles inconvenientes legales. Así mismo, se verificará la suscripción de un contrato expreso entre el Ayuntamiento y la entidad 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.

g) Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de esta estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del RGPD.

h) En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos del tratamiento, no pudiendo oponer a este acceso el responsable o el encargado de tratamiento la existencia de cualquier deber de confidencialidad o secreto de acuerdo con la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) y el RGPD.

i) En todo caso, se garantizará la confidencialidad de la información suministrada que pueda afectar a la seguridad e integridad de las redes y de los servicios de comunicaciones electrónicas o al secreto comercial o industrial.

CAPÍTULO X. METADATOS Y DATOS OCULTOS DE LOS DOCUMENTOS ELECTRÓNICOS

Artículo 19.

1. Se define "metadatos" o "información o datos ocultos" como aquella información existente en los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de las aplicaciones informáticas utilizadas para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos para su visualización. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

2. Cuando se generan documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.), un documento PDF o realiza una fotografía, estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, 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, etc.

3. Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc…) pueden tener integrados en sus propiedades una serie de datos ocultos y/o metadatos, 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, etc.

Artículo 20.

1. Los metadatos 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 internamente en el Ayuntamiento, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc…), deberá ser revisado para determinar los metadatos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento establecido para ello en el Ayuntamiento y puesto a disposición en la intranet municipal, pudiendo solicitar en caso necesario asistencia a la D.G. de la Oficina Digital a través de la apertura de incidencia en el Centro de Atención y Soporte al Usuario (CAU).

CAPÍTULO XI. SALIDA DE INFORMACIÓN

Artículo 21.

1. La salida de información del Ayuntamiento de Las Rozas (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por el Ayuntamiento, autorización que contemplará igualmente a la propia información que sale. En este caso se deberá de enviar una solicitud, a través del Centro de Atención y Soporte al Usuario (CAU) al D.G. de la Oficina Digital para que asesore sobre las medidas de seguridad que deberán ser implementadas.

2. Si la información contiene datos de carácter personal, se atenderá a lo establecido en la normativa de protección de datos.

3. Las personas usuarias se abstendrán de sacar al exterior cualquier información del Ayuntamiento de Las Rozas en cualquier dispositivo (dispositivos ópticos (CDs, DVDs), memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

CAPÍTULO XII. USO DEL CORREO ELECTRÓNICO CORPORATIVO

Artículo 22.

1. 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.

2. 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:

3. Todos los correos salientes enviados fuera del Ayuntamiento de Las Rozas a otras organizaciones deberán incluir en el pie de firma, como mínimo, la información señalada en el siguiente modelo o aquel que se determine en un futuro manual de estilo de la organización.

Ayuntamiento de
Las Rozas

[Nombre y Apellidos]
[Cargo en el Ayuntamiento]
[Área/Servicio/Unidad/Departamento]
Tlf: _____
Dirección: _____

Artículo 23.

1. 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:

a) **Uso responsable:** Empleo del correo electrónico en base al "sentido común" y teniendo en cuenta la responsabilidad y funciones desempeñadas por la persona usuaria, tratando en cualquier caso de no poner en compromiso ni los sistemas, ni la imagen del Ayuntamiento.

b) Servicios de detección de correo no deseado: La D.G. de la Oficina Digital quedará facultada 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, …) 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.

c) Contenido adicional informativo: 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.

d) Cuentas de correo departamentales/genéricas: Las personas responsables de las Áreas/Departamentos/Servicios 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 correcto desarrollo de las funciones y competencias del Área/Departamento/Servicio. Todas las cuentas de correo no nominativas deberán tener un usuario administrador, siendo este responsable del uso de dichas cuentas y único interlocutor con el D.G. de la Oficina Digital para cualquier petición que se realice sobre las mismas.

e) No ceder el uso de la cuenta de correo a terceras personas. Esto provocaría una suplantación de identidad y el acceso a información "confidencial". 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).

f) Revisar los campos de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la 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.

g) Envío de datos sensibles a través del correo electrónico. En el caso de ser necesario el envío de documentos que contengan datos sensibles/personales por correo electrónico a cuentas externas se deberá cifrar el mensaje según el procedimiento establecido por la D.G. de la Oficina Digital y puesto a disposición en la intranet municipal.

h) No enviar o reenviar correos de forma masiva. Si, previa autorización, 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 su visibilidad 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.

i) 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 al D.G. de la Oficina Digital.

j) 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 deben responderse.

k) 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 ponerlo en conocimiento del D.G. de la Oficina Digital.

