Breve guía de implantación en materia de protección de datos

ALBACETE 2019
David Povedano Alonso
twitter: @pove22
e-mail: pove22@gmail.com

ACERCAMIENTO Y INTRODUCCION

DE LA PROTECCION DE DATOS Y OTRAS MATERIAS

“Tenemos que tener claro que un dato de carácter personal es aquel que nos identifica o que permite que seamos identificados. Algo que cada vez es más fácil. “

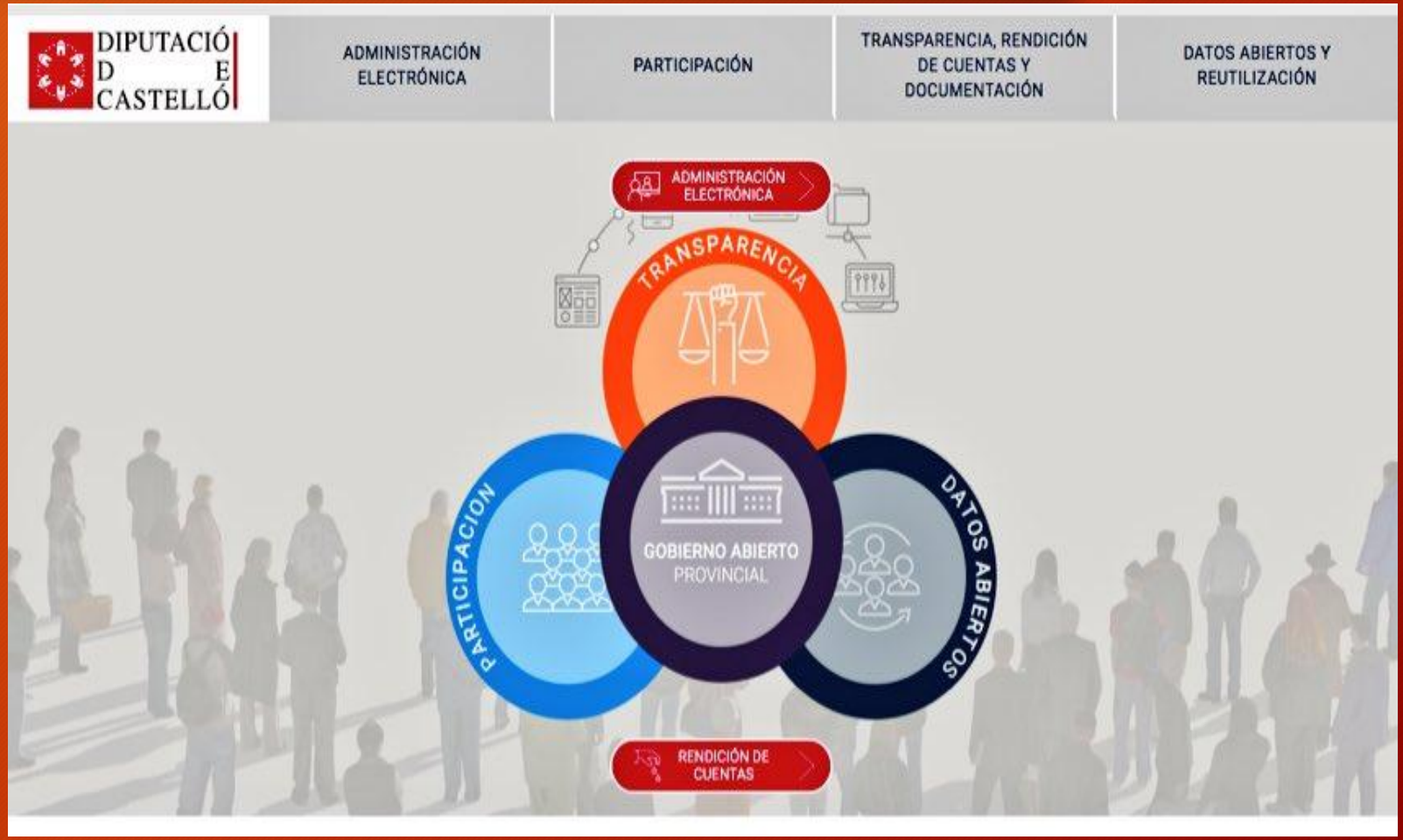
NUEVO MARCO LEGAL DE LAS ENTIDADES LOCALES EN MATERIA DE PROTECCION DE DATOS.

Desde 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 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 (LA LEY 6637/2016) quedando derogada la Directiva 95/46/CE. Asimismo, el 7 de diciembre de 2018 entró en vigor la tan esperada Ley Orgánica 3/2018, de 5 de diciembre (LA LEY 19303/2018) que viene a derogar la anterior LOPD (Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal). La nueva normativa introduce cambios significativos que exigen un alto nivel de proactividad y diligencia a la hora de cumplir y estar en disposición de evidenciar dicho cumplimiento. Esto supone una necesaria asignación de recursos, tanto humanos como económicos, que implica un gran esfuerzo, especialmente para los pequeños Ayuntamientos. Con el fin de establecer una hoja de ruta que facilite la planificación y proceso de adecuación, se enumeran a continuación los distintos aspectos procedimentales y operativos que pueden facilitar el abordaje del actual marco regulatorio en materia de protección de datos. En este camino es imprescindible la figura de la Diputación Provincial

LA CONCEPCIÓN DE LA SEGURIDAD COMO UN PROCESO INTEGRAL Y TRANSVERSAL

Desde un punto de vista práctico, a la hora de implantar de forma efectiva la normativa de protección de datos, es fundamental que la organización interiorice como un elemento estratégico esencial la necesidad de contemplar la seguridad de forma integral y transversal, como una dimensión más del proceso de transformación digital.

