

CERTIFICADO DEL ACUERDO ADOPTADO EN SESIÓN ORDINARIA DE LA JUNTA DE GOBIERNO DE LA EXCMA. DIPUTACIÓN PROVINCIAL DE CASTELLÓN, CELEBRADA EN PRIMERA CONVOCATORIA, EL VEINTINUEVE DE SEPTIEMBRE DEL DOS MIL VEINTISÉIS.

8.- PROPOSICIÓN DE APROBACIÓN DEL DOCUMENTO SOBRE FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO.

Visto que se ha elaborado el documento denominado FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO, a los efectos de dar cumplimiento a los requerimientos efectuados para la obtención de la recertificación de cumplimiento del Esquema Nacional de Seguridad.

Considerando lo dispuesto en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos):

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

Montserrat Pardo Comina (1 de 2)
Oficial Mayor
Firma: 30/09/2026
HASH: 2b3c2993678e74c27e1eed8981b3adb

Marta Barrachina Mateu (2 de 2)
PRESIDENTE
Firma: 30/09/2026
HASH: f9631763c1f1ab8b5731b3b1c6a2db8b



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. [...]

Considerando lo establecido en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Considerando lo dispuesto en la *Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones* de junio de 2025 y otras Guías publicadas por la Agencia Española de Protección de Datos u otras autoridades europeas en materia de privacidad.

La Junta de Gobierno Local, por unanimidad, adopta el siguiente acuerdo:

Primero. Aprobar el documento **FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO.**



Segundo. Publicar el documento en el Boletín Oficial de la Provincia y en el portal de transparencia de la Diputación.

Tercero.- Trasladar el documento al departamento de recursos humanos para su inclusión en la Relación de Puestos de Trabajo

Documento firmado electrónicamente



FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO

EXCMA. DIPUTACIÓN PROVINCIAL DE CASTELLÓN



HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Cambios	Revisado	Aprobado
1.0	25/11/2021	v.1	AYZ	
2.0	01/12/2021	v.2	MBB	
3.0	18/01/2022	v.3	MBB	
4.0	19/02/2024	V.4	ASS	
5.0	29/07/2024	V.5	ASS	
6.0	17/09/2024	V.6	ASS	Acuerdo JGL 17/9/2024
7.0	29/10/2026	V.7	MPC	Acuerdo JGL 29/09/2026



ÍNDICE DE CONTENIDOS

1 OBJETO.....

2 ÁMBITO DE APLICACIÓN.....

3 VIGENCIA.....

4 MARCO NORMATIVO Y ACRÓNIMOS.....

5 ACTORES Y RESPONSABLES.....

6 PROPUESTA DE ELEMENTOS BÁSICOS DE LAS FUNCIONES Y OBLIGACIONES QUE ANUNCIAR EN E
DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO.....

6.1 Puesto 1245 - Jefe/a del Servicio de Informática:.....

6.2 Puesto 1368 - Jefe/a Sección de Sistemas:.....

6.3 Cada uno de los responsables de unidades funcionales siguientes afectadas por el ENS en
términos en los que lo establece el decreto que lo regula:.....

6.4 Puesto 1044 - Jefe/a Servicio Ingeniería Interna.....

6.5 Puestos actuales: 985, 1065, 1340, 1399, 1438, 1460 [Todos los Técnicos de Sistemas] -
Coordinador de técnicos de sistemas:.....

6.6 Puesto 1323 - Jefe/a del Servicio Recursos Humanos:.....

6.7 Puesto 1 - Secretaría General:.....

6.8 Puesto 1434 - Técnico medio archivo:.....

6.9 Puesto 1043 - Jefe/a del Área técnica:.....

6.10 Puesto 1308 - Jefe/a del Servicio de Administración e Innovación Pública.....

6.11 Puesto 1060 - Jefe/a de Sección de Informática Municipal.....

6.12 Miembros del Comité de Crisis: Presidente y Diputado Informática (sin RPT), puestos de
trabajo 1, 1308,1245, 1323, 1368.....

6.13 Equipo de recuperación: Puestos de trabajo: 1044, 1245, 1368, 1323, y 930.....

6.14 Resto del personal:.....

7 ANEXO "A": RELACIÓN DE RESPONSABLES DE SERVICIO.....



1 OBJETO

El objeto del presente documento es la definición de una propuesta de funciones y obligaciones en materia de privacidad y seguridad de la información que incluir en detalle en la relación de puestos de trabajo (en adelante, RPT) de la Excm. Diputación Provincial de Castellón (en adelante, Diputación o Dipcas). En este sentido, se busca proponer un marco de referencia que establezca las responsabilidades generales en la gestión de la privacidad y seguridad de los sistemas de información de la propia Diputación del ámbito subjetivo de aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), así como del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de seguridad (ENS) desarrollando las figuras o roles más significativos que asuman dichas responsabilidades. Supone también la aplicación de la normativa de mayor impacto en materia de seguridad:

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1772 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Si bien la anterior Directiva fue traspuesta a nuestro ordenamiento jurídico por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información desarrollado en el Real Decreto 43/2021, de 26 de enero, la actual, a fecha de redacción del informe, está pendiente de su trasposición. Además, se deberá tener en cuenta, en función de los sectores involucrados, los Reglamentos de Ejecución de la Directiva NIS2 dictados por la Comisión Europea. En función de la consideración de las entidades dentro del alcance de la Directiva NIS2 como esenciales o importantes deberán adoptar diferentes medidas, incluye aquellas para determinados sectores, por ejemplo, en la comunicación de incidentes de seguridad.
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE, actualmente pendiente de transposición. La anterior Directiva se ha traspuesto por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 4 de 56

protección de las infraestructuras críticas, desarrollada por el Real Decreto 704/2011 de 20 de mayo.

- Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial, que será aplicable con carácter general el 2 de agosto de 2024. Incluye la necesidad de atender a los riesgos en ciberseguridad en el desarrollo y despliegue de un sistema de inteligencia artificial (IA) de alto riesgo.

Se aplica en el desarrollo del presente documento las directrices fijadas en la Guía de Seguridad de las TIC CCN-STIC 801 “Esquema Nacional de Seguridad. Responsabilidades y funciones” de junio de 2025¹

Con la implantación del presente documento se atiende a lo establecido en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos):

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. [...]*

¹. Link de acceso a la guía: <https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/501-ccn-801-responsabilidades-y-funciones-en-el-ens/file.html>



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 5 de 56

Así como, con el cumplimiento de lo establecido en la Disposición adicional primera de la Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales:

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en el tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar los tratamientos de datos personales las medidas de seguridad que correspondan de acuerdo con las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión o encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Asimismo, para la elaboración del presente documento se han tomado como base directrices señaladas en la normativa anteriormente mencionada, la *Guía de Seguridad de la Información CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones*, y las Guías publicadas por la Agencia Española de Protección de Datos u otras autoridades europeas en materia de privacidad.

A este respecto, la Diputación ha establecido y aprobado su propia Organización de Seguridad de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que está recogida en la Política de Seguridad de la Información y, en la normativa interna sobre Protección de Datos. Es por ello que, derivado de esta Organización de Seguridad resulta necesario regular las funciones y obligaciones que deben asumir distintos empleados de la organización en el desarrollo de sus roles y responsabilidades. Estas funciones y obligaciones vienen reguladas en la

continuación.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 6 de 56

2 ÁMBITO DE APLICACIÓN

Esta normativa es de aplicación a todo al ámbito de gestión de la seguridad de los sistemas de información de la Diputación. Concretamente, resulta aplicable a la redacción y elaboración de la Relación de Puestos de Trabajo (RPT). Bien es conocido por todos, que la RPT es un instrumento técnico sobre el que las Administraciones Públicas diseñan su estructura organizativa personal para adecuarla a las necesidades del servicio público (tanto internamente como hacia la ciudadanía). Es por tanto el eje sobre el que pivota la gestión de recursos humanos. La eficacia y gran diferencia de la RPT respecto a un organigrama radica en su objetividad y tiene en consideración a la persona que ocupa el puesto de trabajo sino al puesto en sí.

Atendiendo estos aspectos, y de acuerdo con lo comentado anteriormente, a través del presente documento se establecen aquellas funciones y obligaciones a incluir en el RPT determinados roles establecidos por la normativa de seguridad y privacidad y que obligatoriamente deben estar designados en la propia Diputación.

3 VIGENCIA

La presente normativa entrará en vigor a partir de su aprobación inicial por la Oficina Provincial de Protección de Datos y Seguridad de la Diputación de Castellón y estará vigente hasta su sustitución por otra normativa del mismo alcance o similar.



4 MARCO NORMATIVO Y ACRÓNIMOS

Acrónimo	Concepto
RGPD	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).
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales
LBRL	Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
ET	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.
EBEP	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.
ENS	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
TC	Tribunal Constitucional.
TS	Tribunal Supremo.
SAN	Sentencia de la Audiencia Nacional.
RPT	Relación de Puestos de Trabajo



5 ACTORES Y RESPONSABLES

La gestión de la seguridad de los sistemas de información en las organizaciones *-definición, implantación y mantenimiento-* exige establecer una Organización de la Seguridad. En este caso, la Diputación ha determinado con precisión los diferentes actores que la conforman, funciones y responsabilidades, así como la implantación de una estructura que las soporte.

Si bien en la anterior regulación, en el artículo 10 del ENS se definían las funciones (las negritas son nuestras):

Artículo 10. La seguridad como función diferenciada

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

*El **responsable de la información** determinará los requisitos de la información tratada; el **responsable del servicio** determinará los requisitos de los servicios prestados; y el **responsable de la seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.*

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Imagen 1. Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad. Responsabilidades y funciones.

