EstudNET

Adaptación al Reglamento General de Protección de Datos y Esquema Nacional de Seguridad. N.º Expediente: 86/2019/TEC

Cumplimiento normativo en materia de protección de datos personales

Informe de auditoría interna

Fecha: 25/08/2023

Versión: 1.0

Clasificación: INTERNO

Índice

1. ANTECEDENTES

Dentro del expediente de contratación número 86/2019/TEC la Junta de Gobierno Local, en sesión ordinaria celebrada con fecha 29 de julio de 2021, adoptó el acuerdo de adjudicar el "SERVICIO DE ADAPTACIÓN AL ENS, AL REGLAMENTO EUROPEO Y A LA LEY 3/2018" a la entidad EstudNET SL y a cuyo cargo se establece la función del desempeño de papel de Delegado de Protección de Datos (en lo sucesivo, DPD) del Ayuntamiento de Santa Cruz de Tenerife.

En fecha 13 de septiembre de 2021 el concejal de Tecnología acepta la designación realizada por la empresa EstudNET, SL con CIF B92236603, adjudicataria del contrato de "Servicio de consultoría de adaptación al ENS, al Reglamento Europeo de Protección de Datos y a la Ley Orgánica 3/2018" y se da cuenta del nombramiento a la Agencia Española de Protección de Datos del designado.

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 (en lo sucesivo, RGPD), establece entre las funciones del Delegado de Protección de Datos la de informar y asesorar al responsable o encargado de tratamiento y los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión, en nuestro caso la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDPGDD) y que recoge idéntica función.

EstudNET SL, dentro de la ejecución del contrato, ha planificado y realizado una auditoría interna de cumplimiento en materia de protección de datos del Ayuntamiento de Santa Cruz de Tenerife, cuyo informe se documenta a continuación.

2. OBJETO

El presente informe da respuesta al principio de responsabilidad proactiva (artículo 5.2) del Reglamento (UE) 2016/679 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, que establece que el responsable de los tratamientos, en este caso el Ayuntamiento de Santa Cruz de Tenerife, más allá de cumplir con los principios normativos, deberá disponer de las evidencias de cumplimiento de las medidas implantadas con la finalidad de poder demostrar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos.

En consecuencia, con lo anterior, el objetivo principal de la auditoria es **verificar el grado de cumplimiento por el Ayuntamiento de Santa Cruz de Tenerife de la normativa en protección de datos personales, identificando sus insuficiencias y proponiendo las medidas correctoras necesarias para su subsanación.**

Para verificar lo anterior, los **objetivos secundarios** de la auditoría realizada son los siguientes:

1. Recopilar y verificar las evidencias de cumplimiento del Ayuntamiento de Santa Cruz de Tenerife, en materia de protección de datos personales.

2. Identificar y evaluar las No Conformidades del Ayuntamiento de Santa Cruz de Tenerife que constituyan un incumplimiento, formal o material, de las obligaciones normativas materia de protección de datos personales.

3. Proponer las acciones correctivas y preventivas a implantar por el Ayuntamiento de Santa Cruz de Tenerife para la subsanación de las No Conformidades detectadas materia de protección de datos personales.

La realización de la auditoría ha sido realizada por la entidad EstudNET SL en calidad de Delegado de Protección de Datos, en el desarrollo de sus funciones de informar y asesorar, bien de oficio o cuando le sea solicitado al Ayuntamiento de Santa Cruz de Tenerife y a las personas autorizadas para tratar los datos personales bajo su autoridad directa.

Cabe poner de manifiesto la competencia del Delegado de Protección de Datos, así como que en el desempeño de sus competencias actúa de manera independiente y, en concreto, por previsión normativa el artículo 38 del RGPD establece que «*no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones*».

Se ha encomendado la materialización como Auditor-Responsable a Don Ángel Yuste Barranquero, Abogado, Delegado de Protección de Datos según certificado ES1912270 por AEC bajo los criterios que la Agencia Española de Protección de Datos.

3. ALCANCE

El **ámbito subjetivo** de la auditoría es el siguiente:

- Incluye
  - los órganos municipales del Ayuntamiento de Santa Cruz de Tenerife, entendiendo por órganos a sus áreas y distritos municipales, así como a sus unidades administrativas
  - el Instituto Municipal de Atención Social (IMAS)

- Excluye
  - Gerencia Municipal de Urbanismo
  - Sociedad de Desarrollo de Santa Cruz de Tenerife
  - Viviendas, Proyectos y Obras Municipales de Santa Cruz de Tenerife, S.A.

El **ámbito objetivo** de la auditoría son las operaciones de tratamiento de datos de personales llevadas a cabo Ayuntamiento de Santa Cruz de Tenerife (en adelante, la entidad), en calidad de responsable y encargada de tratamiento de datos personales.

Por otra parte, el alcance de la auditoría cubre la revisión normativa de los sistemas de información, procesos y personal de la entidad que traten, recojan, consulten, utilicen, almacenen o necesiten acceder a datos de carácter personal ya sea de manera automatizada o no.

Los ámbitos de las obligaciones a evaluar por la auditoria cubren las obligaciones normativas de la entidad en materia de protección de datos personales, a saber:

- **Ámbito Organizativo**: se revisa la organización y la normativa y procedimientos de la entidad

- **Ámbito Técnico**: se revisa el cumplimiento de las medidas de seguridad de los tratamientos de datos llevados a cabo por la entidad.

  El presente informe se complementa en los ámbitos anteriores con el emitido, asimismo, por EstudNET SL de auditoría interna de conformidad con el esquema Nacional de Seguridad de Seguridad.

- **Ámbito Jurídico**: se revisan las categorías de los datos tratados por los sistemas de información de la entidad, y si se realiza un análisis de riesgos y/o, en su caso, Evaluaciones de impacto de algunos de los tratamientos que realiza.

4. NORMATIVA Y DOCUMENTACIÓN DE REFERENCIA

La normativa de aplicación en el ámbito de la auditoría es la siguiente:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. (LCSP)

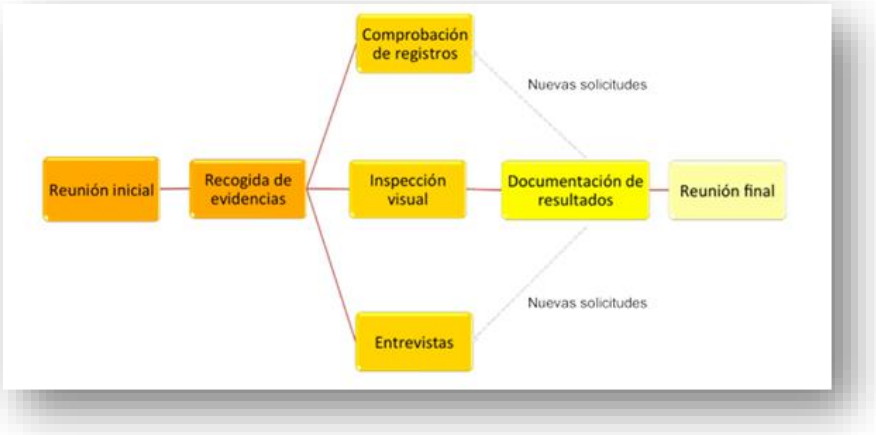
La documentación de referencia en el ámbito de la auditoría es la siguiente:

- UNE-EN ISO/IEC 27701:2021. Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información.
- Guía de Buenas Prácticas en Auditorías RGPD de ISMS Forum
- Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. AEPD
- Guía práctica para Evaluaciones de Impacto en Protección de los Datos sujetas al RGPD. AEPD
- Guía práctica (enero de 2018, versión 2.0). Evaluación de impacto relativa a la protección de datos. EIPD-APDCAT
- Guía de orientaciones y procedimientos-anonimización de datos personales. AEPD
- Guía para la gestión y notificación de brechas de seguridad. AEPD
- Guía de Privacidad desde el Diseño - Agencia Española de Protección de Datos (2020)
- Guía sobre el uso de las cookies. AEPD. Julio 2020
- Guía La privacidad desde el diseño y la privacidad por defecto. Guía para desarrolladores. Febrero 2023. APDCAT.

5. METODOLOGIA

La metodología seguida para la evaluación del cumplimiento normativo de la entidad se fundamenta, en primer término, en la aportación de evidencias objetivas documentales que demuestren el cumplimiento de una obligación en materia de protección de datos personales.

En consecuencia, se han recopilado y evaluado las evidencias documentales en las que se fundamentan los hallazgos de la auditoría, desde el 07/09/2021 hasta la fecha del presente informe, de acuerdo con las fases metodológicas siguientes:



A su vez, una **desviación o insuficiencia normativa** detectada distinguirá las calificaciones siguientes:

- **No Conformidad Mayor:** un incumplimiento formal de una obligación legal por la entidad.
- **No Conformidad Menor:** un incumplimiento material de una obligación legal por la entidad.

de acuerdo con los criterios de impacto siguientes:

- **Perjuicio a las personas:** Puede ocasionar un daño a los derechos y libertades fundamentales de las personas con las que se relaciona la entidad en materia de protección de datos.
- **Incumplimiento normativo:** Existe un incumplimiento de una disposición legal, administrativa o regulación de la entidad.
- **Daño reputacional**: Puede ocasionar un perjuicio reputacional a la imagen pública e institucional de la entidad.

NO CONFORMIDAD	PERJUICIO A LAS PERSONAS	INCUMPLIMIENTO NORMATIVO	DAÑO REPUTACIONAL
Mayor	Daño grave de difícil o imposible reparación (*)	Incumplimiento material grave de una norma jurídica.	Perjuicio reputacional grave a la imagen pública e institucional
Menor	Daño relevante de posible subsanación.	Incumplimiento formal de una norma jurídica de posible subsanación.	Perjuicio reputacional relevante a la imagen pública e institucional.

(*) Entre los supuestos de grave daño al afectado se encuentran aquellos que afecten al ejercicio de sus derechos fundamentales y libertades públicas establecidos por la Constitución Española, como la revelación no autorizada de datos personales de categoría especial.

En aquellos tratamientos en los que se evidencia una adecuación al ordenamiento jurídico se hará constar su **CONFORMIDAD.** En otros supuestos, se realizarán **RECOMENDACIONES** entendidas como, aquellas tratamientos adecuados al ordenamiento jurídico (**CONFORMES**) que presentan oportunidades de mejora .

6. PLANIFICACIÓN Y ORGANIZACIÓN

Se mantiene reunión presencial (25/05/2023) con los responsables del Área de Organización y Gobierno Abierto de la entidad para la validación de la organización y planificación de la auditoría. Se incluye como anexo I el documento 20230524_ESTUDNET_Auditoría_RGPD_Planificación_v1.1

A continuación, se identifican los responsables que han participado en la auditoría.

- Por parte de la entidad

    - D. José Antonio Herrera Umpierrez, Responsable de la Información y del Servicio
    - D. Manuel Pérez Coca, Responsable de Seguridad de la Información
    - Dña. María del Cristo Morales, Jefe de Servicio Organización y Gobierno Abierto.

