Nº resolución:
2025002440
Fecha resolución:
12/06/2025

| | |
|---|---|
| Referencia: | **2025/00003473H** |
| Procedimiento: | **Estudios e Informes** |
| Solicitud: | Estudios e Informes |
| **Informática (LMRN)** | |

RESOLUCIÓN

En virtud de contrato suscrito en fecha 30 de abril de 2024, la mercantil SEGURDADES S.L. desarrolla para este Ayuntamiento el servicio de "ADECUACIÓN AL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES, ASÍ COMO EL MANTENIMIENTO DEL CUMPLIMIENTO DE LAS OBLIGACIONES DERIVADAS DE LA CITADA NORMATIVA".

Entre las prestaciones objeto de dicho contrato figuran, entre otras, las relacionadas con la realización de análisis de riesgos e implementación de medidas de seguridad, tanto técnicas como organizativas y jurídicas.

En cumplimiento parcial de dicho extremo, en fecha 29 de abril se presenta borrador de política de protección de datos, que es facilitado al Delegado de Protección de Datos municipal que, a su vez, en fecha 15 de mayo presenta propuesta de ampliación con regulación de un apartado específico dedicado al acceso a expedientes administrativos.

La redacción final del documento es validada por el DPD en fecha 5 de junio.

Considerando el art. 24, en sus apartados 1 y 2, del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD):

*"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

*2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos."*

Considerando, asimismo, lo establecido por el art. 39.1 b) de la mencionada norma:

*"El delegado de protección de datos tendrá como mínimo las siguientes funciones:*
*(…)*
*b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;"*

Considerando que la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPD) señala, asimismo, en el apartado primero de su art. 28:

*"Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento."*

Considerando que la competencia para la aprobación de este instrumento es de Alcaldía, de conformidad con lo previsto en el art. 21.1 s) de la Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local; y resolución nº 2727 de 2023, en virtud de la cual la Alcaldía es competente en materia de modernización y nuevas tecnologías.

Visto el expediente
Esta Alcaldía, RESUELVE:

**PRIMERO**.- Aprobar la política de protección de datos del Ayuntamiento de Llíria cuyo texto se transcribe a continuación:

## POLÍTICA DE PROTECCIÓN DE DATOS.

### 1.- DECÁLOGO DE LOS DIEZ PUNTOS BÁSICOS.

1. Es necesario acceder con el nombre de usuario y contraseña habilitado por la entidad, y que lo identifica de forma personal, sin que sea permitido en ningún caso su utilización compartida o anotación en ningún medio, que permita el acceso a otra persona.

2. Cualquier sistema o soporte de telecomunicaciones, informático o sistema que la entidad ha puesto a su disposición para la realización de tareas profesionales, no puede ser utilizado por ninguna otra finalidad personal o particular.

3. No se permite la descarga, instalación o incorporación de ningún programa o servicio informático por parte de los usuarios, para evitar vulnerar la normativa de protección de datos, así como los derechos de propiedad intelectual inherente a estos.

4. Hay que garantizar que solo las personas expresamente autorizadas puedan acceder a la información. Cada trabajador es responsable de no dejar documentos sobre las mesas, estanterías o espacios que puedan ser visionados por terceros.

5. Cualquier documento que sea rechazado tiene que ser, previamente, destruido de forma confidencial con una destructora de papel o con el servicio de destrucción confidencial que disponga la entidad.

6. No se permite la grabación, custodia de datos o información en soportes externos sin disponer de la autorización expresa del responsable del departamento o informático; y sin disponer de las medidas de seguridad que permitan el no acceso a terceros.

7. Todos los correos electrónicos tienen que ser enviados mediante copia oculta, si se realiza a varios destinatarios, salvo que estos tengan relación previa entre ellos y dispongan de los correos electrónicos que figuran en el correo.

8. Hay que guardar el más estricto secreto profesional sobre cualquier dato o información responsabilidad de la empresa, incluido una vez extinguida la relación jurídica entre las dos partes.

9. Será necesario el cumplimiento más respetuoso de la normativa de protección de datos, así como la confidencialidad respecto a toda la información de la empresa, pudiendo exigir las responsabilidades que se puedan derivar por la vulneración del secreto profesional por parte de los empleados.