En fecha 3 de mayo de 2022, se aprobó la nueva regulación del ENS, mediante promulgación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, publicado en el BOE número 106, de fecha 4 de mayo de 2022. Estableciéndose una nueva diferenciación de responsabilidades en materia de seguridad ampliando a cuatro a las figuras que deben designarse en la organización frente a las anteriores.

Es en el actual artículo 11 del ENS, en el que se definen las distintas responsabilidades (las negritas son nuestras):

“Artículo 11. Diferenciación de responsabilidades.

*1. En los sistemas de información se diferenciará el **responsable de la información**, el **responsable del servicio**, el **responsable de la seguridad** y el **responsable del sistema***



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 9 de 56

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada con la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.”

Además de las tres figuras mencionadas en el art. 10 del anterior ENS -Responsable de la Información, Responsable del Servicio y Responsable de la Seguridad-, cuyas competencias y responsabilidades pueden ser indelegables², las organizaciones suelen disponer también de un denominado Responsable del Sistema (de información³), y cuya responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata⁴ (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados⁵.

La nueva regulación del ENS (Real Decreto 311/2021), ya establece la obligatoriedad de contar con cuatro figuras diferenciadas:

1. Responsable de la información
2. Responsable de los servicios
3. Responsable de la seguridad
4. Responsable del sistema

Por otro lado, cuando la entidad está tratando datos de carácter personal, se hace necesario contemplar las figuras de Responsable del Tratamiento, Delegado de Protección de Datos y, en su caso, Encargado del Tratamiento, con las funciones definidas en el RGPD y en la LOPDGDD.

² Parece claro que, mientras que las responsabilidades del Responsable de la Información y Responsable del Servicio son siempre indelegables, no ocurre lo mismo con las correspondientes al Responsable de la Seguridad, que podrían ser asumidas, como competencias propias, por las Diputaciones Provinciales, en el caso de las entidades locales. Por tanto, habrá que sostener, con carácter general, que todas las responsabilidades mencionadas son indelegables en tanto no exista una habilitación legal que permita la delegación.

³ El ENS define “sistema de información” como: “Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir”. (Anexo IV. Glosario).

⁴ Es “autor mediato” quien causa un resultado sirviéndose de otra persona como medio o instrumento para realizar la ejecución. El autor no realiza directa y personalmente el delito, se sirve de otra persona consciente de la trascendencia penal que tiene su acto.

⁵ Cuando se utilizan servicios externalizados (mediante contrato, convenio, encomienda, etc.), es frecuente que la entidad prestadora (pública o privada) cuente asimismo con un Responsable de la Seguridad al que será exigible el mantenimiento de la seguridad de los sistemas de información concernidos, sin que ello suponga merma de la responsabilidad exigible al Responsable de la Seguridad de la entidad prestataria de los servicios.



El cuadro⁶ siguiente muestra las peculiaridades de las figuras más significativas en materia de seguridad de la información y privacidad, atendiendo a la norma legal de la que traen causa

Entidad	Ubicación legal	Funciones, Características o Referencias
Dirección de la Entidad del Sector Público	La derivada de la aplicación de la Ley 40/2015 / otra normativa sectorial considerada (Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local, ...	Entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico. Es el máximo responsable de la implantación del ENS.
Responsable de la Información	ENS, art. 11 y 13	Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de niveles de seguridad de la información constituye asimismo una actividad indelegable.
	ENS, art. 40 y 41	La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y

⁶ Cuadro extraído de la *Guía de Seguridad de las TIC CCN-STIC 801: Esquema Nacional de Seguridad, Responsabilidades y funciones*



Entidad	Ubicación legal	Funciones, Características o Referencias
Responsable del Servicio		derechos de los ciudadanos. Efectúa las valoraciones a las que se refiere el artículo 40 del ENS (categorías de seguridad), así como, en caso, su posterior modificación.
	Op.exp.7	Recibe información sobre los incidentes y de actuaciones realizadas para su resolución.
	Mp. info.2	Determinación de los criterios para asignar y modificar cada información el nivel de seguridad requerido, y su responsable de su documentación y aprobación formal.
	ENS, art. 11 y 13	Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de niveles de seguridad de los servicios constituye asimismo una actividad indelegable.
	ENS, art. 36	Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de correspondientes procedimientos de control.
Responsable de	ENS, art. 40 y 41	Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de ciudadanos. Efectuará las valoraciones a las que se refiere el artículo 40 (categorías de seguridad), así como, en su caso, posterior modificación.
	Op. exp.7. R2.3	Será informado de los incidentes y de las actuaciones llevadas a cabo para su resolución
	ENS, art. 11	Determina las decisiones de seguridad pertinentes para



Entidad	Ubicación legal	Funciones, Características o Referencias
la Seguridad	y 13	satisfacer los requisitos establecidos por responsables de la información y de los servicios supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos reportará sobre estas cuestiones. Será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos requiera que ambas funciones recaigan en la misma persona o en distintas personas con relación jerárquica, se aplicarán medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en artículo 11 del ENS. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
	ENS, art. 13.5	El Responsable de la Seguridad del servicio externalizado realizará funciones de Punto de Contacto (POC), o bien las delegará en una persona que forme parte de su área o tendrá comunicación directa con la misma. EL POC debe contar con el apoyo de la dirección de la entidad. Tiene como funciones la canalización y supervisión tanto del cumplimiento de los requisitos de seguridad como del servicio que presta o solución suministrada como comunicaciones relativas a la seguridad de la información y la gestión de incidentes. En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando



Entidad	Ubicación legal	Funciones, Características o Referencias
		responsabilidad inmediata pueda corresponder (contrato, convenio, encomienda, etc.) a la organizac prestataria del servicio.
	ENS, arts. 28	Formalización y aprobación de las medic seleccionadas del Anexo II en la Declaración de Aplicabilidad, incluyendo las medidas compensatorias complementarias de vigilancia y su correspondencia c las medidas del Anexo II antes citado. Las medidas del Anexo II del ENS, así como aquel otras necesarias para garantizar el adecuado tratamie de datos personales podrán ser ampliadas por causa la concurrencia indicada o del prudente arbitrio el Responsable de la Seguridad del sistema, habida cue del estado de la tecnología, la naturaleza de los servic prestados y la información manejada, y los riesgos a q están expuestos. La relación de medidas seleccionadas del Anexo II formalizará en un documento denominado Declarac de Aplicabilidad, firmado por el Responsable de Seguridad. Las medidas de seguridad referenciadas en el Anexo podrán ser reemplazadas por otras compensator siempre y cuando se justifique documentalmente c protegen igual o mejor el riesgo sobre los activos (Ane I) y se satisfacen los principios básicos y los requisi mínimos previstos en los capítulos II y III del r decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensator implantadas y las medidas del Anexo II que compens y el conjunto será objeto de la aprobación formal l parte del responsable de la seguridad.
	ENS, art. 31 y Anexo III	Análisis de los informes de Auditoria de prime segunda o tercera parte que se refieran a los sisterr



Entidad	Ubicación legal	Funciones, Características o Referencias
		de su ámbito competencial, y presentación de conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.
	ENS, art. 41	La determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio
	Op.exp.5	Aprobación explícita de los cambios que impliquen riesgo de nivel ALTO con carácter previo a su implantación
	Mp.info.1	Cuando el sistema trate datos personales, el Responsable de la Seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios para implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y con la evaluación de impacto en la protección de datos, si se lleva a cabo
	Anexo III	Análisis de los informes de auditoría de primera, segunda o tercera parte, notificando las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
Responsable del Sistema (de información)	ENS, artículo 11 y 13	Será distinto del Responsable de la Seguridad debiendo existir dependencia jerárquica entre ambos. Cuando, con carácter excepcional y justificado, ambas figuras recaigan en la misma persona se implementarán medidas compensatorias como señala el art. 11 del ENS. Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo



Entidad	Ubicación legal	Funciones, Características o Referencias
		responsabilidad Estas funciones las podrá realizar mediante recursos propios de la entidad o contratados
	La derivada de la aplicación de la Ley 40/2015	Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o es compartimentada entre una responsabilidad mediata (la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.
	ENS, art. 31	Adopta las medidas correctoras adecuadas derivadas de los informes de Auditoría de primera, segunda o tercera parte. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a la eventual gravedad de las deficiencias encontradas, podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la explotación del sistema, hasta su adecuada subsanación o mitigación
	Anexo III	Adopción de medidas correctoras de las auditorías de primera, segunda o tercera parte, según conclusiones trasladadas por el Responsable de Seguridad
Administradores del sistema/ de la seguridad	ENS, Art.13	Actúan como delegados del Responsable del Sistema de la Seguridad
	Op.acc.1.r1.1	
	Op.acc.1.r1.3	Mantiene la lista actualizada de usuarios autorizados
Responsable del Tratamiento (Protección de Datos)	Op.exp.3.r2.1	Configuración del sistema operativo, aplicaciones tanto de estaciones y servidores como electrónica de red del sistema.
	RGPD, art. 4.7) y LOPDGDD, Título V	La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o



Entidad	Ubicación legal	Funciones, Características o Referencias
		criterios específicos para su nombramiento por parte de la Unión o de los Estados miembros.
Encargado del Tratamiento (Protección de Datos)	RGPD, art. 4.8) y LOPDGDD, Título V	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta propia o ajena. Responsable del Tratamiento.
Delegado de Protección de Datos	RGPD, art. 39 y LOPDGDD, arts. 34 a 37	El Delegado de Protección de Datos tendrá como mínimo las siguientes funciones: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de datos personales de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos personales; d) supervisar su aplicación de conformidad con el artículo 35; e) cooperar con la autoridad de control; f) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas en su caso, sobre cualquier otro asunto.
	ENS, art. 3	Además de las funciones que le atribuye la normativa especial (RGPD, LOPDGDD) y los criterios de las autoridades de control (Comité Europeo de Protección de Datos).