- Por parte de EstudNET SL
    - D. Ángel Yuste, designado como Delegado de protección de datos
    - D. Jorge Márquez Pacios, responsable del Contrato

La planificación presentada ha tenido en cuenta la celebración de entrevistas con responsables municipales que ha sufrido una incidencia al no haberse podido ser llevadas a cabo ante la ausencia de respuesta y participación de los responsables convocados por la Jefe de Servicio Organización y Gobierno Abierto, a excepción de las siguientes:

- Policía Local
- Sede administrativa de La Granja
- Servicios Jurídicos

Como medida de contingencia se ha tenido que modificar este enfoque metodológico participativo de la auditoría interna que, en sí mismo aporta un hallazgo, más adelante registrado, estableciéndose como base de evidencias las consultas y los informes emitidos por EstudNET SL, desde el 07/09/2021 en calidad de Delegado de Protección de Datos de la entidad, al no poder obtenerse las aportaciones de los responsables municipales.

7. CUADRO DE NO CONFORMIDADES

A continuación, se resumen las principales no conformidades resultado de la auditoría realzada.

#	DESCRIPCIÓN	CALIFICACIÓN
01	El correo electrónico de contacto del Delegado de Protección de Datos (dpd@santacruzdetenerife.es) no es accesible por este, lo que puede suponer una limitación, en plazo y/o forma, de las reclamaciones o consultas en relación con el desarrollo de las competencias que le son propias.	MAYOR
02	Publicación del catálogo de puestos de trabajo del Ayuntamiento con información identificativa.	MAYOR
03	Insuficiente adecuación normativa de los tratamientos de datos personales de la Policía Local. 1. Existencia de archivo no automatizado sin garantías. 2. Insuficiencia de información en materia de protección de datos.	MAYOR
04	Falta de designación de un DPD por el Instituto Municipal de Atención (IMAS).	MAYOR
05	Falta de análisis de riesgos de T-Systems como encargada de servicios de administración electrónica	MAYOR
06	Actualización del Registro de Actividades de Tratamiento del Sistema Interno de Información de la Ley 2/2023.	MENOR
07	Ausencia de una revisión previa en las contrataciones en los que existan encargados de tratamiento.	MENOR
08	Insuficiencia de concienciación y formación en materia de protección de datos	MAYOR

Reseñar, así mismo, que a la fecha del presente informe, se encuentran abiertas dos (2) incidencias en relación con la Agencia Española de Protección de Datos, a saber:

#	IDENTIFICACIÓN	ESTADO
01	Información relativa a brecha de seguridad de suplantación de identidad comunicada por el Ayuntamiento de Santa Cruz de Tenerife el 27/07/2023 dentro del expediente REGAGE23e00051172382.	**EN PLAZO**
02	Traslado de reclamación de una interesada y solicitud de información al IMAS (Expediente N.º: EXP202307047) notificada el 30/05/2023.	**FUERA DE PLAZO**
03	Brecha de seguridad identificada en la herramienta de fichajes del Ayuntamiento de Santa Cruz de Tenerife, Arquero	**CERRADA**
04	Brecha de seguridad debido a la resolución de una incidencia que provoca, de forma involuntaria, la modificación de datos personales por T-SYSTEMS (14/02/2022)	**CERRADA**
05	Solicitud de información remitida el 17 de julio de 2022 por la Agencia Española de Protección de Datos (Expediente EXP202207658) relativa a la reclamación presentada por una ciudadana que había accedió a su área personal de la Sede Electrónica	**CERRADA**
06	Resolución de Procedimiento Sancionador nº: PS/00098/2021 de la Agencia Española de Protección de Datos dirigida al Ayuntamiento de Santa Cruz de Tenerife, con sanción de apercibimiento, por una infracción de los artículos 32 y 33 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, tipificadas en el artículo 83.4, en fecha 1 de julio de 2021.	**CERRADA**

7.1 No conformidad 1: Falta de comunicación directa con el Delegado de Protección de Datos

NO CONFORMIDAD

El correo electrónico de contacto del Delegado de Protección de Datos (dpd@santacruzdetenerife.es) no es accesible por este, lo que puede suponer una limitación, en plazo y/o forma, de las reclamaciones o consultas en relación con el desarrollo de las competencias que le son propias.

CONSIDERACIONES

En septiembre de 2021 el Concejal de Tecnología acepta la designación realizada por la empresa EstudNET, SL con CIF B92236603, adjudicataria del contrato de "Servicio de consultoría de adaptación al ENS, al Reglamento Europeo de Protección de Datos y a la Ley Orgánica 3/2018" y se da cuenta del nombramiento a la Agencia Española de Protección de Datos (AEPD) del designado. Dentro de esta comunicación se señala ante la AEPD el correo electrónico de contacto dpd@santacruzdetenerife.es

Esta designación es consecuente que la función del DPD puede ejercerse también en el marco de un contrato de servicios suscrito con una persona física o con una organización ajena a la organización del responsable o del encargado del tratamiento.

Es igualmente importante que cada uno de estos miembros esté protegido por las disposiciones del RGPD.

El artículo 37, apartado 7, del RGPD requiere, en este caso que el Ayuntamiento publiquen los datos de contacto del DPD y comuniquen los datos de contacto del DPD a la Agencia Española de Protección de Datos.

Como establece el Grupo de Trabajo en el Artículo 29 dentro de las Directrices sobre los delegados de protección de datos (DPD) adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017, sobre este particular viene a establecer:

El objetivo de dichos requisitos es garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades de control puedan contactar de forma fácil y directa con el DPD, sin tener que contactar con ninguna otra parte de la organización*. La confidencialidad es*

igualmente importante: por ejemplo, los empleados pueden ser reacios a presentar quejas al DPD si la confidencialidad de sus comunicaciones no está garantizada.

El DPD estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros (artículo 38, apartado 5). Los datos de contacto del DPD deben incluir información que permita a los interesados y a las autoridades de control comunicarse con este de forma sencilla (dirección postal, un número de teléfono específico y/o una dirección de correo electrónico específica).

No obstante, la comunicación del nombre del DPD a la autoridad de control es fundamental, con el fin de que el DPD actúe como punto de contacto entre la organización y la autoridad de control [artículo 39, apartado 1, letra e)]. Como una buena práctica, el Grupo de Trabajo del artículo 29 recomienda también que las organizaciones informen a sus empleados del nombre y datos de contacto del DPD. Por ejemplo, el nombre y los datos de contacto del DPD podrían publicarse internamente en la intranet de la organización, en el directorio telefónico interno y en el organigrama.

ACCION CORRECTIVA

Acceso directo al correo electrónico de contacto del Delegado de Protección de Datos (dpd@santacruzdetenerife.es), a fin de recibir, en plazo y/o forma, las reclamaciones o consultas en relación con el desarrollo de las competencias que le son propias.

7.2 No conformidad 02: Publicación del catálogo de puestos de trabajo con información identificativa

NO CONFORMIDAD

Publicación del **Catálogo de Puestos de Trabajo del Ayuntamiento de Santa Cruz de Tenerife,** donde aparecen descritos los puestos ocupados y vacantes, **con identificación del personal, (nombres y apellidos**).

https://sede.santacruzdetenerife.es/sede/fileadmin/user_upload/web/Transparencia/empleo/Catalogo_3_febrero_2023.pdf

CONSIDERACIONES

Se entiende, conforme con la normativa de protección de datos, que la incursión de estos datos no

es proporcional al fin del tratamiento (la transparencia).

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno establece, establece en el artículo 15 la protección de datos personales establece un deber de ponderación ***suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.***

Para la realización de la citada ponderación*, dicho órgano tomará particularmente en consideración los siguientes criterios:*

a) ***El menor perjuicio a los afectados derivados*** *del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.*

d) ***La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad****, o se refieran a menores de edad.*

4. ***No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas****.*

En relación con el RGPD, se considera relevantes los principios relativos al tratamiento que se plasman en el artículo 5, en cuanto que los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines

de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

En la aplicación de la Ley básica (Ley 19/2013), la Administración General del Estado no identifica y

como publicidad activa los catálogos de puesto de trabajo con una relación nominal de las personas que los ocupan. En informes emitidos se hacía constar que incluso en relación a determinado grupo de funcionarios, la publicación afecta a la seguridad y en este sentido la identificación de todos los miembros de las Fuerzas y Cuerpos de Seguridad, el Ejército, el Centro Nacional de Inteligencia, etc. O personal que presta sus servicios en infraestructuras críticas.

A su vez en esta Comunidad Autónoma, y salvo error u omisión no se han encontrado listados de catálogos de puestos de trabajo que relacionen a todos los empleados públicos de forma nominal, ni tampoco de su Cuerpo General de la Policía.

Es un hecho a su vez que el Ayuntamiento de Santa Cruz de Tenerife, como se apuntó en informes anteriores, tiene un cuerpo de Policía Local el cual se relaciona en el catálogo de puestos de trabajo con su nombre y apellidos, siendo significativo que todos los miembros de las Policías Locales estarán provistos de un documento de acreditación profesional expedido por el respectivo Ayuntamiento, según modelo homologado por la Consejería competente en la materia, en el que al menos, constará el nombre del municipio, el del funcionario, empleo, número de identificación como agente de la autoridad y número del documento nacional de identidad. Este documento es relevante ya que lo identifica (dándoles la reserva y seguridad) en sus actuaciones profesionales.

Es significativo que los miembros de las Fuerzas y Cuerpos de Seguridad (con la inclusión de la Policía Local) en su trabajo diario aporta el número asignado en la acreditación profesional, incluso ante las autoridades judiciales en sus declaraciones según dispone el artículo 762.5 de la Ley de Enjuiciamiento Criminal y al **tratarse de agentes de la autoridad bastará la reseña del número de carné profesional.**

El Ayuntamiento de Santa Cruz de Tenerife es designado como operador crítico según la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y esto implica identificar servicios esenciales, donde la prestación del servicio es realizada por empleados públicos.

El Tribunal Europeo de Derechos Humanos (TEDH) ha declarado que la libertad de recibir información, no puede interpretarse como que impone a un Estado una obligación positiva de difundir información o revelar información al público (véanse los casos de Leander c. Suecia (1987), Gaskin c. Reino Unido (1989), Guerra c. Italia (1998) y Sîrbu c. Moldavia (2004))

La base legal para el procesamiento de datos personales en el contexto de las medidas de conflicto

de intereses se encuentra

El artículo 6 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, establece que** los datos personales pueden ser tratados si el tratamiento es necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento.

En estas circunstancias, los legisladores tienen el deber de garantizar que las obligaciones legales equilibren los diversos intereses involucrados. De hecho, la legislación debe ser compatible con el derecho a la vida privada y familiar ya la protección de los datos personales de conformidad con el artículo 8 del CEDH y los artículos 7 y 8 de la Carta de la UE. Esto implica que la obligación legal de tratar los datos personales debe ser necesario y proporcionado a los fines legítimos perseguidos, y conforme al principio de limitación de finalidad.

Debemos de tener presente a su vez que la normativa de protección de datos (el RGPD y LOPDGDD), son normas más recientes que las relativas a la transparencia, y estando enfrentado dos derechos (transparencia y derecho fundamental a la protección de datos), debe de primar este y máxime en este supuesto que la relación nominal no aporta ningún añadido a la ciudadanía.