l) No remitir información "confidencial" a un remitente desconocido o un contacto habitual siempre que dude de su procedencia, procure verificar siempre con carácter previo la identidad de a quién se lo envía por algún medio que permita verificar la identidad (por ejemplo, firma electrónica).

m) 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.).

n) Informar de correos con virus, phishing, malware, etc. sin reenviarlos. Si la persona usuaria detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente según el procedimiento establecido por la D.G. de la Oficina Digital y puesto a disposición en la intranet municipal y no reenviarlo, para evitar su posible propagación.

o) El acceso a cuentas de correo personales/gratuitas (Gmail, Yahoo!, Hotmail, etc.) desde los equipos (fijos o móviles) puestos a disposición del personal, supone una amenaza a la seguridad, por lo que su uso no está permitido.

p) Medidas a aplicar en el navegador usado para acceder al correo: 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.

Artículo 24.

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

a) Falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.

b) Leer o acceder a correos electrónicos ajenos, sin autorización previa.

c) Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos tipificados como "confidencial", salvo que se adopten medidas de cifrado o similares. Será el D.G. de la Oficina Digital el encargado de autorizarlo y de implementar las medidas de cifrado.

CAPÍTULO XIII. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

Artículo 25.

1. 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:

a) **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.

b) **Uso de navegador suministrado:** Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por el D.G. de la Oficina Digital en los puestos de usuario, no pudiendo alterarse la configuración del mismo ni utilizar un navegador alternativo.

c) **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.

d) **Comunicación de anomalías:** Deberá notificarse al D.G. de la Oficina Digital 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.

e) **Conexiones autorizadas:** Las conexiones a Internet solo podrán ser realizadas utilizando los medios facilitados por el D.G. de la Oficina Digital. La conexión de los sistemas a redes inalámbricas o de otro tipo deberán contar con la autorización expresa del D.G. de la Oficina Digital.

Artículo 26.

1. Se consideran **usos prohibidos** los siguientes:

a) La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

b) La descarga de aplicaciones informáticas, sin la autorización previa del D.G. de la Oficina Digital, 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.

c) El acceso a recursos y sitios web, o la descarga de aplicaciones informáticas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

d) La utilización de aplicaciones o herramientas (especialmente, el uso de aplicaciones informáticas de intercambio de información, P2P) para la descarga masiva de archivos, aplicaciones informáticas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por el D.G. de la Oficina Digital.

e) La visualización de contenidos multimedia (videos, música, etc.) que no estén relacionados con los fines profesionales.

CAPÍTULO XIV. TRABAJO FUERA DE LAS DEPENDENCIAS MUNICIPALES

Artículo 27.

1. 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.

2. El D.G. de la Oficina Digital podrá habilitar el acceso remoto para el uso de recursos informáticos fuera de las dependencias municipales previa solicitud por parte de la persona Responsable de la persona usuaria. Además de las normas específicas para el trabajo fuera de las instalaciones que puedan ser establecidas por el Comité de Seguridad, las personas usuarias deberán tener en consideración:

a) **Conexión:** Para el acceso a los servicios del Ayuntamiento, se deberán utilizar exclusivamente los medios ofrecidos por el Ayuntamiento, salvo autorización expresa de la D.G. de la Oficina Digital.

b) **Seguridad durante la conexión:** Cada persona usuaria 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.

c) **Desconexión**: Una vez finalizada la sesión, la persona usuaria deberá realizar la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.

CAPÍTULO XV. INCIDENCIAS DE SEGURIDAD

Artículo 28.

1. Cuando una persona usuaria 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 Las Rozas o su imagen, deberá informar inmediatamente al D.G. de la Oficina Digital a través del CAU, que lo registrará debidamente y elevará al Comité de Seguridad de la Información, en caso de que sea necesario.

Artículo 29. Gestión de incidencias de seguridad con afectación a datos personales:

1. Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

2. La gestión de incidencias de seguridad se realizará de acuerdo a los dispuesto en el Artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 así como con la Guía de Notificación de Brechas de Datos Personales, y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

CAPÍTULO XVI. ACCESO Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS

Artículo 30.

1. En el Ayuntamiento se consideran zonas de acceso restringido las siguientes:

   a) **Centro de Proceso de Datos (CPD):** salas donde se ubican los servidores corporativos.

   b) **Cuartos Técnicos de Telecomunicaciones:** salas donde se ubican los racks de telecomunicaciones de las dependencias municipales y/o sistemas de telefonía.

Artículo 31.