Entidad	Ubicación legal	Funciones, Características o Referencias
		de Datos, Agencia Española de Protección de Datos. el ENS indica que asesora al Responsable o Encargado del Tratamiento en la realización de análisis de riesgo evaluaciones de impacto.
	Mp.info.1.	El Responsable de la Seguridad contará con la opinión del Delegado de Protección de Datos en relación con requisitos de la normativa de protección de datos en sistema de información cuando se traten datos personales

Atendiendo a lo señalado en los epígrafes precedentes, podemos representar la Estructura de Seguridad (de la Información y de Protección de Datos) según se muestra en la siguiente:

ENTIDAD/RESPONSABLE TRATAMIENTO			PRESTADOR DE SERVICIOS/ENCARGADO DEL TRATAMIENTO
Director entidad: Presidencia de la diputación de Castellón			
Responsable de la información	Delegado de protección de datos		Delegado de protección de datos
Responsable del servicio	Responsable de seguridad		Responsable de la seguridad (POC)
Responsable del sistema			Responsable del sistema

Esquema de la seguridad de la información y la protección de datos

6 PROPUESTA DE ELEMENTOS BÁSICOS DE LAS FUNCIONES Y OBLIGACIONES QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO

Mediante decreto número 2025/ (se acompaña como anexo), se adoptó el siguiente acuerdo



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 18 de 56

“PRIMERO.- Designar formalmente a las personas que aparecen en los Anexos de la presente Resolución para que desempeñen cada una de las responsabilidades en los términos de Seguridad que exige el ENS.

SEGUNDO.- Publicar la presente resolución en el Boletín Oficial de la Provincia, quedando integrada la misma en la Política de Seguridad de la Diputación.

ANEXO I.- FUNCIONES Y RESPONSABILIDADES ASIGNADAS EN RELACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD.

1. Responsable de la Información: Presidente/a
2. Responsable de la Seguridad: El/La Oficial Mayor
3. Responsable del Sistema: Jefe/a de Sección de Sistemas.
4. Administrador de Seguridad del Sistema: Técnico de sistemas.
5. Responsables de los Servicios / Información de su departamento que a continuación se relacionan:

- Director de Buen Gobierno y Administración
- Jefe del Servicio Jurídico
- Jefe Servicio Bienestar Social e Igualdad
- Jefe Servicio Recursos Humanos
- Responsable de Formación
- Responsable de Prevención y Riesgos Laborales
- Jefe Servicio Cooperación Municipal
- Jefe Servicio de Cultura, Restauración, Deportes y Juventud
- Jefe Servicio de Contratación y Central de Compras
- Jefe Servicio de Patrimonio y Expropiaciones
- Jefe Servicio de Administración e Innovación Pública
- Jefe Servicio de Promoción Económica y Relaciones Internacionales
- Tesorero
- Jefe Servicio de Informática
- Jefe del Área Técnica
- Jefe Servicio de Infraestructura
- Jefe Servicio Oficina Técnica



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 19 de 56

- *Jefe Servicio Carreteras y Obras*
- *Jefe Servicio Ingeniería Interna*
- *Responsable Archivo*
- *Responsable Publicaciones*
- *Interventor*
- *Responsable del Servicio Gráfico y Digital*
- *Jefe de Sección de Informática Municipal*
- *Jefe Servicio Gestión Tributaria y Recaudación*
- *Director Técnico y Coordinador de Peñeta Roja*
- *Responsable Conservación Preventiva y Restauración Colecciones Arte*
- *Responsable del Parque Móvil*

ANEXO II.- COMPOSICIÓN DEL COMITÉ DE SEGURIDAD

- *Presidente: Presidenta de la Corporación o en quien delegue*
- *Responsable de Seguridad/Secretaria: El/La Oficial Mayor (Secretaría General)*
- *Vocales.*
 - 1.1. *Responsable del Sistema: Jefe/a de Sección de Sistemas*
 - 1.2. *Responsable Informática: Jefe del Servicio de Informática*
 - 1.3. *Delegado de protección de datos*
 - 1.4. *Responsable de servicios: Director de Buen Gobierno*
 - 1.5. *Responsable RRHH y Formación*
 - 1.6. *Responsable Administración e Innovación pública*
 - 1.7. *Responsable Informática municipal*

Este decreto, debe tener su reflejo en la relación de puestos de trabajo de la Diputación de Castellón, con su correspondiente valoración. A continuación, se detalla una propuesta de elementos básicos de las funciones y obligaciones que anunciar en detalle en la RPT de la Diputación. Se ha elaborado esta propuesta de funciones y obligaciones atendiendo a distintos puestos de trabajo de la organización que tiene asignado un rol o responsabilidad relevante en materia de privacidad y seguridad. De conformidad con el ENS, el responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos, no obstante, si debido al tamaño y carencia de recursos de la organización no es posible, deberán aplicarse las medidas compensatorias convenientes para garantizar la diferenciación de responsabilidades y ausencia de conflicto de interés.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026 Página 20 de 56

Son los siguientes roles:

6.1 El **responsable del servicio** determinará los requisitos de los servicios prestados. La función principal es la de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Y los criterios de valoración estarán alineados y respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

Los roles del responsable de la información y el responsable del servicio pueden concurrir en la misma persona física que actúe en su representación.

Se establece como responsable del servicio de la Diputación de Castellón, al Director General de Buen Gobierno y Administración (puesto de trabajo número 1475 de la Relación de Puestos de Trabajo provincial)

6.2 El **responsable de la información** determinará los requisitos de la información tratada. La función principal, es la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información. La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Y los criterios de valoración estarán alineados y respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

Los roles del responsable de la información y el responsable del servicio pueden concurrir en la misma persona física que actúe en su representación.

Se establece como responsable de la información de la Diputación de Castellón, a la persona que ostente la presidencia de la Diputación de Castellón

6.3 El **responsable de la seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos, y reportará sobre estas cuestiones al Comité de Seguridad de la Información.

Las funciones esenciales del Responsable de la Seguridad, son:



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 21 de 56

- a. Determinar las medias de seguridad aplicables, en función de las valoraciones hechas los Responsables de la Información y los Servicios.
- b. Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos Responsable de la Información y del Servicio
- c. Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
- d. Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
- e. Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información los procedimientos, normativas e instrucciones en aplicación del ENS.
- f. Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y su caso, del Delegado de Protección de Datos y supervisar su despliegue.
- g. Promover la formación y concienciación en materia de seguridad de la información dentro su ámbito de responsabilidad.
- h. En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CEN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de la información ampliada de forma paulatina.

Se podrán designar **Responsables de Seguridad Delegados**. La propuesta de designación corresponderá al Responsable de la Seguridad, que delegará funciones, no responsabilidades. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito competencial, de todas aquellas funciones delegadas por el Responsable de la Seguridad. Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 22 de 56

Se establece como responsable de la seguridad de la Diputación de Castellón, a la of mayor (puesto de trabajo número 751 de la Relación de Puestos de Trabajo provincial)

Siendo el responsable de seguridad designado un perfil jurídico, este contará con asesoramiento del Jefe del departamento de Informática y en su caso, de asesorías externas para poder desarrollar sus funciones.

6.4 El **responsable del sistema**, por sí o a través de recursos propios o contratados encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de supervisión de la operación diaria del mismo, pudiendo delegar en administradores operadores bajo su responsabilidad.

El Responsable del Sistema tiene entre otras funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Adopción de las medidas correctoras derivadas de las auditorías de seguridad
- En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y servicio y, en caso de afectación a datos personales al Delegado de Protección de Datos afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos

Se podrán designar cuantos **Responsables del Sistema Delegados** considere necesarios propuesta de designación corresponde al Responsable del Sistema, que delega funciones de responsabilidad. Los Responsables del Sistema Delegados se harán cargo, en su ámbito de competencia, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 23 de 56

Se establece como responsable del sistema de la Diputación de Castellón, al Jefe de Sección de Sistemas (puesto de trabajo número 1368 de la Relación de Puestos de Trabajo provincial)

6.5 Administrador de Seguridad (ASEG). el ENS prevé la figura del Administrador de Seguridad (ASEG) como recurso para aquellas organizaciones en las que el Responsable de Seguridad (RSEG) no tenga todos los conocimientos técnicos necesarios y pueda apoyarse en él. En ese caso, el RSEG tendrá un desempeño más estratégico mientras que el ASEG tendrá más operativo. Un ejemplo sería una EE.LL. que nombrase al Secretario de Ayuntamiento como RSEG, el cual deberá apoyarse en un ASEG interno, o externo contratado en modalidad de prestación de servicios.

Son funciones del Administrador dependiente del Responsable de la Seguridad:

- Comprobar que los controles de seguridad establecidos son adecuadamente observados
- Comprobar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Comprobar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 24 de 56

Se podrán designar administradores delegados. Los administradores delegados serán responsables, en su ámbito competencial, de aquellas acciones que delegue el Administrador relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información. El administrador delegado será designado a solicitud del Administrador, del que dependerá funcionalmente.