ACCION CORRECTIVA

Anonimización de la publicación del Catálogo de Puestos de Trabajo del Ayuntamiento de Santa Cruz de Tenerife, donde aparecen los puestos ocupados y vacantes (sin identificación del personal).

7.3 No conformidad 03: Insuficiente adecuación normativa de los tratamientos de datos personales de la Policía Local.

NO CONFORMIDAD

Insuficiente adecuación normativa de los tratamientos de datos personales llevados a cabo por la Policía Local

1. Existencia de archivo no automatizado sin garantías.
2. Insuficiencia de información en materia de protección de datos.

CONSIDERACIONES

Dentro de los servicios de la Policía Local se tienen en cuenta informes anteriores del DPD y estado actual de las insuficiencias detectadas:

1. Existencia de un archivo no automatizado sin garantías

No conformidad detectada en informe del DPD (25/04/2022), donde se comprobó la existencia de un archivo de tratamiento manual, conformado por carpetas y nombres de los afectados.

En algunos casos y por la antigüedad del papel podría ser incorporado o relevante para fines históricos.

Teniendo en cuenta la normativa que obliga a la limitación de la supresión, tal y como se establece en el artículo 8 (Plazos de conservación y revisión) de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, a saber:

1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.

2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.

3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.

Y a su vez el RGPD, en relación de aquellos expedientes que estén fuera de la prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, donde

es de aplicación el artículo 5 establece como uno de los principios del tratamiento, mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

En consecuencia, con lo anterior, se incumple este precepto, debiendo procederse a una revisión y expurgo documental en los términos que los artículos plasman.

2. Insuficiencia en el proceso de información en materia de protección de datos.

Como se hacía constar en anteriores informes del DPD, el RGPD establece el deber de informar a las personas interesadas en el momento en el que soliciten datos personales, y ese deber de información no puede ser obviado independientemente que el procedimiento sea sancionador (en ese caso de aplicación 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 así como Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), o incluido dentro de la actividad de prevención o investigación de infracciones penales al ser el Cuerpo de la Policía Local es una de las autoridades competentes y donde es de aplicación de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en cuanto participa en la prevención, detección e investigación de infracciones penales.

Se deberán distinguir, por tanto, dos tipos de información de protección de datos a ofrecer a los afectados En la toma de datos, como consecuencia de actas de inspección, denuncias, solicitudes en general y toda aquella actuación administrativa.

En este sentido se ha comprobado en la última reunión con motivo de la auditoría que no está finalizado el proceso de información básica en materia de protección de datos en actas y denuncias administrativas.

A su vez dentro de la aplicación Ley Orgánica 7/2021, de 26 de mayo, de protección de datos

personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, la información, tal y como se proponía en el informe de enero 2023, no se ha completado el proceso de adecuación.

ACCCIONES CORRECTIVAS

1. Revisión y expurgo documental de un archivo de tratamiento manual, conformado por carpetas y nombres de los afectados. En algunos casos y por la antigüedad del papel podría ser incorporado o relevante para fines históricos.
2. Distinguir los dos tipos de información de protección de datos a ofrecer a los afectados. En la toma de datos, como consecuencia de actas de inspección, denuncias, solicitudes en general y toda aquella actuación administrativa.
3. Finalizar el proceso de información básica en materia de protección de datos en actas y denuncias administrativas.
4. Incluir en la web municipal una información ampliada.

7.4 No conformidad 04: Falta de designación de un DPD por el Instituto Municipal de Atención (IMAS)

NO CONFORMIDAD

Falta de designación de Delegado de Protección de Datos.

CONSIDERACIONES

Dentro del actual contrato de "Adaptación al Reglamento General de Protección de Datos y Esquema Nacional de Seguridad". (N.º Expediente: 86/2019/TEC), concretó el servicio de consultoría de apoyo al Ayuntamiento de Santa Cruz de Tenerife, para lograr la adecuación y cumplimiento del Reglamento 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, del Esquema Nacional de Seguridad (ENS) regulado en el Real Decreto 3/2010, de 8 de enero, modificado en 2015 a través del Real Decreto 951/2015, de 23 de octubre, y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos digitales, **dejando fuera del ámbito contractual a los "Organismos Autónomos, Sociedades Mercantiles Municipales y Fundaciones Públicas".**

En relación con el IMAS, no obstante, se le ha apoyado de forma puntual, no ha podido ser revisada su política de privacidad, al no poder realizar las funciones propias del Delegado de Protección de Datos.

Es de suma importancia proceder a instar al IMAS a que designe un Delegado de Protección de Datos o se faculte al nombrado por el Ayuntamiento a que asuma las funciones propias dentro de ese organismo autónomo dotado de personalidad jurídica pública, patrimonio y tesorería propios, así como plena capacidad para el desarrollo de los fines por los que se crearon, entre ellos el Instituto Municipal de Atención Social como Organismo Autónomo local constituido al amparo de lo previsto en el artículo 85.2.A).b) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local que cuenta con personalidad jurídica pública, patrimonio y tesorería propios, con plena capacidad para el desarrollo de los fines en los términos del artículo 3 de sus Estatutos.

El artículo 37, apartado 1, del RGPD requiere la designación de un DPD en tres casos específicos como es el caso: *a) cuando el tratamiento lo lleve a cabo una autoridad u organismo público.* No requiere la norma que sea único para esta entidad en cuanto que el citado artículo 37, apartado 2, permite a designar a un único DPD, siempre que este sea fácilmente accesible desde cada establecimiento-

En el estado actual, y bajo esa ausencia, se han atendido peticiones de informe complejas, valga recordar sin afán de exhaustividad el alcance del acceso de los concejales a los expedientes que maneja el servicio con las hojas histórico sociales y declaraciones de vulnerabilidad, dependencia, el traslado de datos a otras administraciones públicas de datos contenidos en los expedientes y que afectan a usuarios del sistema, la petición de datos por un organismo bajo el amparo de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, etc.

Pero es más se tiene conocimiento de una petición de acceso no atendida y donde la AEPD ha solicitado información y que hasta la fecha no consta la emisión de respuesta, independientemente de las muestras de apoyo técnico trasladado para materializar el cumplimiento.

ACCIÓN CORRECTIVA

Designación de un Delegado de Protección de Datos.

7.5 No conformidad 05: Falta de análisis de riesgos de T-Systems

NO CONFORMIDAD

Falta de un análisis de riesgo actualizado que recoja todas las dimensiones de seguridad que se deben analizar (trazabilidad y autenticidad).

CONSIDERACIONES

Dentro del proceso de regulación normativa de la entidad se ha procedido a la firma del acuerdo jurídico como encargado de tratamiento con la entidad T-Systems adjudicataria del contrato público para la prestación de dos servicios de soporte y mantenimiento de los módulos que soportan las funciones siguientes:

- Firma biométrica, Sistema de Interconexión de Registros (SIR), Tablón electrónico y notificación electrónica, Portal del Concejal, Archivo Electrónico. Contratación con integración Plataforma Sector Público (Perfil y Licitación), Atención ciudadana, Registro, Registro electrónico, Carpeta ciudadana, Documento electrónico, Gestión documental, Gestor de expedientes, Firma electrónica, Digitalización masiva, Edicta y censos, Actuate y Documentum

- gestión tributaria y recaudatoria

Se encuentra pendiente la aportación de un análisis de riesgo actualizado, ya que el presentado por motivo de una reclamación ante la AEPD es un análisis muy deficiente y descontextualizado (firmado en 2018) que no recogía todas las dimensiones de seguridad que se deben analizar (trazabilidad y autenticidad) .

En este sentido, en reunión de 3 de febrero de 2023, ante responsables de la mercantil se recordó que una entidad que dispone de una certificación de categoría ALTA, como la mercantil debería disponer de un análisis de riesgo a la altura de esta acreditación. Por parte de la entidad hubo un compromiso de presentar un nuevo análisis de riesgo. A fecha de redacción de esta auditoría no ha sido presentado.

ACCIÓN CORRECTIVA

Requerimiento a T-Systems como proveedora de servicios de administración electrónica del

perceptivo análisis de riesgo, debidamente actualizado y que recoja todas las dimensiones de seguridad a analizar (faltan trazabilidad y autenticidad).

7.6 No conformidad 06: Necesidad de revisión del Registro de Actividades de Tratamiento al Sistema Interno de Información de la Ley 2/2023

NO CONFORMIDAD

Falta de actualización del Registro de Actividades de Tratamiento del Sistema Interno de Información de la Ley 2/2023

CONSIDERACIONES

Incorporación de un nuevo tratamiento que determina el Sistema Interno de Información de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción y que entró en vigor el 10 de junio de 2023

ACCION CORRECTIVA

Actualización del Registro de Actividades de Tratamiento en la próxima actualización del RAT.

7.7 No Conformidad 07: Ausencia de revisión previa en las contrataciones en los que existan encargados de tratamiento

NO CONFORMIDAD

Falta de revisión previa en las contrataciones en los que existan encargados de tratamiento

CONSIDERACIONES

Cabe recordar que la Junta de Gobierno de la Ciudad de Santa Cruz de Tenerife, en sesión Ordinaria celebrada el día 2 de mayo de 2022 aprobó la INSTRUCCIÓN RELATIVA A OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS EN LOS CONTRATOS VIGENTES Y POR LICITAR, A EFECTOS DE APROBACIÓN.

En este sentido debe ser modificada en cuanto que han existido cambio normativo en la cláusula V, donde se establecía:

V.- CLÁUSULA A INCLUIR EN TODAS LAS CONTRATACIONES, EN RELACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD (ENS). En cumplimiento con lo dispuesto en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el licitador incluirá en su oferta referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo recogido en el apartado 4.1.5 del anexo II del citado Real Decreto 3/2010, de 8 de enero

Habiéndose promulgado el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, debe de tenerse presente este nuevo marco para garantizar la seguridad en la administración digital en el Ayuntamiento de Santa Cruz de Tenerife y de los derechos de los ciudadanos, así como actualiza las referencias al marco legal vigente y donde se da una respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

A su vez, existe una elevada atomización de órganos del Ayuntamiento de Santa Cruz de Tenerife que redacta los pliegos como poder adjudicador, entre los que se encuadran:

1. Junta de Gobierno
2. Concejalía Delegada Organización, Regimen Interno, Modernización y Coordinación Administrativa, Atención a la Ciudadanía
3. Concejalía Delegada en Materia de Bienestar Comunitario y Servicios Públicos
4. Concejalía Delegada en Materia de Hacienda, Recursos Humanos y Patrimonio
5. Concejal Presidente del Tagoror del Distrito Centro Ifara
6. Concejal Presidente del Tagoror del Distrito Ofra
7. Concejal Presidente del Tagoror del Distrito Salud La Salle
8. Concejal Presidente del Tagoror del Distrito Suroeste

9. Concejalía Delegada de Deportes del Ayuntamiento
10. Concejalía Delegada de Medioambiente, Sanidad y Accesibilidad
11. Concejalía Delegada en Materia de Juventud y Educación del Ayuntamiento
12. Concejalía Delegada en Materia de Promoción Económica, Empleo, Turismo y Comercio
13. Concejalía Delegada en Materia de Proyectos Urbanos, Infraestructuras y Obras
14. Concejalía Delegada en materia de Información al Consumidor
15. Concejalía Delegada en materias de Atención a la Ciudadanía, Estadística, Población y Demarcación Territorial
16. Concejalía Presidencia del Tagoror del Distrito Anaga
17. Concejalía del Área de Seguridad Ciudadana, Vial y Movilidad
18. Consejero Director de la Gerencia Municipal de Urbanismo
19. Consejero Rector de la Gerencia Municipal de Urbanismo
20. Consejo Rector del Instituto Municipal de Asistencia Social
21. Consejo Rector del Organismo Autónomo
22. Consejo Rector del Organismo Autónomo de Fiestas y Actividades Recreativas
23. Gerencia del Instituto Municipal de Atención Social
24. Presidencia del Instituto Municipal de Asistencia Social
25. Presidencia del Organismo Autónomo de Cultura
26. Presidencia del Organismo Autónomo de Fiestas y Actividades Recreativas

Esta atomización determina que en aquellos contratos que se traten datos personales y por lo tanto encargados de tratamiento, existan anomalidades en relación a lo que exige la normativa de aplicación y la Instrucción establece, donde podemos establecer tres cuestiones básicas: la identificación y relación de los datos personales tratados, el lugar de establecimiento de los servidores donde el encargado tratará los datos personales por cuenta del Ayuntamiento y el acuerdo jurídico que establece RGPD en su artículo 28.3.