Hay que añadir la seguridad: R.D. 14/2019

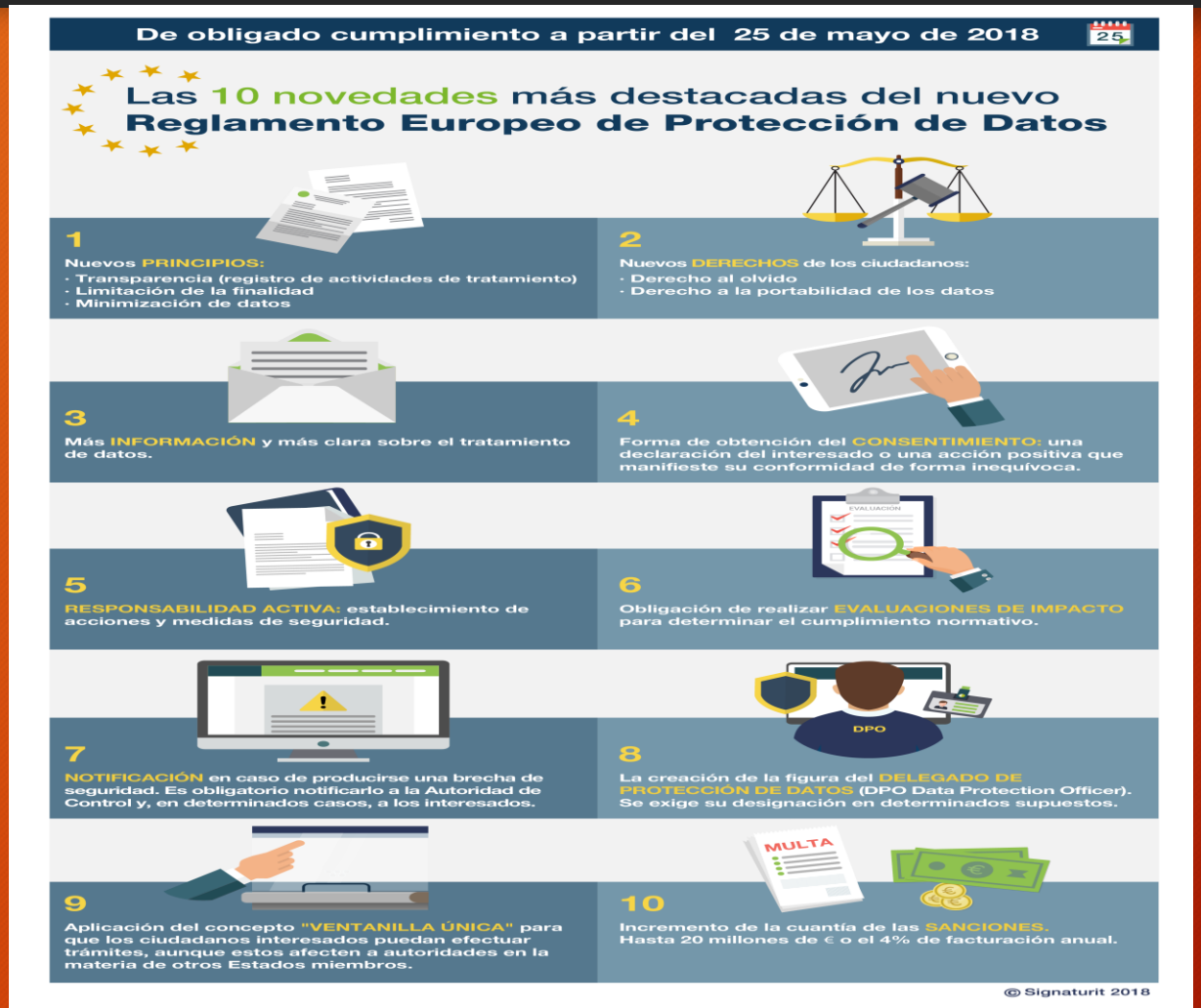


¿PORQUÉ UN REGLAMENTO?¿PORQUÉ NUESTROS DATOS Y LOS DE LOS CIUDADANOS SON TAN IMPORTANTES?

Medidas proactivas

1. • Delegado de protección de datos
2. • Registro de actividades de tratamiento.
3. • Medidas de protección de datos desde el diseño y por defecto
4. • Análisis de riesgos y adopción de medidas de seguridad
5. • Notificación de quiebras de seguridad
6. • Evaluaciones de impacto sobre la protección de datos
7. • La adhesión por parte de responsables y encargados de tratamiento a códigos de conducta,mecanismos de certificación, sellos y marcas de protección de datos

LAS 10 NOVEDADES MAS DESTACADAS DEL REGLAMENTO EUROPEO DE PROTECCION DE DATOS

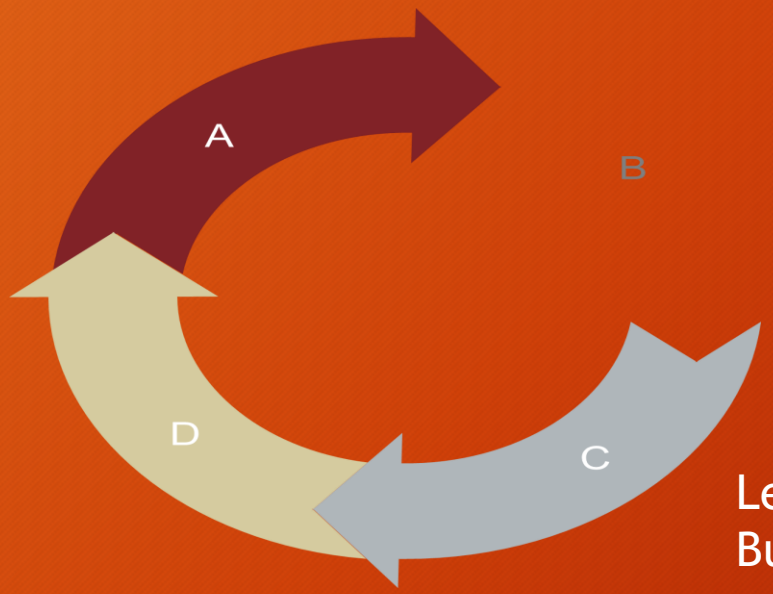


PORQUÉ SON IMPORTANTES NUESTROS DATOS

TRANSPARENCIA Y DEBER DE INFORMACIÓN EN EL PROCESO DE RECOGIDA Y TRATAMIENTO DE DATOS PERSONALES.

Transparencia VS protección de datos

https://elnuevofuncionarioconhabilitaciondecaracternacional.wordpress.com/2018/10/18/transparencia-vs-proteccion-de-datos/



Ley 4/2016, de 15 de diciembre, de Transparencia y Buen Gobierno de Castilla-La Mancha.

PRIMERO LA TRANSPARENCIA Y LUEGO DE LA MANO LA PROTECCIÓN DE DATOS.

Artículo 9. Información institucional y organizativa.
Artículo 10. Información sobre altos cargos y asimilados.
Artículo 11. Información sobre planificación y evaluación.
Artículo 12. Información de relevancia jurídica.
Artículo 13. Información sobre procedimientos administrativos y calidad de los servicios.
Artículo 14. Información económica, presupuestaria y financiera.
Artículo 15. Información patrimonial y estadística.
Artículo 16. Información sobre contratación pública.
Artículo 17. Información sobre convenios, encomiendas y encargos.
Artículo 18. Información sobre subvenciones y ayudas públicas.
Artículo 19. Información sobre ordenación territorial, urbanística y vivienda.
Artículo 20. Información ambiental.
Artículo 21. Información sobre cuentas abiertas.
Artículo 22. Otros contenidos objeto de publicidad.

https://www.boe.es/buscar/doc.php?id=BOE-A-2017-1373

DEBER DE INFORMACION ACTIVA SEGUN EL RGPD

El RGPD añade requisitos adicionales en cuanto a la necesidad de informar a las personas interesadas, incorporando, a los requisitos ya previstos por la LOPD (identidad del Responsable del Tratamiento, finalidad del tratamiento, destinatarios de los datos y procedimiento para el ejercicio de derechos) los siguientes aspectos al deber de información:

- La base que legitima el tratamiento;
- El plazo o los criterios aplicados de conservación de la información;
- Los datos de contacto del Delegado de Protección de Datos;
- La existencia, en su caso, de decisiones automatizadas o elaboración de perfiles;
- La previsión de transferencias a Terceros Países;
- El derecho a presentar una reclamación ante las Autoridades de Control.

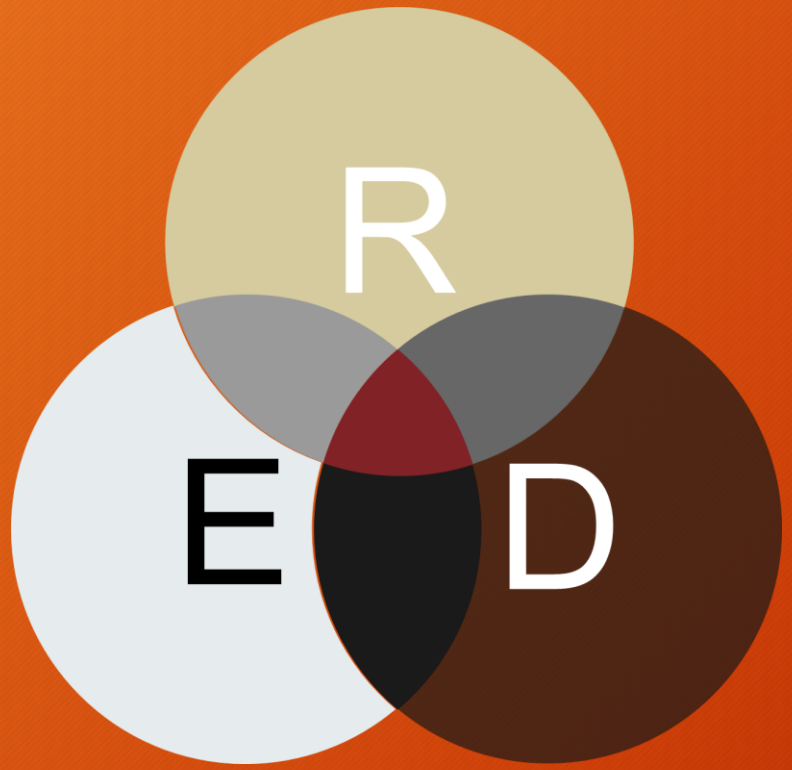
Y además, en el caso de que los datos no se obtengan del propio interesado, se deberá indicar:

- El origen de los datos;
- Las categorías de los datos.