Se establece como administrador de seguridad de la Diputación de Castellón, al Jefe del Área de Informática (puesto de trabajo número 1245 de la Relación de Puestos de Trabajo provincial)

6.6 Administrador de Sistemas (ASIS):

Se establecen como administrador de sistemas de la Diputación de Castellón, a todos los técnicos de sistemas (Puestos actuales: 985, 1065, 1340, 1399, 1438, 1460 [Todos los Técnicos de Sistemas] – Coordinador de técnicos de sistemas de la Relación de Puestos de Trabajo provincial)

En tanto **Administrador de Sistemas**, le corresponden las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- La gestión, configuración y actualización, en su caso, del hardware y software en el que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras y asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente del Sistema de Información garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad de cualquier anomalía, compromiso



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 25 de 56

vulnerabilidad relacionada con la seguridad.

- Monitorizar el estado de la seguridad del sistema.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con equipos que por razón de su cargo o función establece internamente el Plan Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

Debe estar formado en formación avanzada de gestión de incidentes de ciberseguridad según el programa Angeles CCN-CERT.

6.7. Responsable de la seguridad física.

Se establece como responsable de seguridad física, al titular del Puesto 1044 – Jefe/a Servicio de Ingeniería Interna de la Relación de puestos de trabajo de la diputación

De forma general, el Jefe/a del Servicio de Ingeniería Interna por ostentar más de una responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 26 de 56

obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Seguridad Física**, le corresponden las siguientes funciones:

- Implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información.
- Informar a éste de su grado de implantación, eficacia e incidentes.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con equipos que por razón de su cargo o función establece internamente el Plan Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Como **miembro del Equipo de recuperación**, le corresponden las siguientes funciones:

- Participar en las actividades de evaluación y recuperación de los procesos de negocio realizando una evaluación de daños ocasionados por la incidencia en sus respectivas áreas de responsabilidad y adoptando todas aquellas medidas que resulten necesarias para la resolución de la incidencia y el restablecimiento de los procesos de negocio.
- En la gestión de la continuidad del negocio el equipo de recuperación deberá:
 - o Evaluar la repercusión y efectos de la incidencia sobre los recursos de su área de responsabilidad, determinando la posibilidad de recuperación de los mismos.
 - o Iniciar los procedimientos de recuperación de los procesos de negocio de los que son responsables.
 - o Contactar tan pronto como sea posible con las personas que de ellos dependen y coordinar sus acciones para la recuperación de los procesos de negocio que caen bajo su responsabilidad.
 - o Establecer contacto con los terceros (proveedores, socios, ...) con los que habitualmente mantienen relaciones a fin de coordinarse con ellos en la medida en que sea necesario.
 - o Supervisar y coordinar la recuperación de los recursos (infraestructura, hardware, software, información, ...) que hubieran resultado afectados por la incidencia en las Oficinas Centrales.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 27 de 56

- o Adoptar todas aquellas medidas adicionales que resulten necesarias para la reanudación de los procesos críticos de negocio, ya sea en las propias oficinas o en las oficinas de contingencia que les fuera comunicado.
- o Gestionar y coordinar, si procede, el traslado a los centros de contingencia de las personas y los activos de información que fueran necesarios.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

6.8. Responsables de los servicios e información: Cada uno de los responsables de las unidades funcionales siguientes afectadas por el ENS en los términos en los que establece el decreto que lo regula:

- Director de Buen Gobierno y Administración
- Jefe del Servicio Jurídico
- Jefe Servicio Bienestar Social e Igualdad
- Jefe Servicio Recursos Humanos
- Responsable de Formación
- Responsable de Prevención y Riesgos Laborales
- Jefe Servicio Cooperación Municipal
- Jefe Servicio de Cultura, Restauración, Deportes y Juventud
- Jefe Servicio de Contratación y Central de Compras
- Jefe Servicio de Patrimonio y Expropiaciones
- Jefe Servicio de Administración e Innovación Pública
- Jefe Servicio de Promoción Económica y Relaciones Internacionales
- Tesorero
- Jefe Servicio de Informática
- Jefe del Área Técnica
- Jefe Servicio de Infraestructura
- Jefe Servicio Oficina Técnica
- Jefe Servicio Carreteras y Obras
- Jefe Servicio Ingeniería Interna
- Responsable Archivo
- Responsable Publicaciones
- Interventor
- Responsable del Servicio Gráfico y Digital
- Jefe de Sección de Informática Municipal



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 28 de 56

- Jefe Servicio Gestión Tributaria y Recaudación
- Director Técnico y Coordinador de Peñeta Roja
- Responsable Conservación Preventiva y Restauración Colecciones Arte
- Responsable del Parque Móvil

En tanto **Responsable del Servicio y de la información** le corresponden las siguientes funciones, contando con los criterios del Responsable de Seguridad y del Responsable Sistema:

- Establecer los requisitos de los servicios en materia de seguridad. En el marco del E equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinar los requisitos de los servicios prestados y adoptará las medidas de índole técnicas y organizativas necesarias que sean posibles para garantizar la seguridad en el ciclo de vida de los servicios y sistemas.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, tanto, de su protección.
- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con los equipos que por razón de su cargo o función establece internamente el Plan Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 29 de 56

6.9. Jefe/a del Servicio Recursos Humanos:

De forma general, el Jefe/a del Servicio de Recursos Humanos por ostentar más de responsabilidad asignada a su puesto de trabajo en el desempeño de las diferentes obligaciones en materia de privacidad y seguridad deberá abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

En tanto **Responsable de Gestión de Personal**, le corresponden las siguientes funciones:

- Implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información.
- Informar a éste de su grado de implantación, eficacia e incidentes.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con equipos que por razón de su cargo o función establece internamente el Plan Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

6.10 Resto del personal:

Al resto del personal de la Diputación que no tenga encomendada alguna de las funciones anteriormente descritas, le corresponden las siguientes funciones:

- No se permite la difusión de datos de carácter personal ni confidencial pertenecientes a la entidad. Estando obligado a guardar secreto de la información incluso terminada la relación laboral.
- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión de deber del trabajador.
- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificación y contraseña, por tanto, no deberá revelar la contraseña.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo de cerrar sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones en los sistemas de la entidad sin el consentimiento del delegado de protección de datos.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 30 de 56

- El usuario se responsabilizará de guardar copias de todos los correos que incluya anexos con datos personales vinculados a la entidad.
- Asimismo, podrá estar obligado a cumplir con las obligaciones y colaborar con equipos que por razón de su cargo o función establece internamente el Plan Continuidad de Negocio, en su caso, para la gestión de las incidencias y ejecución de las actividades de recuperación.

Debe estar formado en Ciberseguridad según programa propio de la diputación de Castellón

ÓRGANOS COLEGIADOS.

Se establecen los siguiente órganos colegiados en materia de seguridad:

1. Comité de seguridad
2. Equipo de recuperación
3. Comité de crisis
4. Oficina Provincial de Protección de Datos y Seguridad

Se desarrollan a continuación cada uno de ellos:

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La coordinación de la seguridad de la información en las entidades dentro del ámbito de aplicación del ENS es especialmente importante por exigencia de racionalización del gas para evitar disfunciones que propicien la aparición de brechas de seguridad provocadas por puntos débiles en los sistemas de información que posibiliten incidentes accidentales, incluso, ciberataques.

El Comité de Seguridad de la Información, que coordina la seguridad de la información en la entidad, estará formado por todas aquellas personas de la entidad que participen en la responsabilidad, definición o implantación de la ciberseguridad de la información tratada en los servicios prestados, entre ellos, el Titular de la entidad (o persona delegada, que ostente la presidencia del Comité), los responsables de la Información, los Servicios, la Seguridad del Sistema, el Delegado de Protección de Datos y por representantes de otras áreas de la entidad.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 31 de 56

organización afectadas. La composición se determinará en la Política de Seguridad de la Información de la organización.

Entre otras funciones el Comité de Seguridad de la Información ostenta las siguientes:

a. Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.

b. Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.

c. Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.

d. Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

e. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

f. Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión de incidentes, velando por la coordinación de las diferentes áreas en materia de seguridad en la gestión de tales incidentes.

g. Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la información.

h. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.

i. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

j. Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir asesoramiento al Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 32 de 56

creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.

k. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Puesto que el Comité de Seguridad de la Información no es un comité técnico, podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de decisiones y asesoramiento, realizando formación especializada en la materia. También podrá contar con Grupos de Trabajo especializados, internos, externos o mixtos.

El Responsable de la Seguridad actuará como Secretario del Comité de Seguridad, con las siguientes funciones derivadas:

- Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones del presidente del Comité.
- Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.
- Elaborar el acta de las reuniones.
- Remitir el acta de las reuniones a los asistentes, recabando su firma.
- Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

EQUIPO DE RECUPERACIÓN.

Son miembros del Equipo de recuperación: los empleados provinciales que ocupen los Puestos de trabajo números 1044, 1245, 1368, 1323, y 930

Como **miembros del Equipo de recuperación**, les corresponden las siguientes funciones:

- Participar en las actividades de evaluación y recuperación de los procesos de negocio realizando una evaluación de daños ocasionados por la incidencia en sus respectivas áreas de responsabilidad y adoptando todas aquellas medidas que resulten necesarias para la resolución de la incidencia y el restablecimiento de los procesos de negocio.



 DIPUTACIÓN DE CASTELLÓN	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 33 de 56

- En la gestión de la continuidad del negocio el equipo de recuperación deberá:
 - o Evaluar la repercusión y efectos de la incidencia sobre los recursos de su área de responsabilidad, determinando la posibilidad de recuperación de los mismos.
 - o Iniciar los procedimientos de recuperación de los procesos de negocio de los que son responsables.
 - o Contactar tan pronto como sea posible con las personas que de ellos dependen y coordinar sus acciones para la recuperación de los procesos de negocio que caen bajo su responsabilidad.
 - o Establecer contacto con los terceros (proveedores, socios, ...) con los que habitualmente mantienen relaciones a fin de coordinarse con ellos en la medida en que sea necesario.
 - o Supervisar y coordinar la recuperación de los recursos (infraestructura, hardware, software, información, ...) que hubieran resultado afectados por la incidencia en las Oficinas Centrales.
 - o Adoptar todas aquellas medidas adicionales que resulten necesarias para la reanudación de los procesos críticos de negocio, ya sea en las propias oficinas o en las oficinas de contingencia que les fuera comunicado.
 - o Gestionar y coordinar, si procede, el traslado a los centros de contingencia de las personas y los activos de información que fueran necesarios.