A modo de ejemplo se han buscado una última contratación del Tagoror de Distrito EXPEDIENTE 145/2023/AIS RELATIVO A TALLERES VERANO DISTRITO CENTRO-IFARA 2023 A DESARROLLAR EN EL CEIP SALAMANCA. Pues bien el acuerdo jurídico del artículo 28.3 del RGPD es deficiente.

ACCIÓN CORRECTIVA

Se hace necesario que todos los contratos que conlleven el tratamiento de datos de carácter personal fueran previamente informados por el Servicio competente en la materia y donde se integra el Delegado de Protección de Datos del Ayuntamiento de Santa Cruz de Tenerife.

7.8 No conformidad 08: Insuficiencia de concienciación y formación en materia de protección de datos

NO CONFORMIDAD

Insuficiencia de concienciación y formación en materia de protección de datos

CONSIDERACIONES

Durante los pasado meses se han intensificado las acciones de concienciación y formativas, a saber:

1. **CIBERSEGUR@S. Campaña de concienciación para el reforzamiento de las medidas de seguridad básicas**

   - 09/06/23 Prohibición del uso de memorias USB
   - 18/03/22 Cibersegur@s. Ciberseguridad en el teletrabajo
   - 17/03/22 Cibersegur@s. Protección de datos personales
   - 16/03/22 Cibersegur@s. ¿Cómo detectar los correos electrónicos fraudulentos?
   - 15/03/22 Cibersegur@s. Protege las contraseñas
   - 14/03/22 Cibersegur@s. Inicio de la campaña de concienciación dirigida a los/as usuarios/as de los sistemas municipales para el reforzamiento de las medidas de seguridad básicas

2. **ACCIÓN FORMATIVA Nº 47 NORMATIVA ADMINISTRATIVA: CÓD. 47.2.2 LEY 3/2018: LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y LA GARANTÍA DE LOS DERECHOS DIGITALES**

"Curso básico en Materia de Protección de Datos" Dirigida a los grupos A-1 y A-2, realizado del 3 de octubre al 3 de noviembre de 2022.

3. **ACCIÓN FORMATIVA Nº 47.2.1 NORMATIVA ADMINISTRATIVA: CÓD. 47.2.2 LEY 3/2018: LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y LA GARANTÍA DE LOS DERECHOS DIGITALES**

"Curso básico en Materia de Protección de Datos" Dirigida a los grupos C-1 y C-2, realizado del 3 de octubre al 3 de noviembre de 2022.

4. **ACCIÓN FORMATIVA NÚMERO 11, CUROS DE SENSIBILIZACIÓN SOBRE LA CIBERSEGUIRDAD Y LA PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN LOCAL** (abierto a todos los grupos), impartido del 13 de junio al 4 de julio de 2023.

Es de significar que el esfuerzo formativo y de concienciación desplegada por el Ayuntamiento de Santa Cruz de Tenerife, no representa obligatoriedad alguna ni tiene ningún efecto la asistencia y el aprovechamiento de los partic0panets matriculados. Así los resultados conseguidos son muy limitados como reflejan los informes finales de las acciones reseñadas.

Cabe señalar que el Cuerpo de la Policía Local, no obstante cuenta con una plantilla de 387 agentes y normas específicas en materia de protección de datos (Ley Orgánica 7/2021) ha quedado fuera de la planificación de la formación general municipal al tener un programa de formación propio.

Por último, como ya se ha referido, la planificación presentada de la presente auditoría ha tenido en cuenta la celebración de entrevistas con responsables municipales que ha sufrido una incidencia al no haberse podido ser llevadas a cabo ante la ausencia de respuesta y, en consecuencia, de participación de los responsables convocados por la Jefe de Servicio Organización y Gobierno Abierto, a excepción de las siguientes:

- Policía Local
- Sede administrativa de La Granja
- Servicios Jurídicos

Como medida de contingencia se ha tenido que modificar el enfoque metodológico participativo de la auditoría interna lo que, en sí mismo, constituye un hallazgo relevante.

ACCION CORRECTIVA

Elaborar un plan de concienciación y formación en materia de protección de datos personales que afecte a todos los responsables y el personal del Ayuntamiento con carácter de obligatoriedad.

8. EVALUACIÓN DE CUMPLIMIENTO NORMATIVO

A continuación se detalla una evaluación de cumplimiento normativo de la entidad verificando los deberes y obligaciones en materia de protección de datos y tomando como normas marco 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

8.1. Revisión de los procedimientos de la Sede Electrónica

CONTROL	CUMPLE (SI/NO)
Se recogen los datos personales con fines determinados	SI
Se recogen los datos personales con fines explícitos	SI
Se recogen los datos personales con fines legítimos	SI
Se tratan ulteriormente de manera incompatible con otros fines	NO
Los datos personales se mantienen exactos	NO
Se mantienen actualizados	SI
Se rectifican los datos personales inexactos respecto de la finalidad	SI
Se suprimen los datos personales inexactos respecto de la finalidad	SI
Se mantienen durante más tiempo del necesario respecto de la finalidad	NO
Se tratan con fines de archivo en interés público	SI (1)
Se tratan con fines de investigación científica	NO
Se tratan con fines históricos	SI
Los datos personales se tratan con fines estadísticos	NO

Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	SI (2)
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	SI
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	SI
Se mantiene la trazabilidad de los fines del tratamiento	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Si bien se recogen la mayoría de los principios generales de tratamiento y que es la base central del RGPD, existe un elemento clave que no cumple la entidad en cuanto que los 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»).

Se ha acreditado evidencia sobre el particular siendo de aplicación el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad de aplicación al sector público donde se encuentra una Fundación pública.

Hay una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Se dispone de una política de seguridad adecuada lo que no pone en riesgo las dimensiones de seguridad del sistema de información, y se comprueba que están en riesgo los datos personales en cuanto a las dimensiones de seguridad de la integridad y confidencialidad se vea comprometida.

Integridad: O mantenimiento de las características de completitud y corrección de los datos.

Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no

autorizados.

La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

RECOMENDACIONES

1. Algunos supuestos pueden pasar a los archivos históricos por sus relevancia o el tiempo de conservación permite dotarle de esa naturaleza, por ejemplo datos personales del padrón de habitantes
2. La entidad que soporta la sede electrónica y como consta en esta auditoría debe de proceder a aportar un Análisis de Riesgo actualizado tal y como se ha justificado.

LEGISLACIÓN

Reglamento (EU) 679/2016 de 27 de Abril de Protección de Datos

Artículo 5

Principios relativos al tratamiento

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del

interesado («limitación del plazo de conservación»);

f) 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»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. TÍTULO II. Principios de protección de datos

Artículo 4. Exactitud de los datos.

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del

obligado con el responsable o encargado del tratamiento.

8.2. Licitud del tratamiento

CONTROL	CUMPLE SI/NO/No aplica(N/A)
Se tiene consentimiento para cada finalidad del tratamiento	N/A (1)
El tratamiento es necesario para ejecutar un contrato o precontrato	SI
Existe obligación legal	SI
El tratamiento es necesario para proteger intereses vitales	N/A
El tratamiento es necesario para el cumplimiento de interés público	SI
El tratamiento es necesario para satisfacer intereses legítimos	NO

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

La licitud del tratamiento es una base jurídica fundamental y elemento fundamental en el tratamiento de datos personales, en cuanto que cuando falta esta es ilícito. El tratamiento de datos siempre deberá de tener acomodo en una de las seis bases jurídicas que establece el RGPD en su artículo 6.

(1) El consentimiento no es la base general que deba de regir entre una Administración-administrados o empleados públicos, ya que está en una situación de desequilibrio que hace que el consentimiento no reúna los requisitos para entenderlo prestado libremente y en igualdad de condiciones. La base jurídica detectada en la Administración está en el cumplimiento de una obligación legal o por el ejercicio de las competencias del Ayuntamiento (propias o delegadas).

Se constata que los tratamientos analizados siempre se constata una base jurídica adecuada.

LEGISLACIÓN

Ley de Bases de Régimen Local (y toda la normativa que desarrolla las competencias de la Administración Local)

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Artículo 2. Ámbito de aplicación.

*1. El presente real decreto **es de aplicación a todo el sector público**, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.*

Ley 7/2015, de 1 de abril, de los municipios de Canarias.

8.3. Tratamiento de categorías especiales de datos

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se tratan los datos sólo cuando existen normas que lo exceptúen	SI
Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento	NO
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho	SI
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho	SI
Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento	NO

Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical)	N/A
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados	N/A
Se tratan datos que el interesado ha hecho manifiestamente públicos	N/A
Es necesario para la formulación, el ejercicio o la defensa de reclamaciones	NO
Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social	SI
Es necesario por razones de interés público en el ámbito de la salud pública sobre la base normas de Derecho que establece medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional	NO
Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho	NO
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Se tratan los datos de carácter sensible solo en aquellos supuestos que son necesarios para el mantenimiento de la relación laboral y estatutaria de los funcionarios públicos, existiendo en estos supuestos normas con rango de ley que permiten el tratamiento.

RECOMENDACIONES

- Debe seguirse con especial diligencia el tratamiento de estos datos considerados sensibles como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, ya que por su naturaleza son en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

- Consta a su vez el tratamiento del Registro de Jornada que se torna obligatorio por Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo y es llevado a cabo, con carácter general con una aplicación que toma la huella dactilar. A su vez la entidad ha aportado un análisis de riesgos conforme a lo solicitado por esta Administración**, sin embargo debe ser completado con una evaluación de impacto que reafirme que no supone una vulneración a los derechos de los empleados.**

LEGISLACIÓN

Reglamento (UE) 2016/679

Artículo 9

Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados

miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. (…)

***Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales**.*

Artículo 9. Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

8.4. Tratamiento relativos a condenas e infracciones penales

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se tratan los datos bajo la supervisión de las autoridades públicas	SI
Se tratan los datos bajo la autorización de normas de derecho	SI
El registro completo de condenas penales se realiza bajo el control de las autoridades públicas	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

La Policía Local tiene acceso (y en ejercicio de su fusión de garantizar la seguridad ciudadana) a los antecedentes penales de personales mediante mecanismos de intermediación con los Juzgados donde esos datos son necesarios en la elaboración de atestados o en funciones de prevención e investigación de infracciones penales, de acuerdo con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

RECOMENDACIONES.