Primera Capa de información

Responsable del Tratamiento	Identidad del Responsable del Tratamiento
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles.
Legitimación	Base jurídica del tratamiento
Destinatarios	Previsión o no de cesiones/ Previsión de transferencias o no, a terceros países.
Derechos	Referencia al ejercicio de derechos
Procedencia de los datos	Fuente de los datos, cuando no hayan sido aportados directamente por el propio interesado

PROTAGONISTAS EN MATERIA DE SEGURIDAD Y PROTECCIÓN DE DATOS



A **El responsible del tratamiento**

.. El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

B **El encargado del tratamiento**

Viene regulado en los artículos 28 y 29 del RGPD. Se trata de la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

C **Delegado de Protección de Datos**

Respecto a la posición del delegado de protección de datos, actuará como interlocutor del responsable o encargado del tratamiento ante las autoridades de control. .

NUEVOS ESCENARIOS: HOJA DE RUTA

1. DESIGNAR UN DELEGADO de Protección de Datos, si procede. (Ver art.37 *RGPD* y art. 34 *LOPDGDD*)
2. ELABORAR EL Registro de Actividades de tratamiento, prestando atención especialmente a los tratamientos que incluyan categorías especiales de datos o datos de menores, teniendo en cuenta su finalidad y la base jurídica
3. ANALIZAR las BASES JURÍDICAS de los TRATAMIENTOS
4. EFECTUAR UN ANÁLISIS DE RIESGOS. Sobre los resultados de ese análisis, identificar e implantar las MEDIDAS TÉCNICAS Y ORGANIZATIVAS necesarias para hacer frente a los riesgos detectados sobre los derechos y libertades de los ciudadanos y garantizar la integridad, confidencialidad y disponibilidad de los datos personales
5. VERIFICAR LAS MEDIDAS DE SEGURIDAD tras el resultado del análisis de riesgos. Ello incluye verificar la aplicación de medidas de seguridad adecuadas, así como ESTABLECER PROTOCOLOS PARA GESTIONAR Y, EN SU CASO, NOTIFICAR quiebras de seguridad. Las medidas de seguridad aplicables serán las establecidas en el Esquema Nacional de Seguridad (Disposición adicional primera LOPDGDD)
6. SI EL TRATAMIENTO ES DE ALTO RIESGO, DETALLAR E IMPLANTAR UN PROCEDIMIENTO para realizar, una evaluación de impacto de la privacidad y, si fuera necesario, consultar previamente a la autoridad de control (art. 35 y 36, *RGPD*)

LOS PROTAGONISTAS DE LA PROTECCION DE DATOS

NUEVOS ROLES EN EL RGPD Y EN LA LOPDGDD


RESPONSABLE Y ENCARGADO DEL TRATAMIENTO
EL DELEGADO DE PROTECCIÓN DE DATOS
ORGANISMO DE CONTROL
AEPD
TITULARES DEL DERECHO

NUEVA ORGANIZACION EN MATERIA DE PROTECCION DE DATOS

Política de Seguridad > **Organización de la seguridad**

Aprobación Organización de la seguridad por el órgano competente (políticas, procedimientos, funciones, régimen de funcionamiento…)

Acto constitución:

Asumen funciones seguridad RGPD-LOPDGDD + ENS

RESPONSABLE DE TRATAMIENTO (RGPD-LOPDGDD)
RESPONSABLE DE LA INFORMACIÓN (ENS)
Alcalde/Alcaldesa del Ayuntamiento

RESPONSABLE DE SEGURIDAD (ENS)
Órgano colegiado

Composición mínima:
- Secretaria general o Técnico/a jurista
- Informática **(Responsable Sistemas - ENS)**
- Alcaldía
- DPD

En ayuntamientos de mayor tamaño sería conveniente además:
- Gerencia/Dirección Organización y RRHH
- Oficina de Atención Ciudadana

Responsables funcionales de la Información (RGPD-LOPDGDD) y responsables del Servicio (ENS)
Direcciones de Servicio, departamento, sección…

Decisión sobre la finalidad, contenido y uso que se da a los tratamientos y servicios

DELEGADO DE PROTECCIÓN DE DATOS (DPD)

EL DELEGADO DE PROTECCION DE DATOS

Características

1.- OBLIGATORIO

2.- INDEPENDIENTE

3.-EL PERFIL

FUNCIONES

1.- Informar y asesorar

2.-Supervisar el cumplimiento de la normativa

3.-asesorar la evaluación de impacto

4.-cooperar con la autoridad de control

5.- actuar de contacto con la autoridad

6.-Otras

DERECHO DE LA LEY 3/2018

DERECHOS SOBRE LA PROTECCION DE DATOS Y NUEVOS DERECHOS DIGITALES

LOS DERECHOS DE LAS PERSONAS EN MATERIA DE PROTECCIÓN DE DATOS DESDE LA PERSPECTIVA DE LA ADMINISTRACIÓN LOCAL.

Derecho de Acceso

Dicho derecho comprende, **en primer lugar,** el conocimiento de si la entidad está o no tratando datos personales del solicitante, y **en segundo lugar,** el acceso a los mismos y a la siguiente información:
Fines del tratamiento, categorías de datos objeto de tratamiento, destinarios a los que se comunican dichos datos, plazo previsto de conservación, existencia de los derechos ARCO-POL y a la presentación de reclamación ante la autoridad de control (AEPD o equivalente autonómica), información sobre el origen de los datos cuando éstos no se hayan obtenido del interesado e información sobre la existencia o no de decisiones automatizadas, incluida la elaboración de perfiles.

Derecho de Rectificación

Aunque el art. RGPD hace referencia a que dicha rectificación, si fuese procedente, deberá realizarse por el responsable del tratamiento “sin dilación indebida”, entendemos de aplicación la previsión del plazo máximo de un (1) mes prevista en el Considerando 59 y en el art. 12.3 del RGPD.

La regulación de la LOPDGDD sobre el ejercicio de este derecho, que remite nuevamente al Reglamento Comunitario, se completa con la previsión de que la persona solicitante deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse, acompañando, cuando sea preciso, la documentación justificativa de la inexactitud o del carácter incompleto de los datos objeto de tratamiento.

Derecho de Supresión

Este derecho, del que son titulares las personas físicas respecto de sus datos personales en poder de las Entidades Locales, no debe entenderse como un derecho absoluto, en el sentido de que las EELL responsables están obligadas a que se cancelen, supriman o eliminen, es decir, dejen de ser tratados, los datos personales de un/a interesado/a, ante una mera solicitud de persona legitimada.

Para que proceda su estimación por la entidad local responsable, debe darse alguna, al menos una, de las siguientes circunstancias: innecesariedad de los datos el relación con los fines para que fueron recogidos o tratados, retirada del consentimiento cuando esta sea la única causa legitimadora del tratamiento, oposición de la persona interesada sin que prevalezcan otros motivos legítimos, obtención ilícita de los datos tratados, que exista una obligación legal que obligue a dicha supresión, o cuando dichos datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

Derecho al olvido

La referencia al “derecho al olvido”, que si es novedosa respecto a la regulación que contenía la anterior LOPD del derecho de cancelación, la establece el RGPD al indicar que cuando proceda la supresión solicitada, y dichos datos se hayan hecho públicos, el responsable del tratamiento (la Entidad Local), teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

En este sentido, la Guía del RGPD para responsables de tratamiento publicada por la AEPD y las autoridades de control de las C.A. del País Vasco y Cataluña considera al derecho al olvido como una “manifestación de los derechos de cancelación u oposición en el entorno online (según la jurisprudencia que el TJUE estableció en el caso Google Spain”).