Debe estar formado en Ciberseguridad y Formación de roles ENS y PCN según programa propio de la diputación de Castellón.

COMITÉ DE CRISIS.

Son miembros del Comité de Crisis: Presidente y Diputado Informática (sin RPT), puestos de trabajo 1, 1308, 1245, 1323, 1368

Como **miembros del Comité de Crisis**, le corresponden las siguientes funciones:

- Coordinar la respuesta ante los incidencias graves o catastróficas determinando en caso de considerarlo necesario, el traslado de las operaciones a las ubicaciones



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 34 de 56

contingencia, y garantizando la reanudación de las mismas en el marco temporal establecido para ello.

- Concretamente:
 - o Prestar un apoyo visible por parte de la Dirección al PCN.
 - o Garantizar que la Diputación dispone de un PCN acorde a las necesidades del negocio.
 - o Desarrollar programas de concienciación y formación sobre el PCN para el personal de la Diputación.
 - o Supervisar la realización de pruebas y el mantenimiento y actualización del PCN.
 - o Aprobar los cambios del PCN.
 - o Activar el/los Plan/es de Emergencia y/o Plan/es de Evacuación en el supuesto de que se dieran las condiciones que obliguen a la evacuación de las personas de las instalaciones de la Diputación.
 - o Activar el PCN en cualquiera de los escenarios de contingencia o de desastre previamente establecidos.
 - o Gestionar las reclamaciones de cobertura de las pólizas de seguros contratadas por la Diputación.
 - o Asegurarse de contar con los recursos económicos necesarios para afrontar partidas de gastos extraordinarios en los que sea necesario incurrir durante el estado de contingencia o desastre y autorizar la ejecución de los mismos.
 - o Mantener informada a la opinión pública, accionistas y proveedores acerca de la situación de la Diputación tras la contingencia o el desastre.
 - o Proveerse de centros alternativos de operación en el supuesto de que resultara necesario, así como autorizar y coordinar el traslado de las operaciones del negocio a los lugares seleccionados.

Debe estar formado en Ciberseguridad según programa propio de la diputación de Castellón



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD D	
	INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRAB	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026 Página 35 de 56

OFICINA PROVINCIAL DE PROTECCIÓN DE DATOS Y SEGURIDAD (Este órgano cambiado su configuración, centrándose en la figura del DPD tras Decreto 2026/2 Reestructuración de la Oficina Provincial de Protección de Datos Seguridad)

El 24 de mayo de 2018, mediante Decreto del Presidente se creó formalmente la Oficina Provincial de Protección de Datos y Seguridad, con el objetivo de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que así lo soliciten.

La oficina provincial de protección de datos y seguridad, se constituyó mediante decreto 2018/1900, modificado por decreto número 2018/2089, y por decreto número 2021/1981, cuya parte dispositiva es la siguiente:

“PRIMERO.- Crear la Oficina Provincial de Protección de Datos y Seguridad, que desarrolle las funciones previstas tanto en la normativa nacional como comunitaria, relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que así lo soliciten.

SEGUNDO.- Adscribir a los funcionarios que se relacionan a continuación a la Oficina Provincial de Protección de Datos y Seguridad:

- *Borja Colón de Carvajal Fibla, Jefe del Servicio de Administración e Innovación Pública, como representante de la Oficina ante la Agencia Española de Protección de Datos así como ante interesados y/o afectados que así lo requieran.*
- *Manuel Pesudo Esteve, Secretario General de la Diputación.*
- *Antonio Sáez Sanz, Jefe del Servicio de Informática, que se integra en la misma como responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad, debiendo abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.*
- *Álvaro Porcar Barreda, Jefe de Sección de Informática Municipal.*
- *Mónica Marí Torán, Jefa del Servicio de Recursos Humanos.*
- *Sandra Cañamás Femenía, Auxiliar Administrativa de Actas y Decretos, que ejercerá las funciones administrativas de secretaría de la Oficina.*

TERCERO.- Encomendar a la Oficina Provincial de Protección de Datos y Seguridad las funciones específicas que aparecen recogidas como Anexo I a la presente Resolución, debiéndose realizar la distribución de las mismas entre los integrantes de la citada Oficina previstos en el apartado anterior



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 36 de 56

CUARTO.- Encomendar al Servicio de Administración e Innovación Pública la contratación de asistencia técnica que dé el soporte necesario para que la Oficina Provincial de Protección de Datos Seguridad pueda empezar a prestar servicio a la Diputación y a los Ayuntamientos lo antes posible, específicamente en las funciones vinculadas al Delegado de Protección de Datos.

QUINTO.- Encomendar el Servicio de Recursos Humanos que disponga la creación de una plaza específica de Delegado de Protección de datos en cuanto la normativa así lo permita.

SEXTO.- La Oficina Provincial de Protección de Datos y Seguridad ejercerá sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento, dando reporte a los máximos órganos directivos de la Diputación de Castellón."

SEGUNDO.- Dar cuenta al Pleno de la Diputación de la versión consolidada del Decreto del Presidente número 1900 de fecha 24 de mayo."

Como funciones generales de la citada oficina se establecen, mediante decreto las siguientes:

- Informar y asesorar al responsable, al encargado y empleados.
- Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y formación del personal.
- Asesorar acerca de la evaluación de impacto y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto en cuestiones relativas al tratamiento de los datos, incluyendo consultas previas.
- Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y se aplican procedimientos correctos para su destrucción cuando corresponda.
- Supervisar que los tratamientos disponen de bases jurídicas o legitimación.
- Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas)
- Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Asesorar y supervisar el diseño e implantación de políticas de protección de datos
- Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección



- Supervisar la primera versión de los registros de actividades de tratamiento así como los cambios que se realicen en los mismos
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre protección de datos
- Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados
- Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre protección de datos
- Supervisar las evaluaciones de impacto sobre la protección de datos
- Mantener las relaciones con las autoridades de supervisión
- Mantener el contacto con los interesados
- Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de los usuarios
- Reportar periódicamente a Dirección sobre el estado de cumplimiento en la materia y las acciones que haya que acometer así como reportar ante incidencias y circunstancias que se produzcan puntualmente

Con carácter general, además de las funciones relativas al Esquema Nacional de Seguridad, esta Oficina ejercerá las funciones que detalla el artículo 39 del RGPD, que pueden resumirse en:

- a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personal incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación
- d) cooperar con la autoridad de control;



e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento y realizar consultas, en su caso, sobre cualquier otro asunto.

A sus miembros, les corresponden las siguientes funciones:

- Desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma como para los municipios de la provincia que se sitúan por debajo del umbral de 20.000 habitantes que así lo soliciten. Concretamente:
 - o Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
 - o Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de las disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
 - o Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
 - o Cooperar con la autoridad de control;
 - o Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 y realizar consultas, en su caso, sobre cualquier otro asunto.

Dichas funciones fueron distribuidas mediante decreto 2019/0479, de 28 de enero de 2019, se acompaña como anexo.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 39 de 56

ANEXO I: Decreto número 2025/1734 de asignación de funciones

“Expte.: 3001/2017

La Ilma. Sra. Presidenta de esta Excm. Diputación Provincial de Castellón mediante dec. núm. 2025-1734 de 15 de mayo ha resuelto el siguiente tenor literal:

“El presente decreto anula y sustituye el decreto número 1215 de fecha 28 de abril de 2022 por los efectos de adaptar el mismo a las modificaciones orgánicas recientes, procediéndose a redactar la versión consolidada de acuerdo con el siguiente tenor literal:

La Diputación de Castellón depende de sus sistemas de informáticos y tecnológicos para alcanzar objetivos institucionales. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada por los servicios prestados.

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información (confidencialidad, integridad, disponibilidad y usos previstos) y la prestación continuada de los servicios actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante incidentes.

Esto implica que la organización y su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, aprobado por el Real Decreto 311/2022, de 2 de mayo, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

En este sentido, la Diputación de Castellón debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, es por todo lo anterior, por lo que RESUELVO:

PRIMERO.- Designar formalmente a las personas que aparecen en los Anexos de la presente Resolución para que desempeñen cada una de las responsabilidades en los términos de Seguridad que exige el Esquema Nacional de Seguridad.

SEGUNDO.- Publicar la presente resolución en el Boletín Oficial de la Provincia, quedando integrada en la Política de Seguridad de la Diputación.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 40 de 56

ANEXO I.- FUNCIONES Y RESPONSABILIDADES ASIGNADAS EN RELACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD.