Se había dejado constancia en informes anteriores que el sistema de información policial utilizado (Eurocop) y en especial todas las medidas organizativas deben de adecuarse a la Política de Seguridad del Ayuntamiento

LEGISLACIÓN

Reglamento (UE) 2016/679

Artículo 10

Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 10. Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Carencia o existencia de Delitos de Naturaleza Sexual que constan en el Registro Central de Delincuentes Sexuales en la fecha en que son expedidos.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

8.5. Identificación de interesados

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	NO
Se obtiene y/o trata información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	NO
Se puede demostrar que los datos anonimizados no permiten identificar a los interesados	SI
Se informa al interesado y se recaba su consentimiento cuando se llega a su identificación	N/A
Se cancelan los datos cuando se llega a identificar al interesado	SI

NIVEL DE CUMPLIMIENTO CONFORMIDAD.

No se da el supuesto de tratamientos que no requieran autentificación.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679

Artículo 11

Tratamiento que no requiere identificación

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente

Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

8.6. Derechos del interesado. Transparencia de la información

CONTROL	CUMPLE (SI/NO/No aplica)
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	SI (1)
La información se facilita de forma concisa, transparente e inteligible	SI
La información se facilita en lenguaje claro y sencillo	SI
Se facilita por escrito o por otros medios, incluidos los electrónicos	SI
Se facilita verbalmente, previa acreditación de su identidad	SI
Se facilita al interesado el ejercicio de sus derechos	SI
Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	N/A
Se informa al interesado en el plazo de un mes	SI

desde la recepción de su solitud	
Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud	N/A
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	SI
Se permite a los interesados el ejercicio de derechos por medios electrónicos	SI
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	SI
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud	SI
Se facilita gratuitamente el ejercicio de derechos	SI
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	SI
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	N/A

NIVEL DE CUMPLIMIENTO:CONFORMIDAD.

Revisadas la cláusula de los formularios, página web, cumple el derecho de informar. A su vez utiliza la información por capas multinivel lo que permite una fácil comprensión a los interesados (la hace concisa y transparente). No se emplea tal y como se hacía constar lenguaje farragoso en su redacción.

NO CONFORMIDAD en tratamientos de la Policía Local de conformidad con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, extremo que se ha puesto en apartado aparte del informe.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679

Artículo 12

Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los

motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a)cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 12. Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

8.7. Derechos del interesado. Información

CONTROL	CUMPLE SI/NO/No aplica
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	SI
Se facilitan los datos de contacto del delegado de protección de datos	SI
Se facilitan los fines del tratamiento a que se destinan los	SI

datos personales y la base jurídica del tratamiento	
Se facilita información sobre el interés legitimo	N/A (1)
Se informa sobre los destinatarios o las categorías de destinatarios	SI
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	SI
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	SI
Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento	N/A
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se informa de las cesiones basadas en requisitos legales o contractuales	SI
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	N/A
Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento	N/A
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	SI

NIVEL DE CUMPLIMIENTO:CONFORMIDAD.

De la revisión de la documentación (formularios, registros de tratamiento) se cumple con el deber de facilitar información.

No se aplica en dos tratamientos, en cuanto no existe ninguno que suponga la existencia de elaboración de perfiles y a su vez no hay tratamiento que tengan su base una finalidad distinta de la inicial.

(1) El Ayuntamiento de Santa Cruz de Tenerife no utiliza como base jurídica el interés legítimo en cuanto que no es una base jurídica adecuada conforme al RGPD.

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos.

Artículo 13

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c)los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d)cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f)en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al

hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a)el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b)la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c)cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e)si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f)la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

8.8. Derechos del interesado. Acceso

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se informa respecto a los fines del tratamiento	SI
Se informa de las categorías de datos personales que se tratan	SI
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	SI
Se informa del plazo previsto de conservación de los datos personales	SI
Se informa de los criterios utilizados para determinar el plazo de conservación	SI
Se informa del derecho a solicitar la rectificación o supresión de sus datos	SI
Se informa del derecho a solicitar la limitación del tratamiento de los datos	SI
Se informa del derecho a solicitar la oposición al tratamiento	SI (1)
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	SI
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	SI
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se	SI

facilite otro medio	

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Analizados todos los formularios se comprueba que informan sobre el derecho de acceso y de conformidad con la legislación

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 15

Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c)los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d)de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e)la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g)cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h)la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

artículo 13. Derecho de acceso.

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista

causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

8.9. Derechos del interesado. Rectificación

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se rectifican los datos personales inexactos sin dilación indebida	SI
Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Del análisis de la documentación y recogidas las evidencias, se cumple con este derecho de los interesados.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 16

Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la

rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 14. Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

8.10. Derechos del interesado. Supresión (Derecho al olvido")

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	SI
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	N/A (1)
Se suprimen los datos cuando se opone al tratamiento	SI
Se suprimen los datos cuando han sido tratados ilícitamente	SI
Se suprimen los datos cuando lo exige una obligación legal	SI
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la	N/A

información	

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

De las revisiones efectuadas mediante la ejecución de pruebas técnicas: accesos, visualización de recursos, se ha comprobado que el ejercicio al derecho de supresión es correcto, existiendo procedimientos para que sea real y efectivo.

(1) No existen tratamientos con la base jurídica del consentimiento en cuanto que los tratamientos de la sede electrónica derivan del ejercicio de competencias propias o mandato legal

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 17

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a)los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b)el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c)el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e)los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f)los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 15. Derecho de supresión.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

8.11. Derechos del interesado. Limitación

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	SI
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso	SI

Se limita el tratamiento cuando no son necesarios para los fines pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones	SI
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	SI
Se informa al interesado cuando se levanta la limitación del tratamiento	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Del análisis de la documentación (formularios de la sede electrónica) y recogidas las evidencias, se cumple con este derecho de los interesados.

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 18

Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a)el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b)el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c)el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d)el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 16. Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

8.12. Derechos del interesado. Rectificación, supresión o limitación en el tratamiento

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se comunican al interesado la rectificación, supresión o limitación en el tratamiento	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD

Del análisis de la documentación y recogidas las evidencias, se cumple con este derecho de los

interesados.

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 19

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

8.13. Derechos del interesado. Portabilidad

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica	N/A (1)
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato.	N/A
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	N/A
Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente	N/A

(1) En los tratamientos que realiza el Ayuntamiento de Santa Cruz de Tenerife y por su propia naturaleza, no se puede aplicar ya que el tratamiento y su base jurídica se asienta en el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Del análisis de la documentación y recogidas las evidencias, se cumple con este derecho de los interesados.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 20

Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a)el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de

otros.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 17. Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

8.14. Derechos del interesado. Oposición

CONTROL	CUMPLE SI/NO/No aplica (N/A)
Se atienden las solicitudes de oposición y se dejan de tratar los datos	SI
Se atienden las solicitudes de oposición, pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	SI
Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Del análisis de la documentación y recogidas las evidencias, se cumple con este derecho de los interesados.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 21

Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 18. Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido,

respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

8.15. Derechos del interesado. Decisiones individuales automatizadas, incluida la elaboración de perfiles

CONTROL	CUMPLE SI/NO/No aplica (n/a)
No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos	SI
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato	NO
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	NO
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	NO
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	NO
Si se realizan tratamientos que suponen la toma una	NO

decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión	NO
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado	NO
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	NO
Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas	N/A
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	NO

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

De las evidencias obtenidas (acceso y visualización de registros) se comprueba que **no existen** tratamientos automatizados basados en la elaboración de perfiles.

RECOMENDACIONES. No se formulan

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 22

Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a)es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b)está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

8.16. Derechos del interesado. Responsabilidad

CONTROL	CUMPLE SI/NO/ No aplica (n/a)
Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD	SI
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	SI
Se aplican medidas técnicas y organizativas apropiadas	SI
Las medidas se revisan y actualizan cuando es necesario	SI
Se han confeccionado políticas de protección de datos	SI
Se aplican las políticas de protección de datos	SI

NIVEL DE CUMPLIMIENTO:CONFORMIDAD.

De las revisiones efectuadas se puede establecer que existe una política de privacidad completa. Las medidas adoptadas garantizan los derechos básicos de los ciudadanos, existen como se ha puesto de manifiesto posibles ejercicios de derechos, existe una política completa de privacidad que prevea esas situaciones lo que facilita la gestión y decisión.

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos *Artículo 24*

Responsabilidad del responsable del tratamiento

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.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.

1. 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.

8.17. Protección de datos desde el diseño y por defecto

CONTROL	CUMPLE SI/NO
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento	SI

Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	SI
Durante el tratamiento se aplican las medidas que han sido determinadas	SI
Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	SI
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	SI
Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad	SI
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

De las comprobaciones realizadas se comprueba que se ha valorado el riesgo para determinar las amenazas en el tratamiento de datos personales y valorar si fuera necesario establecer más medidas de seguridad. El sistema de información se basa en el principio de la necesidad de conocer.

RECOMENDACIONES. Nos se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 25

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el

momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

8.18. Corresponsables del tratamiento

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se han determinado de modo transparente, y de mutuo acuerdo, las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD	N/A
El acuerdo fija las respectivas obligaciones de suministro de información al interesado	N/A
El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados	N/A
Los aspectos esenciales del acuerdo están a disposición del interesado	N/A

NIVEL DE CUMPLIMIENTO

(1) De las revisiones de los tratamientos no existe ninguno de ellos donde se constate esta figura, es decir el Ayuntamiento no figura junto a otro responsable determinen conjuntamente los objetivos y los medios del tratamiento.

RECOMENDACIONES. No se efectúan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 26

Corresponsables del tratamiento

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 29. Supuestos de corresponsabilidad en el tratamiento.

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los

corresponsables del tratamiento.

8.19. Encargado del tratamiento

CONTROL	CUMPLE (SI/NO o N/A)
Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado	SI
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	SI
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	SI (1)
El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos del responsable	SI
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable	SI
El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria	SI
El contrato establece que se tomarán las medidas de seguridad necesarias	SI
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	SI

El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados	SI
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	SI
El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable	SI
El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho	SI
El contrato consta por escrito	SI
Sólo se accede a los datos siguiendo instrucciones del responsable	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

De las evidencias constatadas se comprueba que la relación con los encargados de tratamiento es conforme a la norma y se rige por un acto jurídico que establece las obligaciones del encargado.

Se ha formulado una instrucción general para unificar los acuerdos jurídicos de conformidad con el artículo 28.3 del RGPD

RECOMENDACIONES.

