Seguridad del tratamiento

SEGURIDAD DEL TRATAMIENTO

CUMPLIMIENTO CON LO ESTABLECIDO EN EL ART. 32 DEL REGLAMENTO (UE) 2016/679

audidat
PROTECCIÓN DE DATOS

OBJETIVO DEL DOCUMENTO

El 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (en adelante, RGPD), proporciona un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa.

En tal sentido, el artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento será responsable del cumplimiento (y capaz de demostrarlo), entre otros, del principio de «integridad y confidencialidad», según el cual:

> *Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*

De tal modo, el Considerando 39 del Reglamento (UE) 2016/679 establece lo siguiente:

> *(...) Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.*

Igualmente, el Considerando 83 del Reglamento (UE) 2016/679 establece lo siguiente:

> *(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.*

En su consecuencia, el artículo 32 del Reglamento (UE) 2016/679, bajo el epígrafe "Seguridad del tratamiento" establece lo siguiente:

> *Artículo 32 Seguridad del tratamiento*
>
> *1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
>
> *2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*
>
> *3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*
>
> *4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.*

Como corolario de todo lo anterior, el presente documento se elabora con el propósito de dar cumplimiento a lo establecido en el artículo 32 del precitado 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), referente a la "Seguridad del tratamiento".

ÁMBITO DE APLICACIÓN

Este documento ha sido elaborado bajo la responsabilidad de AYUNTAMIENTO DE LOS NAVALMORALES, que, como responsable del tratamiento, se compromete a adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Su ámbito de aplicación comprende la totalidad de las actividades de tratamiento responsabilidad de AYUNTAMIENTO DE LOS NAVALMORALES relacionadas en el correspondiente registro de las actividades de tratamiento, atendiendo, en todo caso, a las siguientes definiciones recogidas en el 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos):

- «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción; (art. 4.2) RGPD).

- «Datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; (art. 4.1) RGPD).

- «Responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros; (art. 4.7) RGPD).

- «Encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento; (art. 4.8) RGPD).

MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Con carácter general, las medidas de seguridad a que se refiere el artículo 32, apartado 1, del Reglamento (UE) 2016/679, pueden clasificarse en cinco áreas distintas, en cada una de las cuales el responsable del tratamiento ha identificado una serie de posibles medidas técnicas y organizativas que pudieran ser apropiadas en función del riesgo aplicable:

SECCIÓN I: MEDIDAS GENERALES

1. Documento de política de protección de datos de carácter personal

El principio de «responsabilidad proactiva» exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

En tal sentido, la Dirección / Órgano de Gobierno AYUNTAMIENTO DE LOS NAVALMORALES aboga por una política proactiva de cumplimiento en el seno de la misma, en pos de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

En su consecuencia, la entidad responsable del tratamiento debe elaborar un documento con el objeto de establecer su Política en relación con el cumplimiento 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y en la normativa española de protección de datos de carácter personal (Ley Orgánica, sus normas de desarrollo y la legislación sectorial específica).

2. Funciones y obligaciones de los usuarios y normas de uso de los recursos TIC

De conformidad con lo establecido en el artículo 32.4 del RGPD, el responsable del tratamiento deberá tomar las medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable.

En tal sentido, el responsable del tratamiento establecerá una “Política de uso del sistema de información”, entendiéndose por tal las normas de uso del conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto.

3. Capacitación y educación de los usuarios en protección de datos

El responsable del tratamiento se rige, entre otros, por el principio de información y formación, según el cual una de las claves para garantizar la protección de los datos personales es la formación e información que se facilite al personal involucrado en el tratamiento de los mismos, educando a los empleados en la denominada cultura de la protección de datos.

En su consecuencia, todo el personal del responsable del tratamiento con acceso a los datos deberá ser convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la normativa de protección de datos, recibiendo el apropiado conocimiento, capacitación y actualizaciones regulares de la Política de Protección de Datos de la entidad responsable del tratamiento.

4. Inventario de activos de información

El responsable del tratamiento deberá elaborar un listado de todos aquellos recursos físicos (hardware) que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos, siguiendo el siguiente esquema:

- Tipo de activo
    - Ordenador sobremesa
    - Portátil
    - Dispositivo de almacenamiento externo (disco duro, pen drive, etc.)
    - Dispositivo móvil (tableta, smartphone, etc.)
    - Otros: ……
- Número de referencia (000/0000)
- Fecha de creación
- Fecha de destrucción (en su caso)
- Tipo de datos que contiene
- Área / Local de ubicación

SECCIÓN II: MEDIDAS EN MATERIA DE SEUDONIMIZACIÓN Y CIFRADO DE DATOS PERSONALES

1. Medidas técnicas y organizativas de seudonimización

En relación con actividades de alto riesgo, el responsable del tratamiento podrá adoptar medidas técnicas y organizativas de «seudonimización», consistentes en el tratamiento de los datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

2. Software de cifrado de archivos

En relación con actividades de alto riesgo, el responsable del tratamiento podrá adoptar medidas técnicas de cifrado de archivos, consistentes en transformar la información de modo que pase a ser ilegible para todos salvo para las personas autorizadas a acceder a dicha información. En general, el acceso a la información original a partir de su versión cifrada se lleva a cabo mediante el uso de claves y algoritmos.