La LOPDGDD regula específicamente el derecho al olvido en búsquedas de internet y en servicios de redes sociales o servicios equivalentes, en sus artículos 93 y 94 respectivamente

Derecho de oposición

En el ejercicio de este derecho, las personas interesadas pueden oponerse en cualquier momento a que los datos personales que le conciernan sean tratados por una Entidad Local por motivos relacionados con la situación particular de la persona solicitante.

Al igual que ya indicamos al analizar el ejercicio del derecho de supresión, debemos señalar que el de oposición tampoco es un derecho absoluto, y que una vez ejercido el mismo por persona interesada, la entidad local responsable es la que debe o bien dejar de tratar los datos personales, o bien continuar el tratamiento, debiendo para ello acreditar motivos legítimos imperiosos para dicho tratamiento y que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Es decir, salvo que tenga lugar dicha acreditación por parte de la entidad local responsable, se debe cesar el tratamiento de los datos contra el que se formulado dicha oposición.

DERECHO DE LIMITACIÓN DEL TRATAMIENTO

El RGPD define a la limitación del tratamiento como el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Ante una solicitud de ejercicio de este derecho, la entidad local responsable deberá estimar dicha solicitud cuando se dé al menos una de las siguientes circunstancias: que el interesado impugne la exactitud de los datos personales y procediendo en este caso la limitación durante un plazo que permita al responsable verificar la exactitud de los mismos, que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso, que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones, o que el interesado se haya opuesto al tratamiento y en este caso, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

DERECHO A LA PORTABILIDAD DE LOS DATOS

Este derecho nace con la intención de que las personas interesadas tengan en todo momento el control sobre sus propios datos, alentando la utilización de formatos interoperables que permitan la portabilidad de los mismos.

De este modo, este derecho permite a las personas interesadas recibir aquellos datos que solicite de un responsable al que se los haya facilitado, y le permite transmitirlos a otro responsable, sin impedimentos. La obligación del responsable, en este supuesto, consiste en facilitar los datos en un formato estructurado, de uso común y de lectura mecánica e interoperable.

Este derecho puede ejercerse cuando la legitimación del tratamiento por el responsable se base en el consentimiento o en un contrato, pero no cuando la base jurídica del tratamiento es otra, y por lo tanto no se aplicará, cuando el tratamiento se realice en uso de una obligación legal, interés público o ejercicio de poderes públicos.
La persona interesada tiene igualmente al solicitar la portabilidad de los datos personales que le concierne, a que éstos se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

DERECHOS DIGITALES DE LOS EMPLEADOS PUBLICOS

EMPLEADOS Y DISPOSITIVOS ELECTRONICOS

ELABORACIÓN DE CRITERIOS DE UTILIZACIÓN DE LOS DISPOSITIVOS DIGITALES (CON PARTICIPACIÓN DE LA REPRESENTACIÓN DE LOS TRABAJADORES DE LA E.L.)

APROBACIÓN DE DICHOS CRITERIOS O, AL MENOS, PLASMACIÓN EN DOCUMENTO ADMINISTRATIVO ELECTRÓNICO

INFORMACIÓN DE DICHOS CRITERIOS DE UTILIZACIÓN, Y ENTREGA DE LOS DISPOSITIVOS DIGITALES A LOS EMPLEADOS PÚBLICOS DESTINATARIOS

De este esquema parece extraerse la obligación de que las EELL dispongan de dichos “criterios de utilización de los dispositivos digitales” que entreguen a sus empleados públicos, cuya plasmación podría venir a través de una instrucción interna o en forma de acto administrativo (decreto de la Presidencia donde se aprueben dichos criterios), los cuales preceptivamente han debido ser “negociados” (no en sentido estricto, pero sí al menos con audiencia previa) con la representación unitaria, funcionarial o laboral, en función de los empleados públicos destinatarios, de dicha entidad local.

Dichos criterios de utilización de los dispositivos digitales, de los que los empleados públicos deben ser informados, deberán especificar usos autorizados y que se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

DERECHO A LA DESCONEXION DIGITAL

derecho a la desconexión digital, su finalidad es la de garantizar que los empleados públicos (y trabajadores en general), gocen fuera del tiempo de trabajo legal o convencionalmente establecido, del respeto a su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Se prevé expresamente que las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

LAS BASES DEL TRATAMIENTO

TRAMTAMIENTO Y LICITUD

PRINCIPALES BASES LEGITIMADORAS EN MATERIA DE PROTECCIÓN DE DATOS

BASES DEL TRATAMIENTO DE DATOS. ANALISIS

- El proceso de obtención de datos: se propone detallar los procesos habilitados para la recogida de datos personales respecto de cada colectivo de datos de carácter personal identificados.
- La base que legitima dicho tratamiento: respecto de cada proceso de obtención de datos, se propone analizar la base conforme a las distintas previsiones del RGPD, que legitima el tratamiento de datos de cada caso.
- La aportación de evidencias: en cumplimiento del principio de responsabilidad proactiva, se propone inventariar cada proceso de recogida de datos (indicando pantallazos, enlaces o vínculos), de modo que sirva de evidencia para justificar el correcto análisis de la base que legitima el tratamiento de datos en cada caso.

Principios relativos al tratamiento y licitud del tratamiento

- Limitación de la finalidad. Principio por el que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- Minimización de datos. Principio por el que sólo están amparados los tratamientos de datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que dichos datos son tratados.
- Exactitud. Principio por el que se adoptarán todas las medidas razonables para que se actualicen, supriman o rectifiquen los datos personales inexactos con respecto a los fines para los que se tratan. En este punto toma importancia la Disposición adicional octava de la nueva LOPD, que regula la Potestad de verificación de las Administraciones Públicas, y que más tarde retomaremos.
- Limitación del plazo de conservación. La regla general es que sólo deben conservarse el tiempo necesario para los fines del tratamiento de los datos personales.

APLICACIÓN PRACTICA DE BASE DE TRATAMIENTOS

Con carácter general, la base jurídica de los tratamientos de datos de las AAPP será o el cumplimiento de una obligación legal (art.6.1 c) RGPD) o, el necesario cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art.6.1e) RGPD).

El consentimiento (art.6.1a) RGPD) no se considera como base jurídica adecuada en las relaciones del ciudadano con las AAPP.

El RGPD excluye el interés legítimo (art.6.1f) RGPD) como posible base jurídica de los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones (sin distinguir si dichas funciones están sometidas al derecho público o al privado).

LEER ARTÍCULO 6 DEL RGPD

CESIÓN DE DATOS ENTRE AAPP

La Ley 40/2015 establece un deber de colaboración entre las Administraciones públicas (art.3.1k, 3.2 y 155), pero este deber está sujeto a que se respete el derecho a la protección de datos de las personas físicas (establecido en el art.13 h de la ley 39/2015). Dicha colaboración habrá de instrumentarse a través de las plataformas de intermediación u otros sistemas establecidas al efecto (art.28.2 Ley 39/2015 en relación con el art.155 Ley 40/2015).

*Por el Real Decreto 14/2019 de 31 de octubre se modifica el art. 155 de Ley 40/2015, insistiendo en que “En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales”). Como dice Victor Almonacid, la Administración necesita nuestros datos para sus cometidos públicos, no para vendernos aspiradoras.

BASE JURÍDICA EN OTROS CASOS ESPECIALES DE TRATAMIENTO DE DATOS PERSONALES EN AAPP.

TRATAMIENTO DE DATOS EN LAS SMART CITIES.

LA FIRMA BIOMÉTRICA COMO DATO EN LAS RELACIONES ELECTRÓNICAS CON LAS AAPP.

TRATAMIENTO DE LOS REGISTROS DE PERSONAL DEL SECTOR PÚBLICO (D.A 12 LOPD).

TRATAMIENTO DE DATOS DE CONTACTO, DE EMPRESARIOS INDIVIDUALES Y DE PROFESIONALES LIBERALES (ART.19 LOPD).