Como ya ase ha referido con anterioridad el gran número de unidades y organismos del Ayuntamiento que participan en la contratación pública, genera disfunciones y, en algunos casos, analizados el acuerdo jurídico del artículo 28.3 del RGPD no sigue en su integridad lo establecido en la instrucción.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 28

Encargado del tratamiento

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a)tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b)garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a

respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d)respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e)asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f)ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g)a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h)pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos

digitales

Artículo 33. Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

8.20. Registro de Actividades de tratamiento

CONTROL	CUMPLE SI/NO/NO APLICA (N/A)
Se lleva un registro de las actividades de tratamiento	SI (1)
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	SI
El registro recoge los fines del tratamiento	SI
Se recoge una descripción de las categorías de interesados y de las categorías de datos personales	SI
Se recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	SI
Se recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	N/A
Se incluyen los plazos previstos para la supresión de las categorías de datos	SI
Se incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	SI
Se publica en la web de la entidad	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

De la documentación analizada, la comprobación de la web, se comprueba la publicación del RAT con las exigencias de la Ley.

RECOMENDACIONES.

(1) Consecuente de la revisión continúa se ha constatado en el cuerpo de esta auditoría la necesidad de inclusión de un nuevo tratamiento.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 30

Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las

categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a)el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c)en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d)cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 31. Registro de las actividades de tratamiento.

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

8.21. Seguridad del tratamiento

CONTROL	CUMPLE SI/NO/No aplica (n/a)/
Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	SI
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	SI
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	SI
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	SI
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	SI
Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción,	SI

pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	
Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

(1) El Ayuntamiento de Santa Cruz de Tenerife está en proceso de adecuación al ENS, la sede electrónica y principales servicios tiene un encargado de tratamiento, T-Systems, certificado en la CATEGORÍA ALTA en el sistema de información TAO, desde donde se presta el servicio de soporte y mantenimiento de los módulos que soportan la: Firma biométrica, Sistema de Interconexión de Registros (SIR), Tablón electrónico y notificación electrónica, Portal del Concejal, Archivo Electrónico. Contratación con integración Plataforma Sector Público (Perfil y Licitación), Atención ciudadana, Registro, Registro electrónico, Carpeta ciudadana, Documento electrónico, Gestión documental, Gestor de expedientes, Firma electrónica, Digitalización masiva, Edicta y censos, Actuate y Documentum.

No obstante se la ha solicitado a ese proveedor un análisis de riesgos actualizado.

RECOMENDACIONES.

Deberá continuarse con la adecuación al ENS y requerir el análisis de riesgo solicitado al encargado de tratamiento T-Systems y que fue objeto de análisis específico.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

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.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Artículo 2. Ámbito de aplicación.

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

Artículo 3. Sistemas de información que traten datos personales.

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

8.22. Notificación de brechas de la seguridad de los datos personales

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	SI
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	SI
Existe un procedimiento para notificar a la autoridad de	SI

control en el plazo de 72 horas	
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	SI
Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	SI
Se documenta cualquier brecha de seguridad de los datos personales	SI
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	SI
Se ha comprobado que el procedimiento de notificación funciona	SI
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades	SI
La comunicación al interesado se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

El Comité de Seguridad del Ayuntamiento de Santa Cruz de Tenerife ha aprobado un protocolo para la gestión de las brechas personales. Y en las brechas detectadas se ha aplicado lo que ha permitido gestionar el incidente.

RECOMENDACIONES. No se realizan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 33

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

8.23. Evaluación de impacto

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se recaba el asesoramiento del DPD	SI
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	SI
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	SI
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	SI
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	SI
La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido	SI
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	SI
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	SI
Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y	SI

de otras personas afectadas	
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	SI
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	SI
Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo	SI
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	SI
Se informa de los fines y medios del tratamiento previsto en la consulta	SI
Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	SI
Se facilitan los datos de contacto del delegado de protección de datos	SI
Se incluye la evaluación de impacto	SI

NIVEL DE CUMPLIMIENTO: CONFORMIDAD.

Las EIPD realizadas responden a los anteriores criterios.

RECOMENDACIONES. No se realizan,

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 35

Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a)evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b)tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente

aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a)una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b)una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c)una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d)las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen

las operaciones de tratamiento.

8.24. Delegado de protección de datos

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se ha designado un DPD por requerimiento legal	SI
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	SI
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	SI
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	SI
Se da respaldo en el desempeño sus funciones	SI
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento	(1)
Se le facilitan los recursos necesarios para mantener sus conocimientos	SI
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	SI
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	SI
El DPD rinde cuentas directamente al más alto nivel	SI

jerárquico	
El DPD atiende las solicitudes de los interesados	SI
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	SI
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	NO
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	SI
El DPD coopera y actúa como punto de contacto con la autoridad de control	SI

(1) En este informe consta una NO CONFORMIDAD sobre el uso indirecto del correo electrónico asignado y comunicado a la Autoridad de Control (dpd@santacruzdetenerife.es) y donde entiende el DPD que debe de tener acceso sin intermediación de los correos recibidos, independientemente que se trate de un DPD perteneciente a una entidad externa.

El correo electrónico facilitado a la Autoridad de Control y que figura como punto de contacto deberá ser accesible directamente por el DPD.

RECOMENDACIONES. No se formulan

L**EGISLACIÓN**

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 37

Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a)el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b)las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c)las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38

Posición del delegado de protección de datos

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de

datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 34. Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran

escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. Posición del delegado de protección de datos.

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales

y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

8.25. Transferencias a países terceros u organizaciones internacionales

CONTROL	CUMPLE SI/NO/No aplica (n/a)
Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de	N/A

nivel de protección adecuado por la Comisión Europea	
Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea	N/A
Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales.	N/A
Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas	N/A

NIVEL DE CUMPLIMIENTO

De las evidencias obtenidas del Ayuntamiento de Santa Cruz de Tenerife no realiza ninguna transferencia de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional.

RECOMENDACIONES. No se formulan.

LEGISLACIÓN

Reglamento (UE) 2016/679 de Protección de Datos

Artículo 44

Principio general de las transferencias

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos

digitales

Transferencias internacionales de datos

Artículo 40. Régimen de las transferencias internacionales de datos.

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

9. CONCLUSIONES Y PROPUESTA DE ACTUACIONES

PRIMERA.- Se han evidenciado un conjunto de **OCHO (8) NO CONFORMIIDADES** normativas que deberán ser subsanadas por el AYUNTAMIENTO DE SANTA CRUZ DE TENERIFE.

#	DESCRIPCIÓN	CALIFICACIÓN
01	El correo electrónico de contacto del Delegado de Protección de Datos (dpd@santacruzdetenerife.es) no es accesible por este, lo que puede suponer una limitación, en plazo y/o forma, de las reclamaciones o consultas en relación con el desarrollo de las competencias que le son propias.	MAYOR
02	Publicación del catálogo de puestos de trabajo del Ayuntamiento con información identificativa.	MAYOR
03	Insuficiente adecuación normativa de los tratamientos de datos personales de la Policía Local. 3. Existencia de archivo no automatizado sin garantías. 4. Insuficiencia de información en materia de protección de datos.	MAYOR

04	Falta de designación de un DPD por el Instituto Municipal de Atención (IMAS).	MAYOR
05	Falta de análisis de riesgos de T-Systems como encargada de servicios de administración electrónica	MAYOR
06	Actualización del Registro de Actividades de Tratamiento del Sistema Interno de Información de la Ley 2/2023.	MENOR
07	Ausencia de una revisión previa en las contrataciones en los que existan encargados de tratamiento.	MENOR
08	Insuficiencia de concienciación y formación en materia de protección de datos	MAYOR

SEGUNDA.- A la fecha del presente informe, se encuentran abiertas **DOS (2) INCIDENCIAS** en relación con la Agencia Española de Protección de Datos, a saber:

#	IDENTIFICACIÓN	ESTADO
01	Información relativa a brecha de seguridad de suplantación de identidad comunicada por el Ayuntamiento de Santa Cruz de Tenerife el 27/07/2023 dentro del expediente REGAGE23e00051172382.	**EN PLAZO**
02	Traslado de reclamación de una interesada y solicitud de información al IMAS (Expediente N.º: EXP202307047) notificada el 30/05/2023.	**FUERA DE PLAZO**

TERCERA.- Se ha realizado una evaluación de cumplimiento normativo de la entidad verificando los deberes y obligaciones en materia de protección de datos y tomando como normas marco 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la que se propone un conjunto de recomendaciones que deberán ser priorizadas para su debida implantación.

10. ANEXO I.

Adaptación al Reglamento General de Protección de Datos y Esquema Nacional de Seguridad. N.º Expediente: 86/2019/TEC

Planificación de auditoría de cumplimiento normativo en materia de protección de datos personales

Fecha: 25/05/23

Versión: 1.0

Índice

5. ANTECEDENTES

Dentro del expediente de contratación número 86/2019/TEC la Junta de Gobierno Local, en sesión ordinaria celebrada con fecha 29 de julio de 2021, adoptó el acuerdo de adjudicar el "SERVICIO DE ADAPTACIÓN AL ENS, AL REGLAMENTO EUROPEO Y A LA LEY 3/2018" a la entidad EstudNET SL y a cuyo cargo se establece la función del desempeño de papel de Delegado de Protección de Datos (en lo sucesivo, DPD) del Ayuntamiento de Santa Cruz de Tenerife.

En fecha 13 de septiembre de 2021 el concejal de Tecnología acepta la designación realizada por la empresa EstudNET, SL con CIF B92236603, adjudicataria del contrato de "Servicio de consultoría de adaptación al ENS, al Reglamento Europeo de Protección de Datos y a la Ley Orgánica 3/2018" y se da cuenta del nombramiento a la Agencia Española de Protección de Datos del designado.

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 (en lo sucesivo, RGPD), establece entre las funciones del Delegado de Protección de Datos la de informar y asesorar al responsable o encargado de tratamiento y los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión, en nuestro caso la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDPGDD) y que recoge idéntica función.

Una de las funciones del DPD es informar y asesorar al Ayuntamiento de Santa Cruz de Tenerife y a los empleados que se ocupen del tratamiento, sobre las obligaciones del RPGD y demás normativa aplicable en protección de datos, así como supervisar su cumplimiento, dentro de esta función se desarrolla el presente informe.

6. OBJETO DEL PRESENTE INFORME

El objeto del presente informe es documentar la planificación de la auditoría de cumplimiento normativo en materia de protección de datos personales del Ayuntamiento de Santa Cruz de Tenerife.

La auditoría da respuesta al principio de responsabilidad proactiva (artículo 5.2) del RGPD, que indica que el responsable de los tratamientos, más allá de cumplir con los principios normativos, deberá disponer de las evidencias de cumplimiento de las medidas implantadas con la finalidad de poder demostrar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos.

7. OBJETIVOS DE LA AUDITORÍA

Los objetivos perseguidos a través de la auditoría son los siguientes:

- Recopilar y verificar las evidencias de cumplimiento del AYUNTAMIENTO en materia de protección de datos personales.

- Identificar y evaluar las No Conformidades del AYUNTAMIENTO que constituyan un incumplimiento, formal o material, de las obligaciones normativas de protección de datos personales.

- Revisar y validar las acciones correctivas y preventivas a implantar por el AYUNTAMIENTO para la subsanación de las No Conformidades detectadas.