1. Así mismo, se consideran diferentes tipos de perfiles de acceso:

   a) **Acceso permanente:** personal que realiza tareas habituales en las salas de operación y en el CPD, y que dispone de mecanismo de acceso asignado a su nombre, personal e intransferible. Aunque el acceso sea permanente podrían existir limitaciones horarias en función del grupo al que pertenezcan.

   b) **Acceso ocasional (temporal):** personal interno o externo del Ayuntamiento que debe realizar tareas ocasionales durante un periodo de tiempo definido, y a los que se debe proveer de autorización temporal.

Artículo 32.

1. Los terceros, en la medida que les sea de aplicación, deberán cumplir las siguientes normas, así como el resto de las normativas de seguridad del Ayuntamiento.

a) Acceso y permanencia en los edificios, instalaciones y dependencias:

   i. Los terceros que temporalmente deban acceder a los edificios, instalaciones o dependencias del Ayuntamiento, deberán hacerlo siempre bajo la supervisión de algún miembro de esta y previa autorización de la persona Responsable del departamento afectado.

   ii. 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, pasillos, salas de espera, etc.).

b) Acceso lógico a los sistemas de información del Ayuntamiento de Las Rozas: Para los accesos (incluido el acceso remoto) al sistema de información municipal, por parte de terceros, se crearán credenciales de usuario temporales que serán eliminadas una vez concluido su trabajo. 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 al D.G. de la Oficina Digital.

2. Cualquier incidencia que pudiera afectar o comprometer la seguridad de los sistemas de información del Ayuntamiento, durante el acceso de terceros, deberá de ponerse en conocimiento del D.G. de la Oficina Digital, a la mayor brevedad posible.

CAPÍTULO XVII. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

Artículo 33.

1. 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:

a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

b) Monitorizará los accesos a la información contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y aplicaciones.

d) Monitorizará los servicios de Internet, correo electrónico, impresión y copia, así otras herramientas de colaboración.

2. Con este fin, se registrará la actividad de las personas usuarias, 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.

3. Dicha información formará parte de un tratamiento responsabilidad del Ayuntamiento de Las Rozas. La legitimación para el tratamiento se encuentra amparada en el artículo 6.1 c) y e) del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD): cumplimiento de una obligación legal y cumplimiento de una misión realizada en interés público o en el

ejercicio de poderes públicos conferidos al responsable del tratamiento y además, se atenderá a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica).

3. 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.

4. Las personas afectadas podrán ejercitar los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad, dirigiendo su solicitud a (solicitudes_ARCO@lasrozas.es), o bien por correo postal al Ayuntamiento de Las Rozas – Plaza Mayor, 1, 28231 Las Rozas de Madrid (Madrid) indicando en el asunto: Ref. Protección de Datos.

Artículo 34.

1. En caso de considerar vulnerado su derecho a la protección de datos personales, las personas afectadas pueden interponer una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es). Con carácter previo, podrá contactar con el Delegado de Protección de Datos del Ayuntamiento de Las Rozas.

2. Esta supervisión se realizará, 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.

Artículo 35.

1. 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.

2. 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. 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.

3. 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.

CAPÍTULO XVIII. INCUMPLIMIENTO DE LA NORMATIVA

Artículo 36.

1. Todas las personas usuarias del Ayuntamiento de Las Rozas y aquellas incluidas en el ámbito de aplicación de esta norma están obligadas a cumplir lo prescrito en la presente Normativa General de Utilización de los Recursos y Sistemas de Información.

2. El Director General de la Oficina Digital en colaboración con las restantes áreas/departamentos y unidades del Ayuntamiento de Las Rozas, velará por el cumplimiento de la presente normativa e informará al Comité de Seguridad de la Información sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

Artículo 37.

1. En el supuesto de que una persona usuaria 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.

2. 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.

CAPÍTIULO XIX. REGISTRO DE INCIDENCIAS RELACIONADAS CON DATOS DE CARÁCTER PERSONAL

Artículo 38. Creación del Registro de Incidencias Relacionadas Con Datos De Carácter Personal del Ayuntamiento de Las Rozas de Madrid

1. Mediante el presente se crea el Registro de Incidencias Relacionadas Con Datos De Carácter Personal del Ayuntamiento de Las Rozas de Madrid a fin de dar cumplimiento a las obligaciones de registro, documentación y notificación de las incidencias y brechas de seguridad que dispone el Reglamento (UE) 2016/679 General de Protección de Datos así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Este registro queda adscrito a la Oficina de la Junta de Gobierno Local y de conformidad con el Reglamento Orgánico de Gobierno y Administración Municipal.

3. Podrá otorgarse habilitación a los funcionarios en situación de servicio activo, que dispondrán de un certificado electrónico de empleado público.