6. Responsable de la Información: Presidente/a
7. Responsable de la Seguridad: El/La Oficial Mayor
8. Responsable del Sistema: Jefe/a de Sección de Sistemas.
9. Administrador de Seguridad del Sistema: Técnico de sistemas.
10. Responsables de los Servicios / Información de su departamento que a continuación se relacionan

- Director de Buen Gobierno y Administración
- Jefe del Servicio Jurídico
- Jefe Servicio Bienestar Social e Igualdad
- Jefe Servicio Recursos Humanos
- Responsable de Formación
- Responsable de Prevención y Riesgos Laborales
- Jefe Servicio Cooperación Municipal
- Jefe Servicio de Cultura, Restauración, Deportes y Juventud
- Jefe Servicio de Contratación y Central de Compras
- Jefe Servicio de Patrimonio y Expropiaciones
- Jefe Servicio de Administración e Innovación Pública
- Jefe Servicio de Promoción Económica y Relaciones Internacionales
- Tesorero
- Jefe Servicio de Informática
- Jefe del Área Técnica
- Jefe Servicio de Infraestructura
- Jefe Servicio Oficina Técnica
- Jefe Servicio Carreteras y Obras
- Jefe Servicio Ingeniería Interna
- Responsable Archivo
- Responsable Publicaciones
- Interventor
- Responsable del Servicio Gráfico y Digital
- Jefe de Sección de Informática Municipal
- Jefe Servicio Gestión Tributaria y Recaudación
- Director Técnico y Coordinador de Peñeta Roja
- Responsable Conservación Preventiva y Restauración Colecciones Arte
- Responsable del Parque Móvil

ANEXO II.- COMPOSICIÓN DEL COMITÉ DE SEGURIDAD

- Presidente: Presidenta de la Corporación o en quien delegue
- Responsable de Seguridad/Secretaría: El/La Oficial Mayor (Secretaría General)
- Vocales.
 - 1.8. Responsable del Sistema: Jefe/a de Sección de Sistemas
 - 1.9. Responsable Informática: Jefe del Servicio de Informática
 - 1.10. Delegado de protección de datos
 - 1.11. Responsable de servicios: Director de Buen Gobierno
 - 1.12. Responsable RRHH y Formación



 DIPUTACIÓ D E CASTELLÓ	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 41 de 56

- 1.13. Responsable Administración e Innovación pública
- 1.14. Responsable Informática municipal"

Lo que se hace público para general conocimiento.

Castellón de la Plana, a la fecha de la firma.

LA PRESIDENTA, Marta Barrachina Mateu	LA OFICIAL MAYOR., Montserrat Paricio Comins
--	---

(Documento firmado electrónicamente)"



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026 Página 42 de 56

ANEXO II DECRETOS RELATIVOS A PROTECCIÓN DE DATOS

Decreto 2018/1900 Creación de la oficina.

“DECRETO CREACIÓN OFICINA PROVINCIAL DE PROTECCIÓN DE DATOS Y SEGURIDAD.

Considerando que el 25 de mayo de 2018 resultará de aplicación directa a las Entidades Locales 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 (en adelante, RGPD), por lo que resulta urgente e inaplazable la adopción de cuantas medidas resulten necesarias para permitir su cumplimiento.

Considerando que el art. 37.3 del RGPD prevé la posibilidad de designar un único Delegado de Protección de Datos para varias autoridades u organismos públicos, de modo que la Diputación de Castellón puede acometer esta tarea también para los Ayuntamientos de la provincia con menos de 20.000 habitantes que así lo soliciten.

Resultando que el RGPD no impone una configuración determinada de la figura del Delegado de Protección de Datos, permitiendo el ejercicio de sus responsabilidades a través de un órgano colegiado.

Es por ello por lo que en base a todo lo anterior RESUELVO:

PRIMERO.- Crear la Oficina Provincial de Protección de Datos y Seguridad, que desarrollará funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquéllas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que lo soliciten.

SEGUNDO.- Adscribir a los funcionarios que se relacionan a continuación a la Oficina Provincial de Protección de Datos y Seguridad:

- Borja Colón de Carvajal Fibla, Jefe del Servicio de Administración e Innovación Pública, como representante de la Oficina ante la Agencia Española de Protección de Datos así como ante los interesados y/o afectados que así lo requieran.
- Manuel Pesudo, Secretario General
- Antonio Sáez, Jefe del Servicio de Informática, que se integra en la misma como responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad, debiendo abstenerse en aquéllas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades
- Álvaro Porcar, Jefe de Sección de Informática Municipal
- Mónica Marí, Jefa del Servicio de Recursos Humanos
- Sandra Cañamás, Auxiliar Administrativa de Actas y Decretos, que ejercerá las funciones administrativas de secretaría de la Oficina



TERCERO.- Encomendar a la Oficina Provincial de Protección de Datos y Seguridad las funciones específicas que aparecen recogidas como Anexo a la presente Resolución, debiéndose realizar una distribución de las mismas entre los integrantes de la citada Oficina previstos en el apartado anterior.

CUARTO.- Encomendar al Servicio de Administración e Innovación Pública la contratación de una asistencia técnica que dé el soporte necesario para que la Oficina Provincial de Protección de Datos y Seguridad pueda empezar a prestar servicio a la Diputación y a los Ayuntamientos antes posible específicamente en las funciones vinculadas al Delegado de Protección de Datos.

QUINTO.- Encomendar al Servicio de Recursos Humanos que disponga la creación de una plaza específica de Delegado de Protección de datos en cuanto la normativa así lo permita.

SEXTO.- La Oficina Provincial de Protección de Datos y Seguridad ejercerá sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento dando reporte a los máximos órganos directivos de la Diputación de Castellón.

SÉPTIMO.- Dar cuenta del presente Decreto al Pleno de la Diputación de Castellón.

Documento firmado
electrónicamente al margen

ANEXO.- Funciones encomendadas a la Oficina Provincial de Protección de Datos y Seguridad que deberán ser distribuidas entre los integrantes de la misma.

- Informar y asesorar al responsable, al encargado y empleados.
- Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y formación del personal.
- Asesorar acerca de la evaluación de impacto y supervisar su aplicación.
- Cooperar con la autoridad de control
- Actuar como punto de contacto en cuestiones relativas al tratamiento de los datos, incluyendo consultas previas.
- Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
- Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y aplican procedimientos correctos para su destrucción cuando corresponda
- Supervisar que los tratamientos disponen de bases jurídicas o legitimación
- Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
- Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
- Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas)



- Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Asesorar y supervisar el diseño e implantación de políticas de protección de datos
- Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección
- Supervisar la primera versión de los registros de actividades de tratamiento así como los cambios que se realicen en los mismos
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados
- Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño de la protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Supervisar las evaluaciones de impacto sobre la protección de datos
- Mantener las relaciones con las autoridades de supervisión
- Mantener el contacto con los interesados
- Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de los usuarios
- Reporta periódicamente a Dirección sobre el estado de cumplimiento en la materia y las acciones que haya que acometer así como reportar ante incidencias y circunstancias que se produzcan puntualmente”

Decreto 2018/2089 Modificación de decreto 2018/1900

“MODIFICACIÓN (1) DEL DECRETO DE CREACIÓN DE LA OFICINA PROVINCIAL DE PROTECCIÓN DE DATOS Y SEGURIDAD

Considerando que mediante Decreto del Presidente número 1900 de fecha 24 de mayo de 2018 se creó la Oficina Provincial de Protección de Datos y Seguridad con el objeto de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA	
	INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 45 de 56

Resultando que a la citada Oficina se adscribieron una serie de empleados públicos de la Diputación y que ahora se considera singularmente preciso incorporar a una nueva función que represente los intereses derivados de los datos específicos que provienen del ámbito tributario que la Diputación gestiona.

Resultando, asimismo, que era necesario ampliar, además, el ámbito subjetivo del citado Decreto a todas las entidades del sector público dependientes de la Diputación, es por todo lo anterior por lo que RESUELVO:

PRIMERO.- Modificar el Decreto del Presidente número 1900 de fecha 24 de mayo, queda el mismo redactado de la forma siguiente:

“Considerando que el 25 de mayo de 2018 resulta de aplicación directa a las Entidades Locales 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 de 1997, (RGPD), siendo por ello urgente e inaplazable la adopción de cuantas medidas resulten necesarias para permitir su estricto cumplimiento.

Considerando que el art. 37.3 del RGPD prevé la posibilidad de designar un único Delegado de Protección de Datos para varias autoridades u organismos públicos, de modo que la Diputación de Castellón puede acometer esta tarea también para los Ayuntamientos de la provincia de menos de 20.000 habitantes que así lo soliciten, así como para el sector público dependiente de ésta.

Resultando que el RGPD no impone una configuración determinada de la figura del Delegado de Protección de Datos, permitiendo el ejercicio de sus responsabilidades a través de un órgano colegiado.

Es por ello por lo que en base a todo lo anterior RESUELVO:

PRIMERO.- Crear la Oficina Provincial de Protección de Datos y Seguridad, que desarrollará las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan debajo del umbral de los 20.000 habitantes que así lo soliciten.

SEGUNDO.- Adscribir a los funcionarios que se relacionan a continuación a la Oficina Provincial de Protección de Datos y Seguridad:

- *Borja Colón de Carvajal Fibla, Jefe del Servicio de Administración e Innovación Pública, como representante de la Oficina ante la Agencia Española de Protección de Datos así como como interlocutor de los interesados y/o afectados que así lo requieran.*
- *Manuel Pesudo, Secretario General de la Diputación.*
- *Antonio Sáez, Jefe del Servicio de Informática, que se integra en la misma como responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad.*



Nacional de Seguridad, debiendo abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.

- Álvaro Porcar, Jefe de Sección de Informática Municipal.
- Mónica Marí, Jefa del Servicio de Recursos Humanos.
- M^a Ángeles Guillamón, Asesora Jurídica adscrita al Servicio de Gestión, Inspección Recaudación.
- Sandra Cañamás, Auxiliar Administrativa de Actas y Decretos, que ejercerá las funciones administrativas de secretaría de la Oficina.

TERCERO.- Encomendar a la Oficina Provincial de Protección de Datos y Seguridad las funciones específicas que aparecen recogidas como Anexo I a la presente Resolución, debiéndose realizar una distribución de las mismas entre los integrantes de la citada Oficina previstos en el apartado anterior.