3. Software de cifrado de correo electrónico

En relación con actividades de alto riesgo, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

SECCIÓN III: MEDIDAS EN RELACIÓN CON LA CAPACIDAD DE GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA PERMANENTES DE LOS SISTEMAS Y SERVICIOS DE TRATAMIENTO

1. Certificación ISO 27001 de Sistemas de gestión de la seguridad de la información (SGSI)

Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza.

2. Adecuación al Esquema Nacional de Seguridad (ENS)

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

3. Sistema de identificación y autenticación de usuarios

3.1. Se adoptarán las medidas que garanticen la correcta identificación y autenticación de los usuarios.

3.2. Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3.3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3.4. Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc. Para ello se seguirán las siguientes pautas en la elección de las contraseñas:

- Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
- No deberán coincidir con el código de usuario.
- No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario (nombre, apellidos, ciudad y fecha de nacimiento, DNI, nombres de familiares, matrícula del coche, etc.).

3.5. Las contraseñas deberán ser cambiadas, como mínimo, cada seis meses, debiendo almacenarse de forma ininteligible mientras estén vigentes.

4. Sistema de gestión de privilegios de acceso

4.1. El personal propio o ajeno solo deberá acceder a aquellos datos y recursos que precise para el desarrollo de sus funciones.

4.2. Deberá existir una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

5. Límite de intentos reiterados de acceso no autorizado

En relación con actividades de alto riesgo, deberá existir un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

6. Sistema de control de acceso al sistema de información

6.1. El responsable del tratamiento deberá establecer mecanismos para evitar que un usuario pueda acceder datos y recursos con derechos distintos de los autorizados.

6.2. Exclusivamente el responsable del tratamiento o las personas autorizadas por el mismo podrán conceder, alterar o anular el acceso autorizado sobre los datos y recursos.

7. Registro de accesos al sistema de información

En relación con actividades de alto riesgo, se deberá establecer un registro de accesos de acuerdo a los siguientes criterios:

- De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de accesos estarán bajo el control directo de la persona responsable de la protección de datos, sin que deban permitir la desactivación ni la manipulación de los mismos.
- El período mínimo de conservación de los datos registrados será de dos años.
- La persona responsable de la protección de datos se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

8. Sistema de firma electrónica (autenticación)

La firma electrónica es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Es una cadena de caracteres, generada mediante un algoritmo matemático, que se obtiene utilizando como variables la clave privada y la huella digital del texto a firmar de forma que permite asegurar la identidad del firmante y la integridad del mensaje.

9. Red privada de comunicaciones electrónicas

Una red privada es administrada y operada por una entidad en particular. Generalmente, los usuarios son empleados o miembros de esa entidad.

10. Cortafuego (firewall)

El responsable del tratamiento deberá disponer de un dispositivo que proteja la seguridad perimetral del sistema de información.

11. Sistema de análisis y gestión de vulnerabilidades y amenazas

El responsable del tratamiento deberá implementar herramientas que detecten la presencia de defectos en el software reportados por los fabricantes.

12. Sistema de protección contra código malicioso y descargable

El responsable del tratamiento deberá implementar herramientas que analicen el código y el comportamiento de software detectando actividades potencialmente peligrosas.

13. Sistema de detección de intrusiones

El responsable del tratamiento deberá implementar herramientas que busquen, en tiempo real, comportamientos típicos de maniobras de intrusión.

14. Servidor propio

Servidor propiedad de la entidad responsable del tratamiento.

15. Servidor dedicado ubicado en el Espacio Económico Europeo o en un país con nivel de protección de datos adecuado

Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes:

- Los Estados del Espacio Económico Europeo (EEE):
  - Estados de la Unión Europea.
  - Islandia.
  - Liechtenstein.
- Noruega.
- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
- Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.

- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
- Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
- Japón. Decisión de 23 de enero de 2019
- Reino Unido. Decisión de 28 de junio de 2021
- República de Corea. Decisión de 17 de diciembre de 2021
- EU- USA Data Privacy Framework Decisión de 10 de julio de 2023. Relación de las entidades certificadas: https://www.dataprivacyframework.gov/s/.

16. Servidor virtual privado (VPS) ubicado en el Espacio Económico Europeo o en un país con nivel de protección de datos adecuado

    Vid. supra.