10. El trabajador tiene la obligación de notificar, sin demora injustificada, cualquier incidencia que suponga una pérdida de información, la falta de disponibilidad de los datos, la alteración de la integridad de los datos personales o la revelación a terceros de estos. El responsable o el Delegado de Protección de datos, valorará la existencia de una violación de seguridad y procederá a su notificación ante la autoridad competente. Habrá que tener presente que el plazo de comunicación es de 72 horas desde que se tiene conocimiento de ella.

El trabajador tendrá que leer atentamente el texto entero de funciones y obligaciones que le afecta como trabajador, así como cualquier otro comunicado, instrucción o nota informativa que se reciba; y cumplir con las pautas expuestas.

**2.- FUNCIONES Y OBLIGACIONES DE LOS USUARIOS.**

El personal que trabaje con los sistemas de información o acceda a cualquier información, dato o documento de esta entidad tiene que cumplir las normativas siguientes (y/o cualesquiera otra que las complemente o sustituya):

- RGPD 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales, en especial su artículo 5 que establece el deber de secreto profesional del responsable del tratamiento y de todos los que intervengan en cualquier fase del tratamiento de los datos de carácter personal y el deber de

guardarlos, obligaciones que se mantienen después de finalizar las relaciones con el titular del fichero o, si procede, con el responsable.

- Código Penal, en concreto el capítulo dedicado al delito del descubrimiento y revelación de secretos.

**2.1.- Tratamiento de datos e información confidencial.**

El tratamiento de datos personales implica que la entidad tenga que aplicar aquellas medidas técnicas y organizativas necesarias para poder garantizar la confidencialidad, disponibilidad e integridad de los datos, dando cumplimiento a las exigencias legales determinadas en la normativa de protección de datos.

Hay que recordar que la entidad es la responsable del tratamiento de los datos, siendo su titular el único propietario del mismo, y por tanto, la entidad no tiene una libre disposición sobre los datos; y que en muchas ocasiones, la información que se trata puede no ser objeto de protección por esta normativa al no ser datos personales pero que hay que garantizar su confidencialidad por cuestiones de propiedad intelectual, industrial o acuerdos contractuales.

Por estos motivos, será necesario que cualquier usuario que realice un tratamiento de datos o de información confidencial cumpla de forma escrupulosa con estas funciones y obligaciones, y advierta a su responsable en el caso de que detecte el incumplimiento de estas.

**2.2.- Creación o modificación de ficheros o tratamientos con datos de carácter personal.**

La creación, modificación o supresión de uno o más Registros de actividad o bien de ficheros que conforman la estructura básica de estos, se tiene que proponer a la Secretaría municipal, que en su caso realizará las actuaciones pertinentes, incluyendo la notificación al responsable de la entidad o la persona encargada de gestionar el cumplimiento de la normativa de protección de datos.

Asimismo, también hay que notificar cualquier cambio que afecte la finalidad y que la haga sustancialmente diferente o incompatible con la finalidad original.

Es necesaria la autorización previa del órgano competente, en cualquier caso, para:

- Crear ficheros o tratamiento de datos personales.
- Utilizar los datos personales para finalidades incompatibles con aquellas para las cuales los datos se hayan recogido o para finalidades distintas a las comunicadas.
- Cualquier otra actividad expresamente prohibida en este documento o en la normativa vigente.

**2.3.- Utilización de sistemas informáticos, aplicaciones o telecomunicaciones.**

Con carácter general, el uso de los sistemas informáticos, aplicaciones y de telecomunicaciones de la entidad se hará por motivos estrictamente profesionales, tal y como se detalla en los puntos siguientes.

No están autorizadas las siguientes actividades:

- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, los programas o los documentos electrónicos del Responsable o de terceros, sin autorización.
- Utilizar la red de la institución y/o la intranet de esta entidad y sus datos e incurrir en actividades que puedan ser consideradas ilícitas o ilegales que infrinjan los intereses de la institución o de terceros.
- Aprovechar los recursos y sistemas para una finalidad diferente de la prevista.
- Manipular físicamente el hardware disponible para intentar permitir el acceso a capacidades deshabilitadas con ánimo de vulnerar la seguridad de los sistemas.
- Obstaculizar voluntariamente el acceso de otros usuarios en la red mediante el consumo masivo de los recursos informáticos y telemáticos, y llevar a cabo acciones que dañen, interrumpan o generen errores en estos sistemas.
- Introducir voluntariamente programas, virus, macros, applets, apps, controles activeX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos propios y/o de terceros. Si se quiere utilizar programas de control remoto que puedan acceder a los sistemas, aplicativos y/o cualquier directorio hay que disponer de la autorización previa de la entidad.
- Utilizar los sistemas sin los programas antivirus correspondientes y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento conocido destinado a destruir o corromper los datos informáticos.
- Utilizar métodos de grabación de datos, como pueden ser discos duros externos, USB… sin ninguna medida de seguridad. Estos dispositivos siempre tienen que ser cifrados o con medidas de protección frente a terceros no autorizados; todo ello sin perjuicio de lo señalado en el punto 6 del decálogo inicial.