VIDEOVIGILANCIA (ART.22 Y 89 LOPD)

VIDEOVIGILANCIA CON FINES DE SEGURIDAD.

TRATAMIENTO DE DATOS EN EL ÁMBITO DE LA FUNCIÓN ESTADÍSITICA PÚBLICA (ART.25 LOPD).

TRATAMIENTO DE DATOS CON FINES DE ARCHIVO EN INTERÉS PÚBLICO POR PARTE DE LAS AAPP (ART.26 LOPD).

TRATAMIENTO DE DATOS RELATIVOS A INFRACCIONES Y SANCIONES ADMINISTRATIVAS (ART.27 LOPD).

TRANSFERENCIA INTERNACIONAL DE DATOS Y SU IMPACTO EN LA ADMINISTRACIÓN LOCAL

Cabrán cesiones de datos entre AAPP cuando sus competencias no sean diferentes o no versen sobre materias distintas (porque no se altera la finalidad de la recogida de los datos).

En caso de que la finalidad sea distinta, lo primero que deberemos comprobar es si existe una norma de Derecho de la Unión o estatal que permita el tratamiento para salvaguardar los objetivos del art.23.1 RGPD (“que constituya una medida necesaria y proporcional en una sociedad democrática”). Si existiese esa norma, el tratamiento basado en la misma sería lícito, aun cuando su finalidad fuese incompatible con la finalidad de su recogida.

Si no existiese esa norma, siendo la finalidad distinta de la finalidad inicial, se deberá realizar por la Administración cedente (responsable del tratamiento), una ponderación en los términos del art.6.4 RGPD, para determinar si el tratamiento con ese otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales. Con los siguientes criterios:

a. Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b. el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c. la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el art. 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el art.10;
d. las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e. la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

CONTENIDO MINIMO

a) nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) fines del tratamiento;
c) descripción de las categorías de interesados y de las categorías de datos personales;
d) categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales (incluidos los destinatarios en terceros países u organizaciones internacionales);
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y la documentación de las garantías adecuadas, de ser necesarias;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

https://www.pozuelodealarcon.org/tu-ayuntamiento/proteccion-de-datos-personales/registro-de-actividades-de-tratamiento

· REGISTRO DE ACTIVIDADES DEL RGPD

ADMINISTRACIÓN LOCAL (responsables de tratamiento)	**ENCARGADOS DE TRATAMIENTO DE LA ADMINISTRACIÓN LOCAL**
Nombre y datos de contacto del responsable (o representante).	Nombre y datos de contacto del encargado (o representante).
Fines del tratamiento	Categorías de tratamientos efectuados por cuenta de cada responsable
Nombre y datos de contacto del Delegado de Protección de Datos.	Nombre y datos de contacto del Delegado de Protección de Datos.
Categorías de datos personales.	....
Categorías de afectados.	....
Descripción de las medidas técnicas y organizativas de seguridad.	Descripción de las medidas técnicas y organizativas de seguridad.
Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.	
Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.	Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.
Cuando sea posible, plazos previstos para las supresión de las diferentes categorías de datos.	....

SUPUESTOS PRACTICOS

SUPUESTOS PRACTICOS Y DEBATE

¿SE PUEDEN CEDER DATOS DEL PADRÓN MUNICIPAL A PERSONAS FÍSICAS O EMPRESAS PRIVADAS?

No se puede enviar información sobre el Padrón Municipal a personas físicas o empresas privadas. Ahora bien, es frecuente que empresas de nueva instalación en el municipio soliciten el Padrón de habitantes al ayuntamiento, con el fin de enviar publicidad a los residentes sobre sus productos. La respuesta a esta petición ha de ser negativa, ya que no es una finalidad que esté reconocida entre las finalidad es del Padrón Municipal. ¿Y si se trata de un concejal?

¿SE PUEDE FACILITAR INFORMACIÓN SOBRE LAS PERSONASEMPADRONADAS EN UNA VIVIENDA AL PROPIETARIO DE LA MISMA? No es posible facilitar la información de las personas empadronadas en una vivienda ni incluso al propietario de la vivienda. No obstante, para poder empadronar en una vivienda a otra persona que no sea su propietaria es necesario que la persona interesada aporte una copia del título o contrato de arrendamiento del piso o una autorización escrita dela persona propietaria (o persona inscrita como principal ocupante de la vivienda) que legitime la ocupación. Si bien no es posible facilitar datos personales al propietario de una vivienda que solicita información sobre las personas ocupantes de la misma, sí se puede facilitar información sobre el número de personas ocupantes, sin identificarlas.

PUBLICACIÓN DE DATOS PERSONALES EN BOLETINES OFICIALES YTABLONES DE EDICTOS VIRTUALES ¿QUÉ CAUTELAS DEBEN SEGUIRSE? Si la actividad informativa obedece a una decisión discrecional de la entidad local la comunicación que incluya datos de carácter personal sólo puede tener lugar cuando se haya obtenido el consentimiento de las personas interesadas. Por el contrario, si la notificación o publicación a través de un boletín oficial o tablón de anuncios responde al cumplimiento de un deber legal fijado con suficiente precisión, nada impide la publicación de datos personales de las personas afectadas. Un supuesto de este tipo es cuando la publicación obedece a propósitos de transparencia, por ejemplo, con ocasión de la publicación de la composición de un Tribunal de Selección, a fin de que la ciudadanía pueda identificar a las personas bajo cuya responsabilidad se va llevar a cabo un proceso selectivo. Aún cuando la publicación responda aun deber legal, es necesario cumplir los siguientes criterios: Como buena práctica, en la publicación de datos personales en cualquier medio debe acudirse al principio de proporcionalidad. Esto es, sólo se publicarán aquellos datos personales que sean imprescindible para lograr el efecto legal pretendido y que no resulten excesivos. Los boletines oficiales y los tablones de edictos virtuales tienen la consideración de fuentes accesibles al público. En virtud de este carácter, la publicación de datos personales supone facilitar el conocimiento o acceso a terceras personas de datos personales sin el consentimiento dela persona afectada. Por ello, en la publicación oficial debe especificarse que sólo se autoriza el acceso para el fin de dar a conocer su contenido y que no cabe promover un uso abusivo de los datos personales publicados para otras finalidades.

¿SE PUEDEN PUBLICAR EN INTERNET LAS ACTAS DE LOS PLENOSMUNICIPALES Y DE LAS REUNIONES DE LA JUNTA DE GOBIERNOLOCAL CUANDO ÉSTAS CONTIENEN DATOS DE CARÁCTE RPERSONAL? Las actas de los plenos municipales se pueden publicar en internet, sin consentimiento de las personas cuyos datos aparecen en las mismas, si sedan dos condiciones: que así lo determine expresamente el Reglamento Orgánico de la entidad local y que la información con datos de carácter personal que contengan no afecte al honor, ni a la intimidad personal o familiar ni a la propia imagen de las personas afectadas. Las sesiones de los plenos de las corporaciones locales generalmente son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos si así se acuerda por mayoría absoluta. Sin embargo, las sesiones de la Junta de Gobierno Local no son públicas y por ello sus actas no pueden publicarse en internet. La exposición pública y resumida de las actas de los plenos municipales ,cualquiera que sea el medio a través del cual se realice, tiene como finalidad ofrecer una información genérica a los vecinos y a las vecinas y no tiene porqué ser una práctica informativa contraria a la normativa sobre protección de datos. Ahora bien, se aconseja eliminar de este resumen aquellos datos de carácter personal que no sean adecuados, pertinentes o que resulten excesivos y, por supuesto, datos personales especialmente protegidos. En los supuestos en que se autorice la grabación, por medio de imágenes y/o sonidos, de las sesiones que celebre el pleno municipal de la entidad local, esta grabación, y su correspondiente difusión, se suspenderá o limitará durante el tiempo que dure el debate de asuntos que puedan afectar al derecho a la intimidad personal o familiar.