17. Servidor cloud ubicado en el Espacio Económico Europeo o en un país con nivel de protección de datos adecuado

    Vid. supra.

18. Servidor de correo propio

    Servidor de correo propiedad de la entidad responsable del tratamiento.

19. Servidor web propio

    Servidor web propiedad de la entidad responsable del tratamiento.

20. Certificado SSL en página web (protocolo HTTPS)

    El protocolo seguro de transferencia de hipertexto (HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

21. Control de acceso físico a la sala del Centro de Proceso de Datos (CPD) / Sala del servidor

En relación con actividades de alto riesgo, exclusivamente el personal autorizado por el responsable del tratamiento podrá tener acceso físico a la sala donde se hallen los equipos que tengan alojados los datos de carácter personal.

22. Política de gestión de activos de información.

22.1. Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen y ser inventariados. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello.

22.2. La salida de soportes que contengan datos de carácter personal fuera de los locales donde estén ubicados los ficheros deberá encontrarse debidamente autorizada en el presente documento o ser expresamente autorizada por el responsable del tratamiento, utilizando para ello el documento disponible al efecto.

22.3. En relación con actividades de alto riesgo, la identificación de los soportes que contengan datos de carácter personal se podrá realizar, en su caso, utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes identificar su contenido, y que dificulten la identificación para el resto de personas.

22.4. En relación con actividades de alto riesgo, la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

23. Destrucción segura y confidencial de activos de información

Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal deberá procederse a su destrucción, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

24. Seguridad de los activos de información fuera de los locales del responsable del tratamiento

Cuando los datos personales se traten fuera de los locales del responsable del tratamiento, será preciso que exista una autorización previa, utilizando para ello el documento disponible al efecto, debiendo garantizarse, en todo caso, las medidas técnicas de seguridad

apropiadas en función del riesgo aplicable, y haciendo constar, como mínimo, los siguientes aspectos:

- Finalidad para la cual se solicita la autorización;
- Tipo de tratamiento (automatizado, no automatizado, mixto);
- Tipo de dispositivo portátil (en su caso) / Tipo de documentación objeto de tratamiento;
- Tipo de información que contiene el dispositivo portátil o la documentación;
- Fichero/s de donde proceden los datos;
- Periodo de validez de la autorización;
- Medidas de seguridad implementadas para proteger la información;
- Persona autorizada para trabajar fuera de los locales;
- Cargo / Departamento;
- Persona que autoriza;
- Cargo / Departamento;
- Observaciones;
- Firma de la persona que autoriza.

25. Proceso de autorización para nuevos tipos y/o medios de tratamiento de datos

Se prohíbe el uso de nuevos tipos y/o medios de tratamiento para el tratamiento de datos de carácter personal responsabilidad de la entidad, salvo que medie autorización expresa del responsable del tratamiento y previa adopción de las medidas de seguridad apropiadas en función del riesgo aplicable.

26. Adopción de medidas para asegurar la perdurabilidad material de los documentos

El responsable del tratamiento deberá implementar medidas preventivas contra los diversos factores de deterioro, destrucción o desaparición de los documentos que contengan datos de carácter personal (control de humedad, incendio, robo, etc.).

27. Aplicación de los criterios y métodos de organización documental

27.1. El archivo de los documentos que contengan datos de carácter personal se realizará de acuerdo con los criterios previstos en la legislación aplicable a la actividad de tratamiento. Estos criterios deberán garantizar la correcta conservación de los

documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de los interesados.

27.2. En aquellos casos en los que no exista normativa aplicable a la actividad de tratamiento, el responsable del tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo de los documentos, y que deberán garantizar, en cualquier caso, la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de los interesados.

28. Control de acceso a la documentación

28.1. Los armarios, archivadores y dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

28.2. En relación con actividades de alto riesgo, los armarios, archivadores u otros elementos en los que se almacenen los documentos que contengan datos de carácter personal, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

29. Registro de acceso a la documentación

En relación con actividades de alto riesgo, se deberán establecer mecanismos que permitan identificar los accesos realizados a los documentos que contengan datos de carácter personal que puedan ser utilizados por múltiples usuarios.

30. Política de mesas limpias

Mientras la documentación con datos de carácter personal no se encuentre archivada en los correspondientes dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

31. Traslado y envío seguro de la documentación

En el traslado de la documentación que contenga datos de carácter personal se adoptarán las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

32. Normas de uso de las impresoras de documentos

El usuario deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los citados datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

33. Destrucción segura y confidencial de la documentación:

Siempre que vaya a desecharse cualquier documento que contenga datos de carácter personal deberá procederse a su destrucción, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior a través de los siguientes medios:

- Máquinas destructoras de papel ubicadas en los propios locales del responsable del tratamiento. Preferiblemente, han de ser máquinas que destruyan la información en partículas frente a máquinas que destruyan la información en tiras, ya que si estamos ante hojas apaisadas -tipo Excel, por ejemplo- las tiras se podrían leer e incluso, con cierta dosis de paciencia, alguien podría llegar a reconstruir el documento.
- En su caso, a través de empresas de servicios de destrucción de documentos, en cuyo caso el responsable del fichero o del tratamiento deberá:
    - Exigir a la empresa prestadora del servicio un certificado de garantía de destrucción de la documentación que acredite la completa eliminación de la misma.
    - Solicitar a la empresa prestadora del servicio que un representante del responsable del fichero o del tratamiento presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados de la misma.