**2.4.- Propiedad intelectual e industrial.**

No está permitida la instalación y el uso de programas informáticos sin la licencia correspondiente, y también el uso, la reproducción, la cesión, la transformación o la comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

No está permitida la descarga de ningún tipo de material de audio o video no relacionada directamente con el puesto de trabajo y sin el conocimiento ni la autorización previa del Responsable del departamento correspondiente.

**2.5.- Gestión de acceso lógico.**

En relación con este punto las personas usuarias tienen que cumplir los siguientes aspectos:

- Hay que inicializar la contraseña antes del primer acceso de un usuario nuevo al sistema.
- El uso del identificador y la contraseña garantizan una identificación inequívoca e implican la aceptación de la responsabilidad.
- La sesión de usuario expirará en caso de un periodo de inactividad superior a 10 minutos como máximo. No obstante, hay que apagar los equipos informáticos (pc`s) cuando finalice cada jornada laboral.
- La contraseña no puede tener caracteres en blanco.
- La contraseña tiene que ser de longitud mínima de 8 caracteres.

- El identificador y la contraseña tienen que ser diferentes.
- La contraseña tiene que contener como mínimo un carácter alfabético, uno numérico, y un carácter especial; así como mayúsculas y minúsculas. No podrá ser igual a las tres últimas contraseñas utilizadas.

No están permitidas las actividades siguientes:

- Compartir o facilitar el identificador de usuario y la clave de acceso facilitados por esta entidad a otra persona física o jurídica. En caso de incumplimiento de esta prohibición, la persona usuaria es la única responsable de los actos llevados a cabo por la persona física o jurídica que utilice de forma no autorizada su identificación de usuario. Dejar anotadas las contraseñas en lugares visibles por terceros como por ejemplo post-it en monitores y otros soportes documentales que pueden poner en entredicho la seguridad y confidencialidad de las contraseñas.
- Intentar distorsionar o falsear los registros del sistema.
- Intentar descifrar las claves, los sistemas o los algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la entidad.
- Utilizar los sistemas para intentar acceder en áreas restringidas de los sistemas informáticos o de terceros.
- Intentar suplantar otro usuario.
- Intentar crear o modificar usuarios o perfiles sin autorización.

**2.6.- Uso del correo electrónico y mensajería.**

Se considera correo electrónico tanto el interno, entre terminales de la red de la entidad, como el externo, dirigido o proveniente de otras redes privadas o públicas.

Cualquier fichero introducido en la red de la entidad o en el terminal del usuario a través de mensajes de correo electrónico, proveniente de redes externas, tiene que cumplir los requisitos establecidos en estas normas, especialmente las que hacen referencia a la seguridad del tratamiento de datos personales, propiedad intelectual e industrial y al control de virus.

La entidad se reserva el derecho de revisar los archivos con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la entidad.

- Las direcciones de correo electrónico dirigidas a personas se consideran datos personales, por lo cual, en caso de enviar correos además de un destinatario, si no es estrictamente necesario que los otros vean las direcciones de correo del resto, hay que hacerlo como copia oculta «Cco».

Se prohíben expresamente las actividades siguientes:

- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otras personas usuarias. Esta actividad puede constituir un delito de interceptación de las telecomunicaciones (revelación de secretos), previsto en el artículo 197 del Código Penal.
- Enviar mensajes de correo electrónico de manera masiva sin un motivo profesional y sin respetar la normativa de protección de datos y la Ley de la Sociedad de la Información y el comercio electrónico.

- Enviar o reenviar mensajes en cadena o de tipo piramidal.

**2.7.- Copias de seguridad.**

La entidad realiza copias de seguridad de la documentación, información y datos para poder garantizar la continuidad de su actividad, así como cumplir con las exigencias de integridad de la normativa de protección de datos.