¿PUEDE LA POLICÍA LOCAL CEDER DATOS PERSONALESRELACIONADOS CON ACCIDENTES DE CIRCULACIÓN A COMPAÑÍAS ASEGURADORAS? Sí. Es una de las excepciones, recogidas en la Ley, a la necesidad de solicitar el consentimiento para la cesión de datos personales. El responsable del fichero donde se recogen datos de accidentes de circulación puede facilitarlos datos personales recogidos a las compañías de seguros que actúen en calidad de parte interesada en el mismo. Con carácter previo a la cesión, es imprescindible que las compañías aseguradoras acrediten la representación de sus asegurados y que éstos tengan un interés legítimo y directo en el accidente, respecto al cual se solicita la información que dispone la policía local.

¿SE DEBE FACILITAR EL ACCESO A UN EXPEDIENTE DE URBANISMOEN TRAMITACIÓN A LA PERSONA QUE ACREDITE LA CONDICIÓN DE INTERESADA? Sí, se debe facilitar. El derecho de acceso reconocido en el artículo 13 de la LPAC, es una facultad esencial de la que se disfruta si se tiene la condición de persona interesada, esto es, si se tiene un interés legítimo en un determinado procedimiento administrativo, y cuyo ejercicio tiene verdadero sentido mientras dicho procedimiento se encuentra en tramitación.

¿QUÉ CAUTELAS ESPECIALES SE HAN DE OBSERVAR RESPECTODE LOS DATOS DE SALUD DE LOS TRABAJADORES? La entidad local recoge datos de salud de sus empleados para poder cumplir con sus obligaciones en materia de seguridad y salud laboral. La entidad local tiene la obligación legal de crear un servicio de prevención,que asume responsabilidades en prevención y protección de riesgos.Alternativamente, la entidad local puede contratar estos servicios con unaMutua de Accidentes de Trabajo y Enfermedades Profesionales.En este último caso, la entidad local ha de especificar en el contrato o convenio firmado con la Mutua lo relativo al acceso a los datos por cuenta de terceros, en concreto: cómo la mutua tratará los datos personales conforme a las instrucciones del responsable del tratamiento, que no los utilizará para un fin distinto al que figure en el contrato, ni los comunicará a otras personas, así como las medidas de seguridad que está obligada a implementar. Se ha de crear un nivel alto de protección en la actividad del tratamiento para recoger los datos de salud de los trabajadores. Estos datos de salud son especialmente protegidos. El acceso a los datos de salud de los trabajadores está restringido a los profesionales sanitarios de la entidad local o de la mutua y al propio trabajador. En supuestos concretos, se puede ceder información a los delegados de prevención del Comité de Seguridad e Higiene, si bien generalmente se facilitarán datos agregados o sociales y sólo excepcionalmente datos personales.

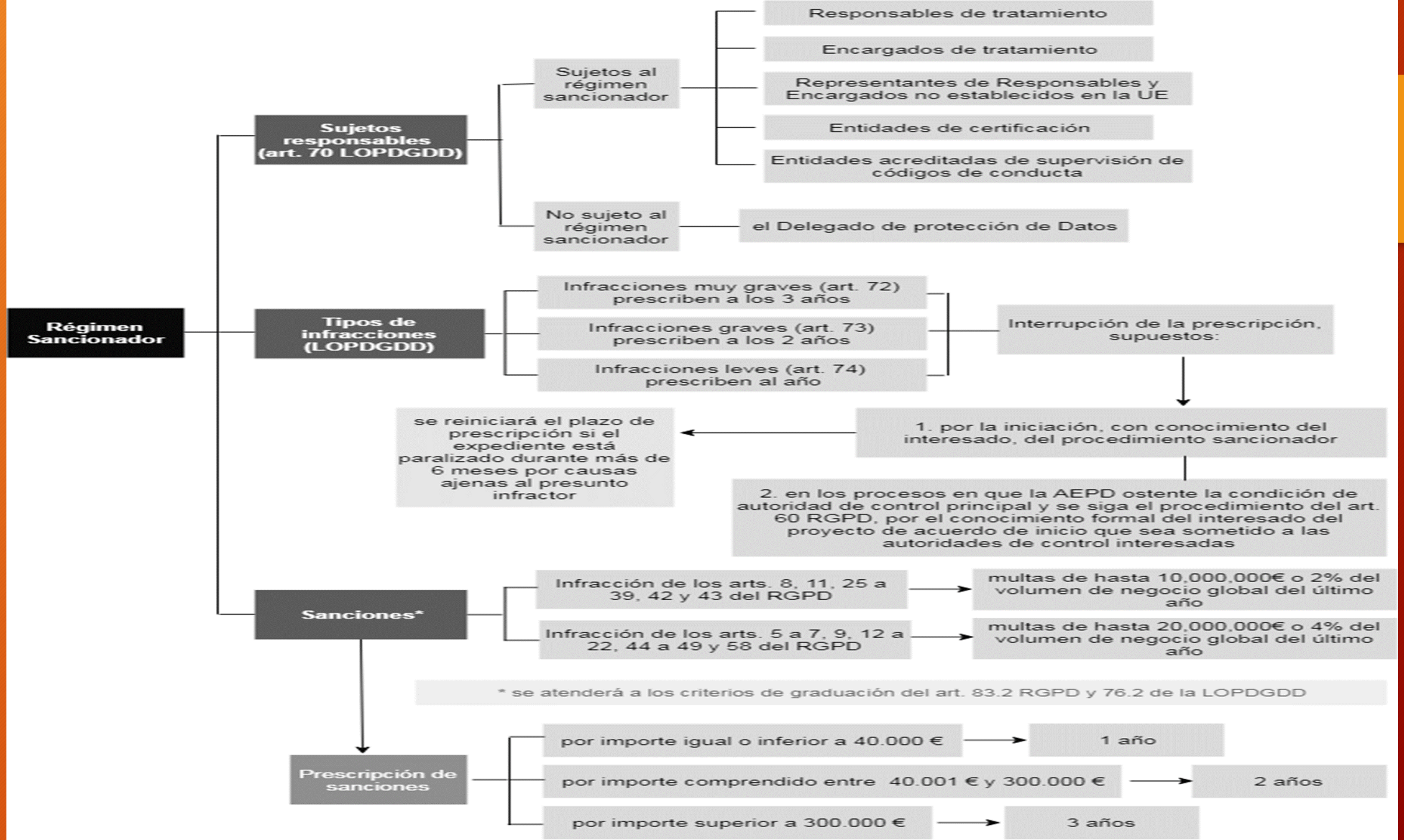
¿ES ADECUADO PUBLICAR EN INTERNET UNA GUÍA DECOMUNICACIÓN DE LA ENTIDAD LOCAL QUE INCLUYA, ADEMÁS DELA IDENTIFICACIÓN DE LOS PUESTOS DE TRABAJO QUE DAN UNSERVICIO PÚBLICO, LOS DATOS DE IDENTIFICACIÓN DE SUS OCUPANTES? Las organizaciones quieren facilitar su comunicación con los ciudadanos. De ahí que las entidades públicas identifiquen sus unidades de servicio, los puestos de trabajo y los datos de contacto (correo electrónico, teléfono y dirección postal) y los publiquen en guías de comunicación, en formato papel y en formato electrónico. Respecto a la cuestión sobre la publicación, en particular en internet, también de los datos de identificación personal (entiéndase, el nombre y los apellidos)de las personas que ocupan los puestos de trabajo, esta práctica comunicativa ha originado frecuentemente conflictos entre los trabajadores y su entidad cuando no ha estado precedida de la solicitud del consentimiento previo alas personas para hacerlo. Desde un punto de vista práctico, esto es, para acercar la administración aun ciudadano y poder ofrecerle la información que necesite con prontitud,por ejemplo, con una simple llamada, no parece necesario, ni proporcional al fin pretendido, la publicación en internet de los datos personales de un funcionario. Máxime cuando, en ocasiones, la rotación de las personas en los puestos o su ausencia en períodos vacacionales o durante bajas laborales puede resultar en que haya que pensar en modificar, provisional o definitivamente, los datos personales publicados en internet.En cualquier caso, si una entidad local decidiera publicar una guía de comunicación incluyendo los datos identificativos de sus empleados de previsible aplicación restrictiva, parece que una práctica muy recomendable es solicitar a los trabajadores su consentimiento previo para hacerlo y explicitar en la publicación que la información no constituye una fuente de acceso público.