SECCIÓN IV: MEDIDAS EN RELACIÓN CON LA CAPACIDAD DE RESTAURAR LA DISPONIBILIDAD Y EL ACCESO A LOS DATOS PERSONALES DE FORMA RÁPIDA EN CASO DE INCIDENTE FÍSICO O TÉCNICO

1. Sistema de alimentación ininterrumpida (SAI) / Grupo electrógeno

   La entidad responsable del tratamiento deberá disponer de un equipo eléctrico encargado de alimentar y proteger cargas críticas, de modo que, en el caso de falta de suministro normal de la red eléctrica, se pueda seguir alimentando dichas cargas críticas durante un espacio de tiempo determinado.

2. Plan de Contingencia y Continuidad de Negocio:

   Plan de Continuidad de Negocio (PCN)
   Establece la continuidad de una entidad desde múltiples perspectivas: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc.

   Plan de Continuidad TIC (o Plan de Contingencia TIC, PCTIC)
   Es uno de los planes que forman el plan de continuidad de negocio de una entidad, pero restringido al ámbito TIC. Mientras que un PCN sirve de disparador para los diferentes planes de contingencia, un PCTIC se limita al ámbito tecnológico.

   Plan de Recuperación ante Desastres (PRD)
   En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si una entidad tiene un plan de desastres para su página web de comercio electrónico, el PRD contendrá todos los pasos para la recuperación de la aplicación.

3. Sistema informático redundante

   Los sistemas redundantes son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.

4. Sistema de identificación, registro y gestión de incidencias

El usuario que tenga conocimiento de cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos deberá notificar la misma por escrito al responsable de la protección de datos o a su superior inmediato, utilizando para ello el documento disponible al efecto, que dará traslado al responsable del tratamiento a fin de que se apliquen las medidas correctoras adecuadas.

En este sentido, se establecerá un registro elaborado a partir de las notificaciones de las incidencias por parte de los usuarios, en el que, como mínimo, se hará constar:

- Tipo de incidencia: informática / fichero no automatizado;
- Descripción detallada de la incidencia;
- Fecha y hora en que se ha producido, o en su caso, detectado la incidencia;
- Persona que realiza la notificación de la incidencia;
- Persona a la que se le comunica la incidencia;
- Efectos derivados o que se hubieran derivado de la incidencia;
- Medidas correctoras aplicadas;
- Firma de la persona que realiza la notificación;
- Firma de la persona a la que se le comunica la incidencia.

En relación con actividades de alto riesgo, en el libro registro de incidencias deberán consignarse, en su caso, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación, siendo necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

5. Sistema de gestión de copias de respaldo y recuperación de datos personales

5.1. La seguridad de los datos de carácter personal no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos. Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y, en su caso, reconstruir los datos de carácter personal, en base a los criterios reflejados en el presente apartado.

5.2. Deberá realizarse, con una periodicidad mínima semanal, una copia de respaldo de los datos de carácter personal, salvo que en dicho período no se hubiera producido ninguna actualización de los mismos.

5.3. En caso de fallo del sistema de información con pérdida total o parcial de los datos de carácter personal, existirá un procedimiento que, partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos de carácter personal al estado en que se encontraban en el momento del fallo.

5.4. Únicamente en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos.

5.5. En relación con actividades de alto riesgo, deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación. En este sentido, la Agencia Española de Protección de Datos ha señalado que es preferible que se trate de un espacio físico diferenciado en el que no se den los mismos riesgos físicos que en de ubicación del sistema de información (por ejemplo, incendio o inundación).

5.6. El responsable del tratamiento se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

6. Sistema de gestión y notificación de violaciones de seguridad de datos personales

Cuando el usuario tenga conocimiento de una violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se notifique a la autoridad de control competente y, en su caso, a los interesados.

SECCIÓN V: MEDIDAS EN RELACIÓN CON EL PROCESO DE VERIFICACIÓN, EVALUACIÓN Y VALORACIÓN REGULARES DE LA EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DEL TRATAMIENTO:

1. Auditoría externa

   El responsable del tratamiento deberá implementar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Dicho proceso podrá consistir en someter las actividades de tratamiento a una auditoría externa que, con una periodicidad mínima anual, verifique la eficacia de las citadas medidas de seguridad.