Es necesario que toda la actividad sea almacenada en el espacio del sistema informático indicado por el responsable para garantizar su correcta realización.

**2.8.- Tratamiento de datos en soporte manual o papel.**

El tratamiento de datos en papel implica que la participación e implicación de todos los usuarios de datos sea más relevante para cumplir con la obligación de confidencialidad debida.

Cada usuario tiene que garantizar que los datos en soporte papel que trate, disponga o almacene, no sean accesibles a terceros no autorizados y cumplir las siguientes condiciones:

- Será necesario que en las zonas de trabajo no se disponga de datos visibles en los documentos a personas ajenas que puedan acceder. Habrá que voltear cara abajo las hojas de manera que no pueda leerse su contenido o almacenarlo en carpetas.
- En el traslado de documento de papel habrá que asegurar que se adoptan las medidas necesarias para evitar la pérdida o acceso por terceros. No se permite extraer documentación en papel si no es imprescindible y será necesario que se custodie con carpetas con gomas, carteras con cremallera o similares.
- Cualquier documento que contenga un solo dato personal no puede ser tirado a una papelera sin destruir previamente. Se requiere que este documento sea previamente triturado o dejado en el espacio indicado por la destrucción de documentos sensibles o con datos, para que la entidad lo destruya con el sistema de destrucción segura.

**2.9.- Información en la recogida de datos, consentimiento de la persona afectada y cesiones o comunicaciones de datos de las personas que autorizan el tratamiento.**

La entidad, como responsable de tratamiento, tiene que informar a la persona interesada de manera expresa, precisa e inequívoca, en el momento de obtener los datos, acerca de la información siguiente:

- Existencia de un tratamiento de datos personales, con el fin de recoger estos datos y los datos de los destinatarios de la información.
- Carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas.
- Consecuencias de obtener los datos o de negarse a suministrarlos.
- Identidad y dirección del responsable del tratamiento, y del delegado de Protección de datos, si procede.

- El responsable ante el cual pueden ejercerse los derechos de acceso, oposición, rectificación, supresión, limitación del tratamiento o portabilidad de los datos personales, y la manera como se puede hacer.
- Intención del responsable de transferir datos personales a un tercer país.
- Plazo de conservación de los datos.
- La existencia de decisiones automatizadas.
- Posibilidad de presentar una reclamación a la Autoridad de Control que corresponda

Cuando se utilicen cuestionarios u otros impresos para recoger datos, hay que incluir la información básica de protección de datos con una referencia al sitio web donde consultar los datos adicionales, si así se considera para limitar la extensión del texto.

Cuando la persona interesada utilice otros medios de comunicación habrá que informarla de la política de protección de datos. En caso de que sea en formato papel o electrónico, habrá que remitir el enlace o adjuntar un anexo en la contestación, donde se describe la política de privacidad y protección de datos del responsable del tratamiento.

Tal y como establece el artículo 6 y siguientes del RGPD, no es necesario el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de esta entidad, el cumplimiento de una obligación legal o se cumple con alguno de los otros motivos de licitud establecido por este artículo 6.

Si durante el transcurso de la actividad de la entidad, fuere necesario ceder o dar acceso a datos de carácter personal a terceros; se hará siempre respetando los derechos de los titulares de las mismos y conforme la regulación establecida en los arts. 6 y 9 RGPD.

### 2.10.- Respecto al ejercicio de los derechos ARCO+.

Cualquier persona tiene el derecho a ejercitar los derechos previstos en la normativa de protección de datos, y por tanto exigir el acceso, rectificación, supresión, limitación de tratamiento, oposición o portabilidad de los datos. Estas peticiones no requieren que se realicen con un formato o metodología normalizado y por tanto, estas peticiones pueden hacerse por varios medios.

En el supuesto de que se reciba una petición de ejercicio de derechos reconocido por la normativa de protección de datos, hace falta que se comunique a la mayor brevedad posible al responsable de la unidad administrativa correspondiente para poder recabar la pertinente información al respecto y dar respuesta en el plazo legal máximo de un mes.

### 2.11.- Incidencias y Violaciones de seguridad.

#### 2.11.1.- Incidencia.

Se considera incidencia cualquier acto u omisión que tenga como consecuencia la destrucción accidental o voluntaria, lícita o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de cualquier tipo de información responsabilidad de la entidad, ya sea digital o bien analógica.