QUÉ DATOS PERSONALES SE PUEDEN PUBLICAR EN LOS LISTADOSDE ASPIRANTES, CANDIDATOS O RESULTADOS, DERIVADOS DE LAGESTIÓN DE LOS PROCESOS SELECTIVOS O DE CONCURSOS DE TRASLADOS?

https://www.aepd.es/prensa/2019-03-04.html

El criterio, provisional hasta que los órganos de gobierno y las administraciones públicas competentes aprueben disposiciones para la aplicación de la Disposición, pretende evitar que la adopción de otras fórmulas pueda dar lugar a la publicación de cifras numéricas de los documentos identificativos de las personas en posiciones distintas, posibilitando la recomposición íntegra de dichos documentos. Para ello, se ha seleccionado aleatoriamente un grupo de cuatro cifras numéricas, que deberían ser las mismas en todas las publicaciones

REGIMEN SANCIONADOR


Régimen Sancionador
Sujetos responsables (art. 70 LOPDGDD)
Sujetos al régimen sancionador
Responsables de tratamiento
Encargados de tratamiento
Representantes de Responsables y Encargados no establecidos en la UE
Entidades de certificación
Entidades acreditadas de supervisión de códigos de conducta
No sujeto al régimen sancionador
el Delegado de protección de Datos
Tipos de infracciones (LOPDGDD)
Infracciones muy graves (art. 72) prescriben a los 3 años
Infracciones graves (art. 73) prescriben a los 2 años
Infracciones leves (art. 74) prescriben al año
Interrupción de la prescripción, supuestos:
1. por la iniciación, con conocimiento del interesado, del procedimiento sancionador
se reiniciará el plazo de prescripción si el expediente está paralizado durante más de 6 meses por causas ajenas al presunto infractor
2. en los procesos en que la AEPD ostente la condición de autoridad de control principal y se siga el procedimiento del art. 60 RGPD, por el conocimiento formal del interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas
Sanciones*
Infracción de los arts. 8, 11, 25 a 39, 42 y 43 del RGPD
multas de hasta 10,000,000€ o 2% del volumen de negocio global del último año
Infracción de los arts. 5 a 7, 9, 12 a 22, 44 a 49 y 58 del RGPD
multas de hasta 20,000,000€ o 4% del volumen de negocio global del último año
* se atenderá a los criterios de graduación del art. 83.2 RGPD y 76.2 de la LOPDGDD
Prescripción de sanciones
por importe igual o inferior a 40.000 €
1 año
por importe comprendido entre 40.001 € y 300.000 €
2 años
por importe superior a 300.000 €
3 años

Cuestiones prácticas para la admon local

- **El ámbito de aplicación de ese régimen excepcional o singular se extiende a todas las Administraciones Públicas, organismos públicos, fundaciones y consorcios, así como (blindaje político puro) a los grupos parlamentarios y a los grupos políticos locales**. Pero no, adviértase, a las sociedades mercantiles vinculadas a la Administración matriz, a las que se les aplicaría el régimen general de sanciones del RGPD y de la LOPDGDD.
- **Si el responsable o encargado cometieran alguna infracción sería sancionado con *apercibimiento* y adopción, en su caso, de las medidas pertinentes**. La notificación se trasladará también a los interesados.
- **La autoridad de control "propondrá"** (atentos a la fórmula verbal) también **la iniciación de actuaciones disciplinarias** cuando existan indicios suficientes para ello, que se tramitarán según la normativa sancionadora aplicable.
- En cualquier caso, **si la infracción es imputable a una autoridad o directivo, y se acredita que se apartaron de los informes técnicos o recomendaciones sobre el tratamiento** (la figura del DPD, emerge), "en la resolución en la que se imponga **la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará su publicación en el Boletín Oficial del Estado o autonómico** que corresponda". Nada se dice de publicarlo también como exigencia de publicidad activa en el Portal de Transparencia o en la página Web de la entidad pública a la que pertenezca, en su caso, el responsable o encargado del tratamiento. Artículo 77 de la Ley 3/2018.

CUESTIONES DE SEGURIDAD Y PROTECCION DE DATOS

¿Hay algún informático en la sala?

LA EVALUACION DE IMPACTO

El Reglamento General de Protección de Datos (RGPD) introduce el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD) en su artículo 35.

Una EIPD es un proceso ligado a los **principios de protección de datos desde el diseño y protección de datos por defecto** concebido para describir, de **manera anticipada y preventiva**, un tratamiento de datos personales, evaluar su necesidad y proporcionalidad y gestionar los potenciales riesgos para los derechos y libertades a los que estarán expuestos los datos personales en función de las actividades de tratamiento que se lleven a cabo con los mismos, determinando las medidas necesarias para reducirlos hasta un nivel de riesgo aceptable.

Esta obligación debe entenderse en el contexto de la responsabilidad proactiva y la obligación general de gestionar adecuadamente los riesgos y demostrar que se han tomado las medidas adecuadas para garantizar el cumplimiento de los requisitos exigidos por el RGPD.

Herramienta FACILITA


Análisis preliminar
Analizar la necesidad de realizar una EIPD
Contexto
1
Describir el ciclo de vida de los datos
2
Analizar la necesidad y proporcionalidad del tratamiento
Gestión de riesgos
3
Identificar amenazas y riesgos
4
Evaluar los riesgos
5
Tratar los riesgos
Conclusión y validación
6
Plan de acción y conclusiones
Supervisión
Supervisar y revisar la implantación
Consulta y asesoramiento por parte del DPD
Revisar ante cambios en el tratamiento

El Esquema Nacional de Seguridad en el marco de la LOPDP.

La Disposición Adicional Primera de la LOPDP, dedicada al establecimiento de “medidas de seguridad en el ámbito del sector público” establece taxativamente en su apartado 2 que se “deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad” (en adelante, ENS), obligación que en la esfera local se encomienda a los responsables o encargados del tratamiento de la correspondiente Entidad.

Del mismo modo, conviene destacar que en el año 2015 se aprobó el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, derivado de la necesidad de dar una respuesta a la evolución en el entorno regulatorio (en particular, a la necesidad de adecuar el ENS al Reglamento 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE), y de reforzar la protección de las Administraciones Públicas frente a las crecientes ciberamenazas, mediante una adecuación a la rápida evolución de las propias tecnologías de la información, partiendo de la experiencia acumulada en la previa implantación del ENS.

Asimismo, conviene indicar que el Centro Criptológico Nacional ha elaborado una serie de documentos bajo la nomenclatura CCN-STIC (Centro Criptológico Nacional – Seguridad de las Tecnologías de Información y Comunicaciones) que ofrece normas, instrucciones, guías y recomendaciones para aplicar el ENS y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración. En particular, la serie CCN-STIC-800 viene a establecer las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS; y de entre esta serie, debe destacarse muy especialmente la Guía de Seguridad de las TIC CCN-STIC-883, para la implantación del ENS en Entidades Locales.

¿COMO LO HACEMOS ?

En efecto, uno de los principios básicos sobre los que descansa la arquitectura del ENS es la gestión de riesgos (artículo 4, letra b), del ENS). A este respecto, el artículo 6.2 del ENS prevé que “la gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.”