2. Auditoría interna

   El responsable del tratamiento deberá implementar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Dicho proceso podrá consistir en someter las actividades de tratamiento a una auditoría interna que, con una periodicidad mínima anual, verifique la eficacia de las citadas medidas de seguridad.

3. Controles internos de cumplimiento

   El responsable del tratamiento deberá implementar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Dicho proceso podrá consistir, al margen de las correspondientes auditorías anuales, en someter las actividades de tratamiento a controles internos de cumplimiento a intervalos planeados.

4. Revisión regular de la política de protección de datos a intervalos planeados

   El responsable del tratamiento deberá revisar la presente política de protección de datos con una periodicidad mínima anual.

ESTRUCTURA DEL SISTEMA DE INFORMACIÓN DE LA ENTIDAD

a) Descripción general de la red de comunicaciones electrónicas de la entidad:

- Número de sedes y ubicación:
  - Número total de sedes: 3
    - Ubicación sede n.º 1: PLAZA DEL ROLLO, 1 CP 45140 LOS NAVALMORALES (TOLEDO) – AYUNTAMIENTO – DEPENDENCIAS MUNICIPALES CENTRALES
    - Ubicación sede n.º 2: CALLE ANTONIO PALOMEQUE TORRES, 2, 45140 LOS NAVALMORALES (TOLEDO) – BIBLIOTECA MUNICIPAL / CASA DE LA CULTURA
    - Ubicación sede n.º 3: C/ LAS CRUCES, S/N - POLIDEPORTIVO / GIMNASIO MUNICIPAL

- Número de servidores y ubicación:
  - Número total de servidores: 1
    - Ubicación servidor n.º 1: PLAZA DEL ROLLO, 1 CP 45140 LOS NAVALMORALES (TOLEDO) – AYUNTAMIENTO – DEPENDENCIAS MUNICIPALES CENTRALES

b) Tipos de redes de comunicaciones electrónicas de la entidad:

- LAN (Local Area Network) Conjunto de máquinas interconectadas, ubicadas en extensiones relativamente pequeñas (vgr., edificio, oficina, etc.)

USUARIOS DEL SISTEMA

Nombre y apellidos	Cargo / Dpto.	Actividades de tratamiento a las que accede	Fecha de alta	Fecha de baja
RAQUEL GONZÁLEZ FERNÁNDEZ	AUXILIAR ADMINISTRATIVO	Expedientes Administrativos (AYUNTAMIENTOS)	12/07/2018	
MARÍA BELÉN HERNÁNDEZ BLÁZQUEZ	AGENTE DE EMPLEO Y DESARROLLO	Empleo (AYUNTAMIENTOS)	12/07/2018	
ANTONIO MANUEL DE LOS RÍOS RUÍZ	POLICÍA LOCAL EN SEGUNDA ACTIVIDAD	Policía Local (AYUNTAMIENTOS)	12/07/2018	01/02/2025
ANA CAPELO BALLESTEROS	SECRETARIA - INTERVENTORA	Todas las actividades de la entidad	12/07/2018	
JAVIER MÁRQUEZ LÓPEZ	OPERARIO DE SERVICIOS MÚLTIPLES (CEMENTERIO)	Cementerio Municipal (AYUNTAMIENTOS)	12/07/2018	
MONITOR DEPORTIVO	MONITOR DEPORTIVO	Gestión Deportiva (AYUNTAMIENTOS), Usuarios Servicios Municipales (AYUNTAMIENTOS)	12/07/2018	
ANTONIO TALAVERA MARTIN	ALCALDE	Todas las actividades de la entidad	04/08/2020	
ANDRES MARTIN DE PAZ	CONCEJAL DE AGUA Y DESARROLLO SOSTENIBLE	Obras / Licencias, Gestión de expedientes municipales, ordenación y organización de actos administrativos dictados por el Ayuntamiento, tanto de alcaldía como de órganos colegiados	01/07/2023	
EVA MARIA GARCIA CRIADO	CONCEJALA DE BIENESTAR SOCIAL, MAYORES, IGUALDAD Y FESTEJOS	Aprovechamiento de los Bienes de dominio público (AYUNTAMIENTOS), Servicios sociales	01/07/2023	
JESÚS ROMERO DEL HOMBRE BUENO	CONCEJAL DE CULTURA Y FESTEJOS,	Gestión Cultural (AYUNTAMIENTOS), Biblioteca	26/05/2026	