El personal tiene la obligación de notificar, sin demora injustificada, cualquier incidencia que descubra a su responsable, para que este tenga conocimiento y, si lo estima oportuno, lo comunique al coordinar legal o de sistemas informáticos, dependiendo de la naturaleza de la incidencia.

Ser consciente de una incidencia por parte del personal y no notificarla se considera una falta contra la seguridad de la información y puede suponer el inicio de acciones legales, así como la reclamación de indemnizaciones, sanciones y daños o perjuicios que el Responsable del Tratamiento se vea obligado a atender como consecuencia de este incumplimiento.

Serán consideradas incidencias, de forma general y no excluyente:

- La pérdida o falta de disponibilidad de datos de carácter personal (pérdida de portátil, expediente papel o teléfono móvil por ejemplo o la entrada de un virus encriptador).
- La revelación a terceros de datos de carácter personal (por ejemplo, enviar un correo electrónico a un destinatario no deseado o hacerlo con copia vista a varios destinatarios que no se conozcan entre ellos).

El procedimiento para la notificación y la gestión de incidencias incluye la comunicación de la incidencia por parte de la persona usuaria donde conste el tipo de incidencia, el momento en que se ha producido/detectado, la persona que la notifica, la persona a quien se le comunica, los posibles efectos que se derivan y las medidas correctoras iniciales aplicadas.

La notificación de la incidencia será necesario que se realice a través del medio que en su caso se establezca al efecto, o bien mediante correo electrónico al responsable de la unidad administrativa.

**2.11.2.- Violación de seguridad.**

Se considera una violación de seguridad cualquier incidencia de las mencionadas anteriormente que tenga que ver con datos personales y representen un riesgo para las personas físicas.

En términos generales y no excluyentes, serán consideradas violaciones de seguridad, cuando nos encontramos ante cualquiera de las siguientes situaciones:

- Vulneración de la confidencialidad de los datos personales (enviar un correo a un destinatario no autorizado, perder un teléfono móvil, pérdida de un expediente en papel etc..)
- Alteración de la integridad de los datos personales (acción de un virus informático tipo criptolocker, cruzamiento de datos erróneo etc..)
- Pérdida de datos personales (indistintamente si son datos en papel o en soporte informático)

Cualquier incumplimiento de la normativa que establece este documento de seguridad y cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal de la institución se considera una violación de seguridad.

Hay que tener presente que la violación de seguridad hay que comunicarla como máximo a las 72 horas de tener conocimiento de ella a la autoridad de protección de datos competente. Con independencia de la notificación a la autoridad pertinente, el responsable del tratamiento tendrá que documentar todas las violaciones de seguridad tal y como establece el RGPD en la misma línea que dictaba el Reglamento de desarrollo de la anterior LOPD con el registro de incidencias.

**2.12.- Confidencialidad de la información y deber de secreto.**

Hay que evitar la remisión de información confidencial de la entidad al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluidos la simple visualización de esta información o el acceso.

Los usuarios de los sistemas de información o con acceso a cualquier dato o información tienen que guardar durante un tiempo indefinido la máxima reserva, y no divulgar directamente ni a través de terceras personas o empresas, bajo su responsabilidad, datos, documentos, metodologías, claves, análisis, programas y otra información a la cual tengan acceso durante su relación laboral con la institución, tanto en soporte material como electrónico. Esta obligación continúa vigente después de la finalización de la relación laboral con esta entidad.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos (artículo 197 del Código Penal).

**2.13.- Uso de dispositivos o sistemas particulares.**

Los terminales móviles, ordenadores, tabletas o cualquier otro dispositivo particular del personal no son equipos que formen parte de la plataforma tecnológica de esta entidad, por lo tanto, no están integrados bajo el arco de protección de la misma.

En relación con su utilización durante la jornada laboral únicamente está permitido por motivos de urgencia y conciliación familiar, de forma puntual y responsable, con especial relevancia en cuanto a los sistemas de mensajería instantánea.

En el supuesto que se utilicen estos dispositivos particulares para tratar datos responsabilidad de esta entidad, (por ejemplo, tener configurado el correo electrónico corporativo o acceder de forma remota al servidor o a aplicaciones online de tratamiento de datos) la persona usuaria tiene que disponer de la autorización de su responsable y se tiene que dirigir al responsable de medidas tecnológicas para que se verifique la seguridad del dispositivo.