4. Además de la Inscripción de aquellas incidencias que determina la legislación en materia de protección de datos se incluirán en este registro aquellas incidencias de los sistemas de información y recursos informáticos que por su naturaleza o impacto se acuerde por parte de la D.G de la Oficina Digital.

Artículo 39. La notificación de brechas de datos personales que puedan suponer un riesgo para los derechos y libertades de las personas físicas a la Autoridad de Control competente

1. De conformidad con el Art. 33 del Reglamento (UE) 2016/679 General de Protección de Datos en caso de violación de la seguridad de los datos personales, el Ayuntamiento de Las Rozas, como responsable de tratamiento, notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que se haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

2. Si la notificación a la autoridad de control se realizara en el plazo de 72 horas, se acompañará de la indicación de los motivos de la dilación.

3. Los concesionarios, adjudicatarios o demás entes que ejercieran como encargados del tratamiento en relación a la administración municipal, en todo caso, notificarán sin dilación indebida al Ayuntamiento de Las Rozas las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

4. La notificación contemplada en el apartado 1 deberá:

   a) Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
   b) Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
   c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
   d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos

5. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Ayuntamiento de Las Rozas la comunicará al interesado sin dilación indebida de acuerdo a las prescripciones del Artículo 34 del Reglamento (UE) 2016/679 General de Protección de Datos.

6. Una vez detectada y evaluada la brecha de datos personales, durante su resolución se debe documentar el proceso con toda la información que se vaya recopilando. Esta documentación será adjuntada al registro de incidentes del Ayuntamiento de las Rozas. El registro y evaluación de la brecha de seguridad contendrá al menos, los siguientes criterios, los cuales deberán ser debidamente registrados y justificados:

a) Incorporar un procedimiento de notificación de brechas de datos personales que concrete todos los aspectos fundamentales que sean necesarios para la correcta aplicación de la legislación en materia de Protección de Datos.
b) Aprovisionar los medios técnicos o de cualquier índole necesarios para notificar, asegurar cumplimiento de los plazos, y en su caso establecer procedimiento de

autorizaciones que se requiera para notificar conforme a las instrucciones del responsable del tratamiento.

c) Establecer un procedimiento para la comunicación a los afectados en el que se concreten aspectos como quién realizará las comunicaciones, cómo se comunicará a los afectados, los canales y medios y en general los detalles que permitan comunicar de forma efectiva.

ANEXO I – PERSONAL DE TERCERO

1. 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) El Ayuntamiento no le 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 D.G. de la Oficina Digital de la Rozas.

b) Todas las peticiones o actuaciones que en la presente Normativa que precisen de autorización previa y se haga referencia a "la persona Responsable de la persona usuaria", deberá de ser tramitada por la persona Responsable del Área/Departamento/Servicio responsable del expediente del que dependa la persona usuaria externa.

c) La persona usuaria externa deberá acceder a los sistemas municipales exclusivamente para realizar las tareas encomendadas teniendo en cuenta las directrices indicadas por la persona Responsable del expediente del que dependa, así como aquellas indicadas por el personal de la D.G. de la Oficina Digital.

d) Será responsabilidad de la entidad de la que depende el usuario externo, 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.

e) La persona usuaria externa, no dispondrá en ningún caso cuenta nominativa de correo electrónico institucional (@lasrozas.es). En caso de que la persona usuaria externa precise de una cuenta de correo se le asignará una cuenta genérica que deberá ser solicitada por la persona Responsable del Área/Departamento/Servicio responsable del expediente del que dependa la persona usuaria externa, debiéndose notificar una persona responsable de la misma siendo éste 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 Concejalía, departamento o servicio.

f) El responsable del contrato por parte del Ayuntamiento será el través del CAU las Altas, Bajas y modificaciones de los usuarios externos, así como de los permisos y accesos que se necesiten para la realización de sus funciones.

g) Respecto al uso de software municipal que pudiera ser necesario instalar en el equipamiento del personal de terceros por necesidades del objeto del contrato, en ausencia de cláusulas/contrato previo de instalación se actuará en base a las instrucciones específicas que dicte el Comité de Seguridad.

ANEXO II – DECLARACIÓN DE USUARIO

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la <<ENTIDAD>>/empleado de la <<EMPRESA>>*], como usuario de recursos informáticos y sistemas de información de la <<ENTIDAD>>, declara haber leído y comprendido las Normas de Creación y Uso de Contraseñas de la <<ENTIDAD>> (*versión x*) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a ____ de _____ de 20__>>

Entidad:	
Trabajador (Nombre y Apellidos)	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por la <<ENTIDAD>>: <<*Nombre y Apellidos*>>

DNI número: _____

Número de Registro de Personal: _____