Nombre y apellidos	Cargo / Dpto.	Actividades de tratamiento a las que accede	Fecha de alta	Fecha de baja
	JUVENTUD, INFANCIA Y DEPORTES	(AYUNTAMIENTOS), Gestión Deportiva (AYUNTAMIENTOS)		
JOSE MARIA ARRIERO BARROSO	CONCEJAL		01/07/2023	
MARÍA BELEN GARCIA ARTEAGA	CONCEJALA DE EDUCACIÓN Y URBANISMO	Servicios sociales	01/07/2023	
ANA ISABEL HINIESTO GARCIA	CONCEJALA DE PARQUES Y JARDINES, TURISMO Y AGRICULTURA	Gestión Deportiva (AYUNTAMIENTOS)	01/07/2023	
BEGOÑA PAVÓN MONCLU	CONCEJALA		01/07/2023	
JOSE MARÍA LUNA GÓMEZ	CONCEJAL		01/07/2023	
PATRICIA CLEMENTE LÓPEZ HORCAJUELO	CONCEJALA		01/07/2023	
ARTURO CARLOS MARQUÉS ANDRÉS	BIBLIOTECARIO	Biblioteca (AYUNTAMIENTOS), Gestión Cultural (AYUNTAMIENTOS)	30/11/2021	
ELISABETH CAÑADA SÁNCHEZ-APARICIO	AUXILIAR ADMINISTRATIVA	Padrón municipal, Archivo municipal, Subvenciones, Gestión de expedientes, Expedientes Administrativos (AYUNTAMIENTOS)	30/11/2021	
MARÍA TERESA PÉREZ JIMÉNEZ	POLICÍA LOCAL	Policía Local (AYUNTAMIENTOS)	30/11/2021	
PILAR DEL PUERTO	Monitor Deportivo "Tu Salud en Marcha"	Servicios sociales	22/11/2022	
FRANCISCO JAVIER SERRANO GÓMEZ AREVALILLO	CONCEJAL		01/07/2023	

Nombre y apellidos	Cargo / Dpto.	Actividades de tratamiento a las que accede	Fecha de alta	Fecha de baja
CARLOS RECUERO PEREA	OPERARIO	Aprovechamiento de los Bienes de dominio público (AYUNTAMIENTOS)	26/05/2026	
MARTA PEREZ GONZÁLEZ	AUXILIAR ADMINISTRATIVA	Padrón municipal, Registro de entradas y salidas, Cementerio Municipal (AYUNTAMIENTOS), Aprovechamiento de los Bienes de dominio público (AYUNTAMIENTOS), Expedientes Administrativos (AYUNTAMIENTOS), Usuarios Servicios Municipales (AYUNTAMIENTOS)	01/10/2025	01/08/2026
OSCAR MUÑOZ HONTANAR	OPERARIO	Aprovechamiento de los Bienes de dominio público (AYUNTAMIENTOS)	26/05/2026	
JESÚS GARCÍA SÁNCHEZ	OPERARIO	Aprovechamiento de los Bienes de dominio público (AYUNTAMIENTOS)	26/05/2026	

INVENTARIO DE ACTIVOS DE INFORMACIÓN

ACTIVO DE INFORMACIÓN N.º 1	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-001
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 2	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-002
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias de Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 3	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-003
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 4	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-004
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 5	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-005
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 6	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref- 006
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 7	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-007
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 8	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-008
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 9	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref-009
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 10	
Tipo de activo	Portátil
Número de referencia (000/0000)	Ref-010
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Tiene acceso a todos los datos por red, a excepción de la contabilidad.
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 11	
Tipo de activo	Dispositivo de almacenamiento externo (disco duro, pen drive, etc.)
Número de referencia (000/0000)	Ref-011
Fecha de creación	08/08/2018
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	
Área / Local de ubicación	Dependencias del Ayuntamiento

ACTIVO DE INFORMACIÓN N.º 12	
Tipo de activo	Ordenador sobremesa
Número de referencia (000/0000)	Ref. 012
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Biblioteca Municipal
Área / Local de ubicación	Biblioteca: C/ Antonio Palomeque Torre, 2 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 13	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 013
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos de Alcaldía, Gestor de expedientes, firma electrónica
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 14	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 014
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales Secretaría, Gestor de expedientes, firma electrónica
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 15	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 015
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales de Operario de servicios múltiples
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 16	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 016
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 17	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 017
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 18	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 018
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 19	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 019
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 20	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 020
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 21	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 021
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 22	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 022
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 23	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 023
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 24	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 024
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 25	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 024
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales- Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 26	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 025
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 27	
Tipo de activo	Dispositivo móvil (tableta, smartphone, etc.)
Número de referencia (000/0000)	Ref. 026
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Contactos municipales - Concejales
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 28	
Tipo de activo	Software
Número de referencia (000/0000)	Ref. 027
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	Gestiona
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º 29	
Tipo de activo	Software
Número de referencia (000/0000)	Ref. 028
Fecha de creación	04/08/2020
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	GIA
Área / Local de ubicación	Ayuntamiento: Plaza del Rollo, 1 - 45140 Los Navalmorales (Toledo)