En todos los casos hará falta que se apliquen las medidas de seguridad detalladas en este protocolo, comprometiéndose el usuario a garantizar la confidencialidad e integridad de los datos en cuánto el tratamiento no se realiza en la sede de la entidad y/o con medios particulares. A modo de ejemplo, este dispositivo tendrá que ir protegido con un patrón de bloqueo o contraseña, garantizar que terceros no puedan visionar los datos, no tirar documentos con datos sin destruir previamente, no emplear sistemas no seguros para la transmisión de datos.

**2.14.- Garantía de los derechos digitales.**

Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral recogido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en sus arts. 87, 88 y 89.

La entidad podrá adoptar los acuerdos pertinentes con cada trabajador, según su cargo, responsabilidades, y características de su puesto de trabajo, para definir las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal. El personal tendrá derecho a la desconexión digital para garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respecto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Por este motivo, se determina que los responsables de los departamentos y/o áreas se someterán a un régimen de total disponibilidad y localización telefónica las 24 horas del día por 365 días el año, y quedará sometido a la máxima disponibilidad en situaciones de urgencia. El resto de los trabajadores se sujetarán al derecho a la conciliación de la actividad laboral y la vida personal y familiar, siendo solo contactados en su horario laboral o por cuestiones de máxima urgencia fuera de su horario laboral si la espera comportase graves y significativos perjuicios o pérdidas por la entidad. Todo ello, en cualquier caso, sin perjuicio de las condiciones del puesto de trabajo de conformidad con los instrumentos organizativos que consten aprobados en cada momento.

## 3.- REGULACIÓN DEL ACCESO A EXPEDIENTES ADMINISTRATIVOS.

### 3.1.- Principio General de Acceso.

El personal del Ayuntamiento solo podrá acceder a expedientes administrativos (electrónicos o en papel) que guarden relación directa con sus funciones laborales o competencias asignadas, conforme al principio de minimización de datos (Art. 5.1.c RGPD). Queda expresamente prohibido el acceso, consulta o manipulación de expedientes ajenos al ámbito de sus responsabilidades, salvo autorización expresa del responsable correspondiente.

### 3.2.- Permisos y obligaciones del personal.

1. Delimitación de Acceso:

   - Cada departamento o unidad administrativa accederá como regla general, únicamente, a los expedientes cuya tramitación le competa. Los departamentos con funciones transversales que impliquen la necesidad de revisión de los expedientes (esencialmente Intervención, Tesorería y Secretaría) podrán tener un nivel de acceso que trascienda el puramente departamental.
   - Cada departamento propondrá y asignará a su vez niveles de acceso a los expedientes en función de las responsabilidades específicas de los puestos de trabajo.
   - El personal deberá utilizar sus credenciales de acceso únicas y personales (nunca compartidas).

2. Sistemas Electrónicos:

- Las plataformas digitales incorporarán controles de acceso basados en roles (RBAC), limitando la visibilidad de expedientes a aquellos vinculados con las tareas del usuario.

3. Expedientes en Papel:

- Los documentos físicos se custodiarán en archivos con acceso restringido, y solo el personal autorizado podrá retirarlos o consultarlos, previo registro en un libro de control de accesos.

**3.3.- Prohibiciones Explícitas.**

- Acceso por curiosidad, interés personal o motivos ajenos a las funciones laborales.
- Compartir información de expedientes con terceros no autorizados, incluidos otros empleados sin competencia en el asunto.
- Almacenar, copiar o difundir datos de expedientes fuera de los sistemas y entornos autorizados.

**3.4.- Excepciones.**

Únicamente se permitirá el acceso a expedientes fuera del ámbito competencial cuando:

- Medie una orden judicial o requerimiento policial.
- Exista autorización expresa de la Secretaría/Intervención/Tesorería Municipal, previa justificación documentada.

**SEGUNDO**.- Dar traslado a todo el personal municipal para su conocimiento, y especialmente a los responsables de las diferentes dependencias administrativas, con la instrucción de velar por su cumplimiento y apoyar al personal que se encuentre bajo su dependencia en cualquier cuestión relativa a su observancia.

**TERCERO**.- Dar traslado, asimismo, a todos los grupos municipales y publicar en el portal municipal de transparencia.

FIRMA ALCALDE

Firmado electrónicamente por:
EL ALCALDE
12/06/2025
16:16:42

EL SECRETARIO
JORGE VICENTE VERA GIL
12/06/2025
12:43:21