Por su parte, el artículo 13 del ENS establece la obligación para cualquier Entidad que desarrolle e implante sistemas para el tratamiento de la información de realizar su propia gestión de riesgos, y ello mediante el análisis y tratamiento de los riesgos a los que está expuesto el sistema, para lo cual “se empleará alguna metodología reconocida internacionalmente”. A tal fin, el Consejo Superior de Administración Electrónica ha desarrollado la “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, conocida por su acrónimo MAGERIT, sustentada sobre las normas ISO 27001 e ISO 31000, y mediante la cual se implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

En consecuencia, a fin de garantizar el mantenimiento de un entorno controlado, minimizando los riesgos en el tratamiento de los datos personales hasta niveles que se consideren aceptables o residuales, el responsable y el encargado del tratamiento deberán llevar a cabo un análisis de los riesgos a los que se encuentra expuesto el sistema, ponderando particularmente los aspectos mencionados por el artículo 32 del RGPD.

A la vista del análisis de riegos efectuados, el responsable y el encargado del tratamiento deberán proceder en última instancia al despliegue de las medidas de seguridad técnicas y organizativas que resulten necesarias para paliar, mitigar o suprimir los riesgos a los que esté expuesto el sistema, medidas que en todo caso deberán estar justificadas y resultar proporcionadas a los riesgos que pretendan paliar, debiendo establecerse un equilibrio entre la naturaleza de los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad adoptadas.

75 MEDIDAS DE SEGURIDAD RECOGIDAS EN EL ENS

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

- POLÍTICA DE SEGURIDAD
- NORMATIVA DE SEGURIDAD
- PROCEDIMIENTOS DE SEGURIDAD
- PROCESO DE AUTORIZACIÓN

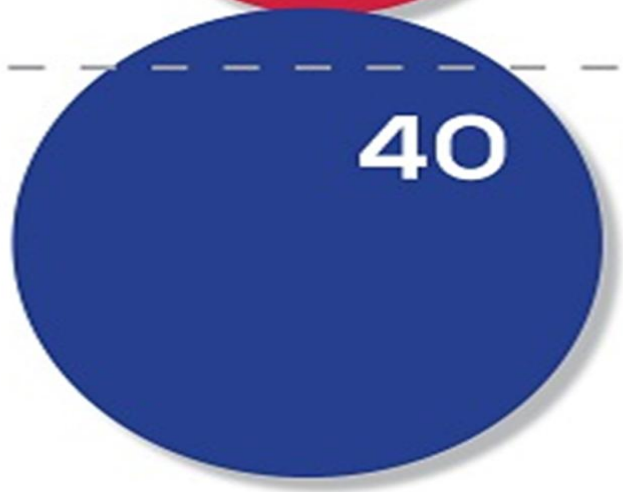
MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

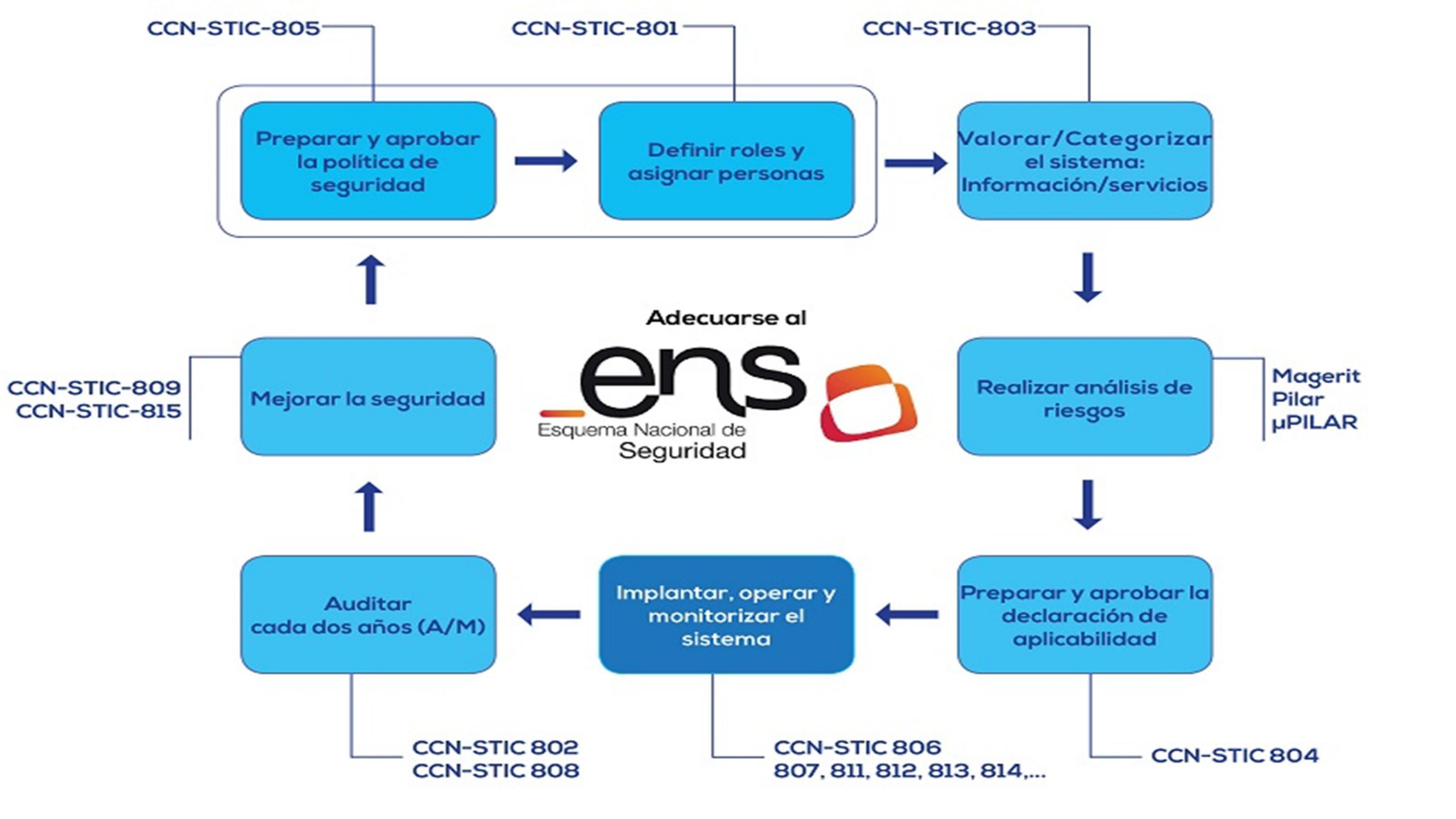
- PLANIFICACIÓN
- CONTROL DE ACCESO
- EXPLOTACIÓN
- SERVICIOS EXTERNOS
- CONTINUIDAD DEL SERVICIO
- MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad



- INSTALACIONES E INFRAESTRUCTURAS
- GESTIÓN DEL PERSONAL
- PROTECCIÓN DE LOS EQUIPOS
- PROTECCIÓN DE LAS COMUNICACIONES
- PROTECCIÓN SOPORTES DE INFORMACIÓN
- PROTECCIÓN APLICACIONES INFORMÁTICAS
- PROTECCIÓN DE LA INFORMACIÓN
- PROTECCIÓN DE LOS SERVICIOS


CCN-STIC-805
CCN-STIC-801
CCN-STIC-803
Preparar y aprobar la política de seguridad
Definir roles y asignar personas
Valorar/Categorizar el sistema: Información/servicios
Adecuarse al
ens
Esquema Nacional de Seguridad
CCN-STIC-809
CCN-STIC-815
Mejorar la seguridad
Realizar análisis de riesgos
Magerit
Pilar
µPILAR
Auditar cada dos años (A/M)
Implantar, operar y monitorizar el sistema
Preparar y aprobar la declaración de aplicabilidad
CCN-STIC 802
CCN-STIC 808
CCN-STIC 806
807, 811, 812, 813, 814,...
CCN-STIC 804

ALBACETE 2019
David Povedano Alonso
twitter: @pove22
e-mail: pove22@gmail.com

DIPUTACIÓN DE ALBACETE

MUCHAS GRACIAS POR SU ATENCION

Ayuntamiento de Collado Mediano:
David Povedano Alonso Secretario General