ACTIVO DE INFORMACIÓN N.º	
Tipo de activo	
Número de referencia (000/0000)	
Fecha de creación	
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	
Área / Local de ubicación	

ACTIVO DE INFORMACIÓN N.º	
Tipo de activo	
Número de referencia (000/0000)	
Fecha de creación	
Fecha de destrucción (en su caso)	
Tipo de datos que contiene	
Área / Local de ubicación	

DISPOSITIVOS DE ALMACENAMIENTO / ALMACENAMIENTO DE LA INFORMACIÓN

DISPOSITIVO DE ALMACENAMIENTO N.º 1	
Tipo de datos que contiene	Registro Civil
Dispositivo de almacenamiento	
Mecanismos de seguridad / Medidas alternativas	
Área / Local de ubicación	Archivo independiente
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º 2	
Tipo de datos que contiene	Juzgado de Paz
Dispositivo de almacenamiento	
Mecanismos de seguridad / Medidas alternativas	
Área / Local de ubicación	Archivo independiente
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º 3	
Tipo de datos que contiene	Datos estadísticos
Dispositivo de almacenamiento	Archivadores
Mecanismos de seguridad / Medidas alternativas	Cerraduras de llave, combinación, etc.
Área / Local de ubicación	Despacho Policía Local
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º 4	
Tipo de datos que contiene	Datos estadísticos
Dispositivo de almacenamiento	Archivadores
Mecanismos de seguridad / Medidas alternativas	Cerraduras de llave, combinación, etc.
Área / Local de ubicación	Garaje Policía Local
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º 5	
Tipo de datos que contiene	Archivo de Biblioteca
Dispositivo de almacenamiento	
Mecanismos de seguridad / Medidas alternativas	
Área / Local de ubicación	Biblioteca Municipal
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º	
Tipo de datos que contiene	
Dispositivo de almacenamiento	
Mecanismos de seguridad / Medidas alternativas	
Área / Local de ubicación	
Mecanismos de seguridad / Medidas alternativas	

DISPOSITIVO DE ALMACENAMIENTO N.º	
Tipo de datos que contiene	
Dispositivo de almacenamiento	
Mecanismos de seguridad / Medidas alternativas	
Área / Local de ubicación	
Mecanismos de seguridad / Medidas alternativas	

LIBRO REGISTRO DE INCIDENCIAS

Tendrán la consideración de **"incidencia"** todos aquellos incumplimientos de las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento, así como cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

FORMULARIO DE NOTIFICACIÓN DE INCIDENCIAS		
Tipo de incidencia: informática / fichero no automatizado		
Descripción detallada de la incidencia		
Fecha y hora en que se ha producido, o en su caso, detectado la incidencia	Fecha	Hora
Persona que realiza la notificación de la incidencia	Persona	Cargo
Persona a la que se le comunica la incidencia	Persona	Cargo
Efectos derivados o que se hubieran derivado de la incidencia		
Medidas correctoras aplicadas		
Firma de la persona que realiza la notificación		
Firma de la persona a la que se le comunica la incidencia		

PROCEDIMIENTO DE RECUPERACIÓN DE DATOS		
Fecha y hora en que se realiza el procedimiento de recuperación de datos	Fecha	Hora
Procedimiento realizado		
Datos restaurados		
En su caso, datos que ha sido necesario grabar manualmente en el proceso de recuperación		
Persona que ejecuta el proceso de recuperación de los datos	Persona	Cargo
Persona que autoriza el proceso de recuperación	Persona	Cargo

AUTORIZACIÓN PARA TRABAJAR FUERA DE LOS LOCALES DEL RESPONSABLE DEL TRATAMIENTO

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, será preciso que exista una autorización previa del mismo, debiendo garantizarse, en todo caso, el nivel de seguridad correspondiente al tipo de fichero tratado.

AUTORIZACIÓN PARA TRABAJAR FUERA DE LOS LOCALES DEL RESPONSABLE DEL TRATAMIENTO	
Finalidad para la cual se solicita la autorización	
Tipo de tratamiento (automatizado, no automatizado, mixto)	
Tipo de dispositivo portátil (en su caso) / Tipo de documentación objeto de tratamiento	
Tipo de información que contiene el dispositivo portátil o la documentación	
Actividad de tratamiento de donde proceden los datos	
Periodo de validez de la autorización	
Medidas de seguridad implementadas para proteger la información	
Persona autorizada para trabajar fuera de los locales	
Cargo / Departamento	
Persona que autoriza	
Cargo / Departamento	
Observaciones	
Fecha	
Firma de la persona que autoriza	