CUARTO.- Encomendar al Servicio de Administración e Innovación Pública la contratación de una asistencia técnica que dé el soporte necesario para que la Oficina Provincial de Protección de Datos y Seguridad pueda empezar a prestar servicio a la Diputación y a los Ayuntamientos antes posible específicamente en las funciones vinculadas al Delegado de Protección de Datos.

QUINTO.- Encomendar al Servicio de Recursos Humanos que disponga la creación de una plaza específica de Delegado de Protección de datos en cuanto la normativa así lo permita.

SEXTO.- La Oficina Provincial de Protección de Datos y Seguridad ejercerá sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento dando reporte a los máximos órganos directivos de la Diputación de Castellón".

SEGUNDO.- Dar cuenta al Pleno de la Diputación de la versión consolidada del Decreto Presidente número 1900 de fecha 24 de mayo.

Documento firmado
electrónicamente al margen

ANEXO I.- Funciones encomendadas a la Oficina Provincial de Protección de Datos y Seguridad que deberán ser distribuidas entre los integrantes de la misma.

- Informar y asesorar al responsable, al encargado y empleados.
- Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y formación del personal.
- Asesorar acerca de la evaluación de impacto y supervisar su aplicación.
- Cooperar con la autoridad de control.



- Actuar como punto de contacto en cuestiones relativas al tratamiento de los datos, incluyendo las consultas previas.
- Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y se aplican procedimientos correctos para su destrucción cuando corresponda.
- Supervisar que los tratamientos disponen de bases jurídicas o legitimación.
- Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recolección inicial de los datos.
- Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas)
- Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos, que sean adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Asesorar y supervisar el diseño e implantación de políticas de protección de datos
- Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección
- Supervisar la primera versión de los registros de actividades de tratamiento así como los cambios que se realicen en los mismos
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados
- Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Supervisar las evaluaciones de impacto sobre la protección de datos



- Mantener las relaciones con las autoridades de supervisión
- Mantener el contacto con los interesados
- Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de usuarios
- Reporta periódicamente a Dirección sobre el estado de cumplimiento en la materia y acciones que haya que acometer así como reportar ante incidencias y circunstancias que produzcan puntualmente”

Decreto 2019/0479 Decreto de asignación de funciones**“DECRETO DE DISTRIBUCIÓN DE FUNCIONES ENTRE LOS MIEMBROS DE LA OFICINA DE PROTECCIÓN DE DATOS Y SEGURIDAD**

Considerando que mediante el Decreto de Presidencia, número 2.089 de 7 de junio de 2019 se creó formalmente la Oficina Provincial de Protección de Datos y Seguridad, con el objeto de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos, así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que así lo soliciten.

Visto que en dicho Decreto se disponía literalmente en su punto tercero que se encomendaba a la Oficina Provincial de Protección de Datos y Seguridad las funciones específicas que aparecían recogidas como Anexo I de éste, debiéndose realizar la distribución de las mismas entre los integrantes de la citada Oficina.

Es por ello, por lo que en base a lo anterior, RESUELVO:

PRIMERO.- Aprobar la distribución de funciones según aparecen indicados en el Anexo I, adjunto al presente Decreto.

SEGUNDO.- Comunicarlo a la Agencia Española de Protección de Datos de Carácter Personal.

Documento firmado electrónicamente al margen.

ANEXO I

FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS	PERFIL	DELEGABLE CONSULTORA	PERSONA
Supervisar sobre la identificación de las bases de datos jurídicas de los tratamientos.	JURÍDICO	SI	Mª A. Guzmán
Valorar la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.	JURÍDICO	SI	Mª A. Guzmán
Supervisar la existencia de normativa sectorial que	JURÍDICO	SI	Mª A.



pueda determinar condiciones de tratamiento específicas.			Guillamón
Supervisar la existencia de medidas de información a los afectados por los tratamientos de datos. (cláusulas)	JURÍDICO	SI	Mª A. Guillamón
Aprobar y supervisar el procedimiento de contratación de encargados de tratamiento, incluido el contenido de los contratos requeridos.	JURÍDICO	SI	Mª A. Guillamón
Aprobar las transferencias internacionales de Datos que se realizan y supervisar que todas ellas disponen de una causa de legitimación	PRESIDENTE COMITÉ	NO	B. Colón
Supervisar y aprobar el diseño e implantación de políticas de protección de datos.	COMITÉ	SI	Mª A. Guillamón
En relación con el registro de actividades de tratamiento:			
Aprobar los registros de actividades de tratamiento	COMITÉ	NO	Mª A. Guillamón
Supervisarlos así como aprobar los cambios que se realicen en relación con los mismos.	COMITÉ	SI	Mª A. Guillamón
En relación con el ejercicio de derechos:			
Mantener las relaciones con las autoridades de supervisión y en su caso interesados en el caso de que se produzcan procedimientos de tutela de derechos o se inicien actuaciones relacionadas con un posible incumplimiento en materia de protección de datos derivado de un derecho.	PRESIDENTE COMITÉ	NO	B. Colón
Alentar y aprobar la implantación de programas de formación y sensibilización del personal en materia de protección de datos en los que se incluya la correcta formación en materia de ejercicio de derechos a los actores con responsabilidades en la materia.	RESPONSABLE RRHH	NO delegar la tarea de alentar si la de asesorar y obviamente ejecutar	M. Marí
Alentar y aprobar la implantación de programas de sensibilización a los interesados (empleados) en relación con el tratamiento de sus datos personales que incluya lo relativo al ejercicio de sus derechos.	RESPONSABLE RRHH	NO delegar la tarea de alentar si la de asesorar y obviamente ejecutar	M. Marí
Establecer mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados	JURÍDICO	SI	B. Colón
En relación con las evaluaciones de impacto:			
Asesorar y aprobar sobre si se debe de llevar a cabo una evaluaciones de impacto sobre la protección de datos.	COMITÉ	SI	A. Porcar



Asesorar sobre la metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos	COMITÉ	SI	A. Porcar
Asesorar sobre si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa,	COMITÉ	SI	A. Porcar
Asesorar sobre qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados	COMITÉ	SI	A. Porcar
Supervisar si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el Reglamento	COMITÉ	SI	A. Porcar
En relación con las auditorías:			
Asesorar sobre qué áreas deben someterse a auditoría de protección de datos interna o externa,	COMITÉ	SI	A. Porcar
Promover la realización de controles y auditorías del Sistema de Gestión de Protección de Datos.	COMITÉ	SI	A. Porcar
Supervisar los resultados de las auditorías.	COMITÉ	SI	B. Colón
Supervisar y aprobar la implantación de las medidas de protección de datos desde el diseño y por defecto adecuadas a los riesgos y naturaleza de los tratamientos.	COMITÉ	SI	A. Porcar
Supervisar y aprobar los análisis de riesgo de los tratamientos realizados.	TÉCNICO	SI	A. Porcar
Supervisar y aprobar la implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.	TÉCNICO	SI	A. Porcar
Supervisar y aprobar la implantación del establecimiento de procedimientos de gestión de violaciones de seguridad de los datos y de notificación a las autoridades y a los afectados.	COMITÉ	SI	Mª A. Guillamón
Mantener las relaciones con las autoridades de control que se deriven de las violaciones de seguridad, procedimiento de tutela de derechos, procedimiento sancionador o cualquier otro motivo.	PRESIDENTE COMITÉ	NO	B. Colón
Mantener las relaciones con interesados que se requieran.	PRESIDENTE COMITÉ	NO	B. Colón
Promover la implantación de programas de formación y sensibilización del personal en materia de protección de datos.	RESPONSABLE RRHH	SI	M. Marí



Supervisar que el sistema de gestión de protección de datos es conveniente, adecuado y eficaz y promover la mejora continua.	COMITÉ	SI	B. Colón
Asesorar a la Dirección sobre los niveles de riesgos aceptables.	PRESIDENTE COMITÉ	NO	B. Colón
Elevar los resultados, de las revisiones del estado de la gestión de la protección de datos a la Dirección.	PRESIDENTE COMITÉ	NO	B. Colón
Resolver los conflictos de responsabilidades que puedan aparecer entre los diferentes roles y/o entre diferentes áreas en relación con la protección de datos de carácter personal.	COMITÉ	SI	M ^a A. Guillamón
Gestionar las reclamaciones que se produzcan en materia de protección de datos que le sean trasladadas.	COMITÉ	SI	B. Colón
Supervisar la gestión de brechas de seguridad, Particularmente antes de su comunicación ante la autoridad de control y/o interesados.	COMITÉ	SI	A. Porcar

”

Decreto 2021/1981 Modificación del decreto 2018/1900

“2ª MODIFICACIÓN DEL DECRETO DE CREACIÓN DE LA OFICINA PROVINCIAL DE PROTECCIÓN DE DATOS Y SEGURIDAD

Considerando que mediante Decreto del Presidente número 1900 de fecha 24 de mayo de 2018 se creó la Oficina Provincial de Protección de Datos y Seguridad con el objeto de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad.

Resultando que a la citada Oficina se adscribieron una serie de empleados públicos de la Diputación de Castellón que ahora se considera eliminar a la funcionaria que representaba los intereses derivados de los departamentos específicos que provienen del ámbito tributario que la Diputación gestiona.