8. ALCANCE DE LA AUDITORÍA

El ámbito subjetivo de la auditoría es el de los órganos municipales del Ayuntamiento de Santa Cruz de Tenerife, entendiendo por órganos a sus áreas y distritos, unidades administrativas,

organismos autónomos y demás entidades públicas vinculadas o dependientes (en adelante, el AYUNTAMIENTO).

El ámbito objetivo de la auditoría son las operaciones de tratamiento de datos de personales llevadas a cabo por los órganos municipales del AYUNTAMIENTO, como responsable y encargada.

En consecuencia, el alcance de la auditoría cubre la revisión normativa de los sistemas de información, procesos y personal que traten, recojan, consulten, utilicen, almacenen o necesiten acceder a datos de carácter personal ya sea de manera automatizada o no.

El alcance de obligaciones a evaluar de la auditoria cubre los aspectos que siguen:

1.- Principios relativos al tratamiento

2.- Licitud del tratamiento

3.- Condiciones para el consentimiento

4.- Consentimiento menores (si aplica)

5.- Tratamiento de categorías especiales de datos

6.- Tratamientos relativos a condenas e infracciones penales

7.- Tratamientos que no requieren identificación

8.- Derechos del interesado. Transparencia de la información

9.- Derechos del interesado. Información a facilitar cuando los datos se obtienen del interesado

10.- Derechos del interesado. Información a facilitar cuando los datos no se obtienen del interesado

11.- Derechos del interesado:

a. Acceso

b. Rectificación

c. Supresión («el derecho al olvido»)

d. Limitación del tratamiento

e. Portabilidad de los datos

f. Oposición

12.- Encargados del tratamiento

13.- Registro de las actividades de tratamiento

14.- Seguridad del tratamiento

9. NORMATIVA Y DOCUMENTACIÓN DE APLICACIÓN

La normativa de aplicación en el ámbito de la auditoría es la siguiente:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen

gobierno.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. (LCSP)

- UNE-EN ISO/IEC 27701:2021. Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información.
- Guía de Buenas Prácticas en Auditorías RGPD de ISMS Forum
- Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. AEPD
- Guía práctica para Evaluaciones de Impacto en Protección de los Datos sujetas al RGPD. AEPD
- Guía práctica (enero de 2018, versión 2.0). Evaluación de impacto relativa a la protección de datos. EIPD-APDCAT
- Guía de orientaciones y procedimientos-anonimización de datos personales. AEPD
- Guía para la gestión y notificación de brechas de seguridad. AEPD
- Guía de Privacidad desde el Diseño - Agencia Española de Protección de Datos (2020)
- Guía sobre el uso de las cookies. AEPD. Julio 2020
- Guía La privacidad desde el diseño y la privacidad por defecto. Guía para desarrolladores. Febrero 2023. APDCAT.

10. METODOLOGIA DE LA AUDITORÍA

La metodología a seguir para la evaluación del cumplimiento normativo se fundamenta, en primer

término, en la aportación de evidencias objetivas documentales que demuestren el cumplimiento por el AYUNTAMIENTO de una obligación en materia de protección de datos personales.

A su vez, una desviación detectada de la norma distinguirá las calificaciones siguientes:

- **No Conformidad Mayor:** un incumplimiento formal de una obligación legal

- **No Conformidad Menor:** un incumplimiento material de una obligación legal

de acuerdo con los criterios de impacto siguientes:

- **Perjuicio a las personas:** Puede ocasionar un daño a los derechos y libertades fundamentales de las personas en materia de protección de datos personales.

- **Incumplimiento normativo:** Existe un incumplimiento de una disposición legal, administrativa o regulación.

- **Daño reputacional**: Puede ocasionar un perjuicio reputacional a la imagen pública e institucional del AYUNTAMIENTO.

	PERJUICIO A LAS PERSONAS	**INCUMPLIMIENTO NORMATIVO**	**DAÑO REPUTACIONAL**
No Conformidad Mayor	Daño grave de difícil o imposible reparación (*)	Incumplimiento material grave de una norma jurídica.	Perjuicio reputacional grave a la imagen pública e institucional
			Perjuicio reputacional relevante a la imagen pública

No Conformidad Menor	Daño relevante de posible subsanación.	Incumplimiento formal de una norma jurídica de posible subsanación.	e institucional.

(*) Entre los supuestos de grave daño al afectado se encuentran aquellos que afecten al ejercicio de sus derechos fundamentales y libertades públicas establecidos por la Constitución Española, como la revelación no autorizada de datos personales de categoría especial.

11. EQUIPO DE AUDITORÍA

A continuación, se identifican los responsables del AYUNTAMIENTO que participará en la auditoría.

- D. José Antonio Herrera Umpiérrez, Responsable de la Información y del Servicio

- D. Manuel Pérez Coca, Responsable de Seguridad de la Información

- Dña. María del Cristo Morales, Jefe de Servicio Organización y Gobierno Abierto.

- D. Ángel Yuste, Delegado de protección de datos

12. AGENDA DE LA AUDITORÍA

La agenda planificada para la ejecución de la auditoría del AYUNTAMIENTO es la siguiente:

Actividad	Semana 1	Semana 2	Semana 3	Semana 4
1. Revisión documental.	29/05-02/06/23			
2. Entrevistas con responsables de Áreas de Gobierno.		5-9/06/23		
3. Elaboración del informe auditoría y del plan de acciones correctivas.			12-16/06/23	
4. Presentación del informe de auditoría y del plan de acciones correctivas.				19/06/23

La muestra de entrevistas propuestas se realizaran, en modo remoto o presencial, atendiendo a la programación siguiente:

Área de Gobierno	Fecha	Hora/Responsables a entrevistar
Presidencia	**05/06/23**	
1. Atención Ciudadana		1. 10:00-11:00 /Responsable 1
2. RRHH		2. 12:00-13:00/Responsable 2
	06/06/23	3. 10:00 – 11:00/Responsable 3
3. Servicio Jurídico		
Seguridad, Movilidad y Accesibilidad Universal	**06/06/23**	
4. Policía Local		4. 10:00-11:00/Responsable 4
Hacienda y Patrimonio		
5. Recaudación	**07/06/23**	5. 10:00-11:00/Responsable 5
6. Contratación		6. 12:00-13:00/Responsable 6
Políticas sociales		
7. Atención social	**07/06/23**	7. 10:00-11:00/Responsable 7

Para la recopilación y almacenamiento de evidencias, EstudNET SL habilitará un repositorio seguro para la custodia de documentos (Google Workspace) con acceso autorizado de los integrantes del

equipo del AYUNTAMIENTO .

13. ENTREGABLES DE LA AUDITORÍA

El informe de auditoría, a elaborar por EstudNET SL tendrá el contenido que sigue:

Capítulo	Contenido
1. ANTECEDENTES	- Figura legal, estructura de áreas de gobierno y competencias del AYUNTAMIENTO. - Objetivos de la auditoría.
2. RESUMEN EJECUTIVO	- Fortalezas, No conformidades de, Observaciones y oportunidades de mejora
3. ALCANCE	- Ámbito objetivo y subjetivo -
4. MARCO LEGAL	- Normativa aplicable y documentación de referencia.
5. METODOLOGÍA	- Descripción de la metodología de evaluación de cumplimiento.
6. HALLAZGOS	- Descripción de fortalezas, observaciones, oportunidades de mejora y de No Conformidades. - Evaluación de No Conformidades (Menor, Mayor) y

trazabilidad con la normativa de referencia.

7. ANEXOS	- Registro de actividades de tratamiento. - Relación de encargados. - Notas de las entrevistas - Historiales profesionales del equipo auditor

El plan de acciones correctivas tendrá el contendido que sigue:

Aspecto	**Contenido**
1. No Conformidad	- Descripción de la No conformidad
2. Acción correctiva	- Descripción de la subsanación de la No Conformidad.
3. Responsable de la acción correctiva	- Persona responsable de la implantación de la acción correctiva
4. Plazo de implantación	- Fecha prevista de implantación de la acción correctiva.
5. Causa raíz	- Análisis de la causa raíz de la No Conformidad. - Acciones para eliminar la causa raíz.
6. Anexos	- Evidencias de la implantación de la acción correctiva.

14. ANEXO: PUNTOS A TRATAR EN LAS ENTREVISTAS CON RSPONSABLES

1. Registro de operaciones de tratamiento. Se revisan las actividades del tratamiento y se comprueba su puesta al día del Registro.

2. Licitud de los tratamientos. Se comprueba que todos los tratamientos de datos son lícitos y se ajustan a la legalidad y lo establecido en el artículo 6 del RGPD, cumpliéndose con los principios para ello.

3. Acuerdos de encargado y con encargados. Se identifican los acuerdos con terceros que acceden a datos responsabilidad del AYUNTAMIENTO y se comprueba su existencia.

4. Formación y concienciación. Se revisa si los empleados han participado en los curso de formación a en materia de protección de datos.

11. ANEXO II. NOTAS DE LAS ENTREVISITAS PRESENCIALES

a. POLICIA LOCAL:

- Interlocutor: Policía Local D. Benito Fortes
- Lugar: Jefatura de la Policía Local
  - Revisión de formularios administrativos (información básica falta por actualizar)
  - Avances en la gestión de Eurocop (por recomendación se está procediendo a establecer un marco organizativo)
  - Necesidad específica de formación: Tienen un plan propio de formación propio, detalla que se haría necesario un plan de formación

- Encuesta:
  - La formación del personal que trata datos personales.
  - La concienciación de mandos que supervisan el tratamiento de datos personales.
  - El asesoramiento del delegado de protección de datos.

b. SERVICIOS JURÍDICOS

- Reunión el 28 de junio
- Lugar: Sede de los Servicios Jurídicos
- Director del Servicio Jurídico: Ceferino Marrero Fariña
- Secretaria Laura Martín
- Objeto: Se comprobó que no tienen encargados de tratamiento y dentro de las funciones podemos señalar la fiscalización en cuanto a la adecuación jurídica del resto de órganos municipales así como la emisión de informes.

c. ATENCIÓN CIUDADANA Y DEMARCACIÓN TERRITORIAL

- Entrevista: María del Carmen Suárez Estévanez (Jefatura de Servicio de Atención Ciudadana)
- Lugar: Sede del Servicio: Oficinas Avenida Madrid (Parque de La Granja)
- Día: 19 de junio en la sede.

- Objeto: Se le trasladó el RAT el cual actualizó en los procedimientos que llevaba ese servicio, competencia de las diferentes unidades administrativas de este Servicio (Atención Ciudadana, Población y Demarcación Territorial y OMIC) y también de algunas como la cita previa o los quioscos, que le había comentado.

- Realizó una primera revisión lo que permite proceder a efectuar los cambios en la próxima actualización del RAT.

  Se ha evaluado la Sede en el Parque la Granja como muestra de referencia el área de Atención Ciudadana donde se ha comprobado que las deficiencias detectadas en materia de protección de datos y documentadas (informe del DPD de 19/10/2021) han sido subsanadas.

  En aquellos momentos existía formularios en papel (solicitudes en general) que no se adecuaban en cuanto a la información básica en materia de protección de datos.

  En este momento todos los formularios están adecuados en cuanto a la información de derechos de derechos para facilitar al interesado según lo preceptuado en los artículos 13 y 14, del RGPD, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

  La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos, extremos que se analizan en esta auditoría de forma independiente.