SALIDAS AUTORIZADAS DE SOPORTES Y DOCUMENTOS

Tipo de soporte o documento	Tipo de información que contiene	Finalidad / Destino	Usuario autorizado	Periodicidad
Teléfono Móvil	Contactos municipales, Gestor de Expedientes, Firma electrónica - Secretaría	Realización de trabajos	ANA CAPELO BALLESTEROS	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	JAVIER MÁRQUEZ LÓPEZ	Diaria
Teléfono Móvil	Contactos municipales, Gestor de Expedientes, Firma electrónica - Alcaldía	Realización de trabajos	ANTONIO TALAVERA MARTIN	Diaria
Teléfono Móvil	Contactos municipales - Alcaldía	Realización de trabajos	ANDRES MARTIN DE PAZ	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	EVA MARIA GARCIA CRIADO	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	JESÚS ROMERO DEL HOMBRE BUENO	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	JOSE MARIA ARRIERO BARROSO	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	MARÍA BELEN GARCIA ARTEAGA	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	ANA ISABEL HINIESTO GARCIA	Diaria

Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	BEGOÑA PAVÓN MONCLU	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	JOSE MARÍA LUNA GÓMEZ	Diaria
Teléfono Móvil	Contactos municipales - Concejales	Realización de trabajos	PATRICIA CLEMENTE LÓPEZ HORCAJUELO	Diaria

Cumplimiento con lo establecido en el artículo 32 del Reglamento (UE) 2016/679

LIBRO REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

La salida de soportes que contengan datos de carácter personal fuera de los locales donde estén ubicados los ficheros deberá estar expresamente autorizada por el responsable del tratamiento, utilizando para ello el documento de salida de soportes. Adicionalmente, en el supuesto de entrada y salida de soportes que contengan datos de carácter personal en relación con actividades de alto riesgo, deberá cumplimentarse el documento de entrada o salida de soportes, según proceda.

ENTRADA DE SOPORTES		
SOPORTE		
Tipo de soporte (descripción)		
Tipo de información que contiene		
Fecha y hora de entrada del soporte	Fecha	Hora
FINALIDAD Y ORIGEN		
Finalidad		
Origen		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Precauciones para el transporte		
AUTORIZACIÓN		
Persona responsable de la recepción		
Cargo / Departamento		
Observaciones		
Firma de la persona que recibe el soporte		

SALIDA DE SOPORTES		
SOPORTE		
Tipo de soporte (descripción)		
Tipo de información que contiene		
Actividad de tratamiento de donde proceden los datos		
Fecha y hora de salida del soporte	Fecha	Hora
FINALIDAD Y DESTINO		
Finalidad		
Destino		
Destinatario		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Precauciones para el transporte		
AUTORIZACIÓN		
Persona responsable de la entrega		
Persona que autoriza		
Cargo / Departamento		
Observaciones		
Firma de la persona que autoriza		

LIBRO REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS

La salida de documentos que contengan datos de carácter personal fuera de los locales donde estén ubicados los ficheros deberá estar expresamente autorizada por el responsable del tratamiento, utilizando para ello el documento de salida de documentos. Adicionalmente, en el supuesto de entrada y salida de soportes que contengan datos de carácter personal en relación con actividades de alto riesgo, deberá cumplimentarse el documento de entrada o salida de soportes, según proceda.

ENTRADA DE DOCUMENTOS		
DOCUMENTO		
Tipo de documento (descripción)		
Tipo de información que contiene		
Fecha y hora de entrada del documento	Fecha	Hora
FINALIDAD Y ORIGEN		
Finalidad		
Origen		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Precauciones para el transporte		
AUTORIZACIÓN		
Persona responsable de la recepción		
Cargo / Departamento		
Observaciones		
Firma de la persona que recibe el documento		

SALIDA DE DOCUMENTOS		
DOCUMENTO		
Tipo de documento (descripción)		
Tipo de información que contiene		
Actividad de tratamiento de donde proceden los datos		
Fecha y hora de salida del documento	Fecha	Hora
FINALIDAD Y DESTINO		
Finalidad		
Destino		
Destinatario		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Precauciones para el transporte		
AUTORIZACIÓN		
Persona responsable de la entrega		
Persona que autoriza		
Cargo / Departamento		
Observaciones		
Firma de la persona que autoriza		

AUDITORÍAS

AUDITORÍA N.º 1	
Fecha de emisión del informe de auditoría	
Auditoría interna / externa	
Entidad auditora	
Objetivo del informe de auditoría	
Actividades de tratamiento auditadas	
Resultado y principales conclusiones del informe de auditoría	
Principales medidas correctoras o complementarias propuestas	

CONTROLES INTERNOS DE CUMPLIMIENTO

CONTROL INTERNO DE CUMPLIMIENTO N.º 1	
Fecha de realización del control interno de cumplimiento	
Objetivo del control interno de cumplimiento	
Actividades de tratamiento objeto del control interno de cumplimiento	
Resultado y principales conclusiones del control interno de cumplimiento	
Principales medidas correctoras o complementarias propuestas	