Resultando, asimismo, que era necesario ampliar, además, el ámbito subjetivo del citado Decreto a todas las entidades del sector público dependientes de la Diputación, es por todo lo anterior por lo que RESUELVO:

PRIMERO.- Modificar el Decreto del Presidente número 1900 de fecha 24 de mayo, quedando el mismo redactado de la forma siguiente:

“Considerando que el 25 de mayo de 2018 resulta de aplicación directa a las Entidades Locales 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 (en adelante, RGPD), siendo ello urgente e inaplazable la adopción de cuantas medidas resulten necesarias para permitir su est. cumplimiento.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 52 de 56

Considerando que el art. 37.3 del RGPD prevé la posibilidad de designar un único Delegado de Protección de Datos para varias autoridades u organismos públicos, de modo que la Diputación de Castellón pueda acometer esta tarea también para los Ayuntamientos de la provincia de menos de 20.000 habitantes así lo soliciten, así como para el sector público dependiente de ésta.

Resultando que el RGPD no impone una configuración determinada de la figura del Delegado de Protección de Datos, permitiendo el ejercicio de sus responsabilidades a través de un órgano colegiado.

PRIMERO.- Crear la Oficina Provincial de Protección de Datos y Seguridad, que desarrollará las funciones previstas tanto en la normativa nacional como comunitaria, relativas al Delegado de Protección de Datos, así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón, las entidades del sector público dependientes de la misma, como para los municipios de la provincia que se sitúan por debajo del umbral de los 20 habitantes que así lo soliciten.

SEGUNDO.- Adscribir a los funcionarios que se relacionan a continuación a la Oficina Provincial de Protección de Datos y Seguridad:

- Borja Colón de Carvajal Fibla, Jefe del Servicio de Administración e Innovación Pública, como representante de la Oficina ante la Agencia Española de Protección de Datos así como ante interesados y/o afectados que así lo requieran.
- Manuel Pesudo Esteve, Secretario General de la Diputación.
- Antonio Sáez Sanz, Jefe del Servicio de Informática, que se integra en la misma como responsable de la seguridad para la Diputación de Castellón en los términos establecidos en el Esquema Nacional de Seguridad, debiendo abstenerse en aquellas decisiones en las que pueda existir conflicto de intereses en el ejercicio de sus responsabilidades.
- Álvaro Porcar Barreda, Jefe de Sección de Informática Municipal.
- Mónica Marí Torán, Jefa del Servicio de Recursos Humanos.
- Sandra Cañamás Femenía, Auxiliar Administrativa de Actas y Decretos, que ejercerá las funciones administrativas de secretaría de la Oficina.

TERCERO.- Encomendar a la Oficina Provincial de Protección de Datos y Seguridad las funciones específicas que aparecen recogidas como Anexo I a la presente Resolución, debiéndose realizar la distribución de las mismas entre los integrantes de la citada Oficina previstos en el apartado anterior.

CUARTO.- Encomendar al Servicio de Administración e Innovación Pública la contratación de asistencia técnica que dé el soporte necesario para que la Oficina Provincial de Protección de Datos y Seguridad pueda empezar a prestar servicio a la Diputación y a los Ayuntamientos lo antes posible, específicamente en las funciones vinculadas al Delegado de Protección de Datos.

QUINTO.- Encomendar al Servicio de Recursos Humanos que disponga la creación de una plaza específica de Delegado de Protección de datos en cuanto la normativa así lo permita.

SEXTO.- La Oficina Provincial de Protección de Datos y Seguridad ejercerá sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento, dando reporte a los máximos órganos directivos de la Diputación de Castellón."

SEGUNDO.- Dar cuenta al Pleno de la Diputación de la versión consolidada del Decreto del Presidente número 1900 de fecha 24 de mayo.

Castelló de la Plana, a la fecha de la firma electrónica.



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 53 de 56

ANEXO I.- Funciones encomendadas a la Oficina Provincial de Protección de Datos y Seguridad que deberán ser distribuidas entre los integrantes de la misma.

- Informar y asesorar al responsable, al encargado y empleados.
- Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y forma del personal.
- Asesorar acerca de la evaluación de impacto y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto en cuestiones relativas al tratamiento de los datos, incluyendo consultas previas.
- Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen aplican procedimientos correctos para su destrucción cuando corresponda.
- Supervisar que los tratamientos disponen de bases jurídicas o legitimación.
- Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas)
- Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar las solicitudes de ejercicio de derechos por parte de los interesados
- Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Asesorar y supervisar el diseño e implantación de políticas de protección de datos
- Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección
- Supervisar la primera versión de los registros de actividades de tratamiento así como los cambios que se realicen en los mismos
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados
- Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño de la protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 54 de 56

- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre protección de datos
- Supervisar las evaluaciones de impacto sobre la protección de datos
- Mantener las relaciones con las autoridades de supervisión
- Mantener el contacto con los interesados
- Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de usuarios
- Reporta periódicamente a Dirección sobre el estado de cumplimiento en la materia y las acciones que haya que acometer así como reportar ante incidencias y circunstancias que se produzcan puntualmente”

Decreto 2026/2466 Reestructuración de la Oficina Provincial de Protección de Datos y Seguridad

DECRETO DE LA PRESIDENCIA ESTABLECIENDO LA REESTRUCTURACIÓN DE LA OFICINA PROVINCIAL DE PROTECCIÓN DE DATOS Y SEGURIDAD Y DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

Visto el decreto de la Presidencia número 2018-1900 de fecha 24 de mayo de 2018 por el que se creó la Oficina Provincial de Protección de Datos y Seguridad con el objeto de desarrollar las funciones previstas tanto en la normativa nacional como comunitaria relativas al Delegado de Protección de Datos así como todas aquellas cuestiones relacionadas con el cumplimiento del Esquema Nacional de Seguridad, tanto para la Diputación de Castellón como para los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que así lo soliciten.

Dicha Oficina Provincial de Protección de Datos y Seguridad se creó originalmente como un órgano colegiado compuesto por diversos funcionarios adscritos.

Vistas las modificaciones realizadas mediante los decretos número 2018-2089 de fecha 7 de junio de 2018 y número 2021-1981 de fecha 9 de julio de 2021, en referencia a la incorporación de una nueva funcionaria y a la eliminación de un miembro de dicha Oficina, respectivamente.

Visto el decreto de la Presidencia número 2019-0479 de fecha 28 de enero de 2019, donde se aprueba la distribución de funciones específicas entre los integrantes de la citada Oficina.

Que, en paralelo a la evolución de la Oficina, se han cumplimentado con éxito las encomiendas de gestión previstas en los citados decretos anteriores, a saber:

- La contratación de una asistencia técnica externa por parte del Servicio de Administración e Innovación Pública que dé el soporte necesario a la Diputación en las funciones vinculadas al Delegado de Protección de Datos.
- La creación por parte del Servicio de Recursos Humanos de una plaza de Técnico de Administración General adscrita al Servicio de Administración e Innovación Pública para el ejercicio de las funciones propias correspondientes al Delegado de Protección de Datos.

Que, habiéndose dotado de los medios descritos anteriormente, resulta innecesario mantener la fórmula de órgano colegiado, procediendo la transición hacia un modelo unipersonal que garantice la eficacia, la unidad de criterio y el cumplimiento del artículo 37 del Reglamento (UE) 2016/679 (RGPD).



	FUNCIONES Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN QUE ANUNCIAR EN EL DETALLE DE LA RELACIÓN DE PUESTOS DE TRABAJO	
	PRIVACIDAD Y SEGURIDAD	EMISIÓN: 29/09/2026
		Página 55 de 56

el artículo 34 de la LOPDGDD 3/2018.

Por todo lo expuesto, dispongo:

PRIMERO.- Dejar sin efecto los Decretos números 2018-1900 de creación inicial, sus posteriores modificaciones 2018-2089 y 2021-1981, así como el 2019-0479 de distribución de funciones de la Oficina Provincial de Protección de Datos. En consecuencia, se declara la extinción de la misma en su formato de órgano colegiado.

SEGUNDO.- La Oficina Provincial de Protección de Datos se constituye, a partir de la fecha del presente Decreto, como un órgano de carácter unipersonal, recayendo toda la responsabilidad de la función de supervisión y asesoramiento en la figura del Delegado de Protección de Datos.

TERCERO.- Designar a Dña. Ana Isabel Moreno Soler, Técnico de Administración General, adscrito al Servicio de Administración e Innovación Pública como Delegado de Protección de Datos (DPD) de la Administración Provincial, de las entidades del sector público dependientes de la misma, así como de los municipios de la provincia que se sitúan por debajo del umbral de los 20.000 habitantes que a hubieran solicitado.

La Oficina Provincial de Protección de Datos y Seguridad ejercerá sus funciones con total independencia reportando directamente al nivel directivo más alto, de conformidad con la normativa vigente.

El DPD contará, asimismo, con la asistencia de Dña. Sandra Cañamás Femenía, Jefe de Negociado de Protección de Datos, que ejercerá las funciones administrativas de secretaría y de apoyo a dicha Oficina, asegurando de este modo la continuidad en las funciones de ésta y el apoyo permanente a todas las actividades.

CUARTO.- El DPD contará para el ejercicio de sus funciones con el apoyo de la asistencia técnica contratada al efecto por el Servicio de Administración e Innovación Pública, así como con los recursos materiales necesarios para garantizar el ejercicio de sus tareas.

QUINTO.- Notifíquese el presente Decreto a los servicios de Recursos Humanos y Administración e Innovación Pública. Asimismo, procédase a la comunicación formal a la Agencia Española de Protección de Datos (AEPD) de la modificación en la designación del DPD.

SEXTO.- Asimismo, notifíquese el cambio a los municipios que tienen encomendada la función de Delegado de Protección de Datos en favor de la Diputación de Castellón.

SÉPTIMO.- Publíquese el presente Decreto en el Portal de Transparencia para general conocimiento.

Lo manda y firma la Presidenta en Castellón de la Plana a la fecha de la firma electrónica, de lo que, como Secretario, certifico.