12. ANEXO III: GLOSARIO

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Alcance de la auditoría

Extensión y límites de una auditoría. El alcance de una auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el periodo de tiempo cubierto (adaptado de la UNE-EN-ISO 19011:2012, definición 3.14).

Auditor

Persona que lleva a cabo una auditoría (adaptado de la UNE-EN-ISO 19011:2012, definición 3.8).

El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

Auditor interno

Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

Auditor externo

Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

Comprobación

1) (DRAE) Verificar, confirmar la veracidad o exactitud de algo.

2) Dentro del contexto de esta guía, son verificaciones de la realización de controles, del establecimiento de medidas de seguridad, y de documentación de políticas, entre otros, dentro de los requerimientos establecidos por la norma de referencia en la auditoría.

Conformidad

Cumplimiento de un requisito (UNE-EN-ISO 19011:2012).

No conformidad mayor: ausencia o fallo en implantar y mantener uno o más requisitos del sistema de gestión de la calidad, o una situación que pudiera, basándose en evidencias o evaluaciones objetivas, crear una duda razonable sobre la calidad de lo que la organización está suministrando. Las entidades certificadoras no pueden conceder el certificado mientras exista una no conformidad mayor.

No conformidad menor (o solamente no conformidad): es una no conformidad detectada, que por sus características no llega a la gravedad de la anterior.

Control / Controles

1) (DRAE) Regulación, manual o automática, sobre un sistema.

2) Mecanismo o procedimiento que evita, previene, o detecta un riesgo.

3) En el contexto de una auditoría, estos pueden ser clasificados en preventivos, detectivos, y correctivos.

Criterio de auditoría

Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cuál se compara la evidencia de auditoría (UNE-ISO/IEC 19011:2012)

Cumplimiento

Ver “prueba de cumplimiento”.

Dictamen

(DRAE) Opinión y juicio que se forma o emite sobre algo.

Dictamen de auditoría

Ver “informe de auditoría”.

Efectividad / Eficacia

(DRAE) Capacidad de lograr el efecto que se desea o se espera.

Evidencia de auditoría

Registros, declaraciones de hechos o cualquier otra información que es pertinente para los hallazgos de auditoría y que es verificable. La evidencia de auditoría puede ser cualitativa o cuantitativa (UNE-EN-ISO 19011:2012).

Las evidencias consisten, principalmente, en las demostraciones y testimonios (documentales, automatizadas, etc.) de los resultados de la aplicación de los procedimientos de auditoría (pruebas). Éstas deben ser suficientes para soportar las conclusiones del auditor. Para ello deben acreditar determinadas situaciones o hechos objetivos en cuanto a los hechos a los que se refieren. La evaluación de estas evidencias corresponde al auditor para documentar su hallazgo.

Experto técnico

Persona que aporta experiencia o conocimientos técnicos específicos al equipo auditor. El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural. Un experto técnico no actúa como un auditor en el equipo auditor.

Guía

Persona designada por el auditado para asistir al equipo auditor.

Hallazgo de auditoría

Resultados de la evaluación de la evidencia de auditoría frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar conformidad o no conformidad. Pueden conducir a la

identificación de oportunidades de mejora o al registro de buenas prácticas. Si los requisitos de auditoría se seleccionan de entre los requisitos legales u otros requisitos, el hallazgo de auditoría se denomina “cumplimiento” o “no cumplimiento” (UNE-EN-ISO 19011:2012).

Informe de auditoría

Es el producto final de las tareas realizadas en una auditoría. En el informe el auditor comunica, a quien corresponda, los resultados de las tareas realizadas, con los resultados obtenidos.

Limitaciones al alcance

Son aquellos registros o documentos, o elementos del alcance de la auditoría, a los que, aunque previstos en las revisiones planificadas, para lograr los objetivos de la auditoría, el auditor no ha podido tener acceso, por distintas razones, y cuya restricción de acceso puede impactar en las conclusiones de la auditoría. Deben estar reflejadas en el informe de auditoría. Dentro del contexto de esta guía de auditoría, aunque podrían surgir en la definición del alcance, esta situación debería ser excepcional. Si las restricciones surgen en la fase inicial de delimitación del alcance, el auditor debe indicarlo, además de en el informe final, en la planificación. Asimismo, si surge en la fase inicial, debe indicarse el posible impacto en la realización de la auditoría, y la obtención de las conclusiones en relación al objetivo de la auditoría. Es conveniente que, en todos los casos, el auditor requiera que se comunique por escrito, la restricción de acceso a registros, documentos o elementos auditables, y justificados por el objetivo de la auditoría.

No conformidad

Incumplimiento de un requisito (UNE-EN-ISO 19011:2012).

Objetividad

Ver “opinión independiente y objetiva”.

Objetivo de la auditoría

1) Las metas específicas que debe lograr la auditoría.

2) En el contexto de esta guía, llegar con concluir si se cumple con lo requeridos por las normas de

referencia.

Observador

Persona que acompaña al equipo auditor pero que no audita. Un observador no es parte del equipo auditor, y no influye ni interfiere en la realización de la auditoría. Un observador puede designarse por el auditado, una autoridad reglamentaria u otra parte interesada que testifica la auditoría (adaptado de la UNE-EN-ISO 19011:2012, definición 3.11).

Observación

Ver “pruebas de auditoría”.

Opinión independiente y objetiva

1) Independiente: (DRAE) que no tiene dependencia, que no depende de otro.

2) Objetiva: (DRAE) Perteneciente o relativo al objeto en sí mismo, con independencia de la propia manera de pensar o de sentir.

3) La auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que está siendo auditada para permitir completar de manera objetiva la auditoría.

4) El auditor debe juzgar y opinar sobre los resultados de la auditoría, en función del objetivo y alcance de la misma, libre de toda parcialidad o sesgo que pueda afectar de forma negativa en los resultados de la auditoría, y que pueda conducir a una interpretación errónea de los hechos identificados.

Plan de auditoría

Descripción detallada (paso a paso) de los procedimientos de auditoría (documentación, pruebas, etc.) que se deben realizar durante la ejecución del trabajo de auditoría para alcanzar el objetivo de la misma. En el plan de la auditoría también se incluye la asignación de tareas, fechas de realización de las tareas, y recursos necesarios para desarrollar la auditoría.

Principios de segregación de funciones

1) (DRAE) Principio: Norma o idea fundamental que rige el pensamiento o la conducta.

2) La separación o segregación de funciones es una regla básica en los controles: evitar que una persona pueda dominar todo un proceso, de tal forma que errores u omisiones, o incumplimientos de controles no puedan ser identificados. Por lo tanto, el auditor debe identificar donde no se cumple con esta norma fundamental, para evaluar el impacto en la efectividad de los controles.

Procedimientos de auditoría

Comprenden el proceso de auditoría: habitualmente aluden a los procesos relacionados con la definición de las pruebas, su planificación y su ejecución. Las pruebas de auditoría pueden ser de cumplimiento o sustantivas, según su objetivo. Asi mismo, las técnicas de auditoría utilizadas en cualquier tipo de las pruebas mencionadas anteriormente pueden ser: observación de la realización de tareas, revisión de documentación, entrevistas, realización de pruebas técnicas, revisión de evidencias del cumplimiento de controles, etc. Entre estas últimas se pueden incluir los criterios para la selección de muestras de elementos a revisar en determinadas pruebas.

Pruebas de auditoría

1) Permiten obtener evidencia y verificar la consistencia de los controles existentes y también medir el riesgo por deficiencia de estos o por su ausencia.

2) Se diseñan y planifican para asegurar que los controles se diseñan adecuadamente y funcionan de forma efectiva y continuada.

Pruebas de cumplimiento

Permiten determinar si un control se está realizando de la forma prevista en las normas y políticas de seguridad establecidas por el organismo responsable del SI. Su objetivo principal es determinar si el control se realiza y si sus resultados son efectivos.

Pruebas sustantivas

Permiten confirmar la exactitud de determinadas situaciones o hechos, pero fundamentalmente permiten sustanciar el impacto y alcance de una deficiencia, o incidencia de seguridad (en el contexto de esta guía), con proyección sobre la integridad de determinada información o de un proceso. Ejemplo: en la revisión de un inventario de copias de respaldo, una prueba de cumplimiento puede determinar si los controles previstos se están cumpliendo o no, pero con una prueba sustantiva, se podría determinar cuántos, y /o cuáles elementos no están incluidos en el

inventario.

Recomendaciones

Pueden ser parte del informe de auditoría, donde además de incluir las conclusiones de las tareas de auditoría realizadas, e identificar las deficiencias observadas, se pueden incluir sugerencias concretas para la solución de los fallos identificados.

Requisito

1) (DRAE) Circunstancia o condición necesaria para algo.

2) Dentro del contexto de esta guía, son las condiciones, en ocasiones mínimas, a cumplir por los auditores, o en cuanto a la aplicación de una norma.

3) En auditoría se suele indicar que existen "requisitos" o mandatos mínimos que debe cumplir el proceso de auditoría, tales como establecer el alcance y objetivo de la auditoría, realizar un programa de auditoría, y las pruebas relacionadas, así como la emisión de un informe, entre otros.

Responsabilidad

1) Obligación o deber de realizar alguna acción.

2) Dentro del contexto de una auditoría, se deben establecer, por ejemplo, responsabilidades mínimas para la función de auditoría interna, responsabilidades del cumplimiento de la metodología de auditoría, y sus requisitos mínimos.

3) El auditor es responsable por la opinión y las conclusiones vertidas en el informe de auditoría.

Satisfacción de auditoría

1) (DRAE) Satisfacer: Cumplir, llenar ciertos requisitos o exigencias.

2) Dentro del contexto de la auditoría, se refiere a que el programa o plan de auditoría, debe cumplir con los objetivos de auditoría, y las tareas realizadas con éste.

Selección de muestras

Se pueden aplicar criterios de muestreo estadístico o no, para seleccionar elementos a revisar en una determinada prueba. La calidad de la muestra y de la selección de los elementos de la muestra puede facilitar el análisis de los resultados de una prueba y también la sustentación de una conclusión de auditoría. Se utiliza fundamentalmente cuando existe una población homogénea de elementos a seleccionar, por ejemplo: cuentas de usuarios.

Suficiencia de las evidencias

Las evidencias que soportan una conclusión deben ser suficientes (bastantes), y relevantes (significativos), para soportar las conclusiones y opinión del auditor.

Supervisión

1) (DRAE) Ejercer la inspección superior en trabajos realizados por otros.

2) Las tareas del equipo de auditoría deben ser supervisadas por el Jefe del equipo de auditoría para asegurar que se ha cumplido con el objetivo de la auditoría dentro del alcance previsto.

Verificación

Cualquiera de las acciones de auditoría encaminadas a la comprobación el cotejo, el contraste y el examen de evidencias, registros y documentos.

Firmado por NOMBRE YUSTE BARRANQUERO ANGEL - NIF ***5744** el día 25/08/2023 con un certificado emitido por ACA CA1, EstudNET: Delegado de Protección de Datos del Ayuntamiento de Santa Cruz de Tenerife. Abogado Colegiado